HP Service Manager

Software Version: 9.41

For the supported Windows® and UNIX® operating systems

Incident Management 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

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

Incident Management overview

You can use HP Service Manager Incident Management to automate reporting and tracking of a single incident or a group of incidents. Incident Management restores normal service operation as quickly as possible and minimizes the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. Incident Management helps you achieve service performance that meets Service Level Agreement (SLA), Operation Level Agreement (OLA), and Underpinning Contract (UC) targets. Incident Management enables you to achieve the following results:

- Require Incident records to follow a set process
- Define the users who are responsible for an type incident, and automatically notify them incident opens or escalates
- Issue alerts or escalate an incident to properly meet the agreed-upon terms of the service contract
- Include SLT information in a incident record
- Post device outages to the SLA application
- Plan outages based on services that could be affected, based on the CIs specified in an incident or change

What is an incident?

Incidents include any event which disrupts, or which could disrupt, a service. This includes events that are communicated directly by Users, either through the Service Desk or through an automated interface between Event Management and Incident Management tools.

Incidents can also be reported and logged by support staff, who may notify the Service Desk if they notice an issue. Not all events are logged as incidents. Many classes of events are not related to disruptions at all, but are indicators of normal operation or are simply informational.

View affected services of Incidents and Changes

If you want to see a list of services that are potentially affected by an outage related to the CIs specified in an Incident or Change record, click the **View Affected Services** command on the **More**

menu. When you open an Incident record, you can examine detailed information for any of the CIs in the list to determine the potential impact of an outage relating to critical, dependent services. The **View Affected Services** command also enables you to plan appropriately when you open a Change record. You can determine how a planned outage affects these services.

When you click **View Affected Services** on the **More** menu, the system processes the outage spreads relating to the CIs in the Incident or Change record by browsing the configuration relationship records in the `cirelationship` table. This process is independent of any outage dependency information specified in the relationship records. No matter how many hierarchy levels a CI is above or below a service, the system browses all levels from the CI in the record to build a list of CIs. After this list is built, the system searches for any outage dependency information specified in the relationship records for those CIs in the list and removes any CIs that do not meet the conditions for outage dependencies. This final list of CIs then opens and you can select a CI for detailed information from the Configuration Management record.

Note: The list of CIs generated does *not* include the CIs specified in the primary Incident or Change record.

Affected Item field in Incident Management

The information available to populate the **Affected Item** field on the CIs and Services tab depends on conditions related to the service recipient. For example, if the recipient has individual or department subscriptions, a list of CIs associated with those subscriptions opens. If a recipient does not have any subscriptions, the following behavior occurs:

- If there is an incident recipient, a list of the CIs assigned to that recipient opens.
- If there is a location, a list of the CIs assigned to that location opens.
- If the system has several companies and there is a company specified, a list of the CIs assigned to that company opens.
- If there is a device type specified, a list of the CIs of that type opens.

Note: If you want to obtain a list of all CIs, do not enter any recipient information before you click the **Affected Item** field.

Creating an incident

HP Service Manager allows you to create an incident via several ways.

You can directly create a new incident in the In the Incident Management module by clicking **Incident Management** > **Create New Incident**.

You can also create an incident by escalating an interaction. For example, if a user cannot print to the network printer, the user calls the Service Desk for help. The Service Desk Agent creates a service desk interaction record to capture the service request. If the agent discovers that he or she cannot resolve the issue during the phone call, the agent escalates the interaction into an incident.

The Incident Coordinator reviews the information and verifies that it is assigned to the correct group. An Incident Analyst resolves the issue or escalates it to initiate a change. When the issue is resolved, the Service Desk Agent informs the user that the record is closed. All phases of this incident are tracked, from opening the service desk interaction record, escalating the incident, resolving the incident, and closing the record.

Activities section

The Activities section allows users to enter new updates for a record or to view journal updates and historic activities for a record.

Note: The Activities section is only available in the interactions that are categorized as complaints or compliments.

New update

Field	Description
New Update Type	Specifies or categorizes the activity update (for example, communication with the customer)
Visible to Customer?	Makes the update visible to customers so they can view related interactions via self service
New Update	Used to enter notes to explain and describe updates made for the record. If Journaling is enabled, the text entered here is displayed in Journal Updates. If Activities are enabled, the text entered in this field is displayed as an activity record for the selected activity type. **Note:** The System Administrator is responsible for enabling Journaling and Activities.

Journal updates

Journal updates displays text entered in the **New Update** field together with a timestamp for the update. This field displays information when Journaling is enabled.

Activity type

To filter the list by the type of activity, select an activity type, and then click **Filter**. Service Manager opens a new record list that displays the records of that activity type.

The activities list displays activities for the current record. The activities are listed in order of occurrence, with the most recent activity displayed first. The following information is displayed for each activity:

- Date/Time
- Type
- Operator
- Description

Incident Details section

Use the following information as a guide when you add data to an incident.

Field	Description
Title	A short description summarizing the incident.
Description	A description of the incident in more detail.
Incident ID	The system-generated unique ID for this incident.
Status	Displays the status of the incident. These statuses are available in the out-of-box: **Categorize** means the incident is being categorized. **Assign** meas the incident is assigned. **Work In Progress** means work is underway to resolve this incident. **Pending customer** means awaiting action from the customer who reported the incident. **Pending Evidence** means that you need evidence from the customer or vendor. **Pending Vendor/Supplier** means awaiting action from a vendor/supplier. **Pending Parent Incident** menas tThe incident has been linked to a parent incident and

Field	Description
	is waiting for the resolution of the parent incident. This status is automatically set when an incident is linked to a parent incident. **Pending Other** means that you need something from an outside source other than customer or vendor. **Resolved** means there is a resolution, but it has not yet been verified by the customer. **Suspended** means the customer has agreed to suspend the incident for a period of time; the incident does not appear in your Inbox during this period.
	The current phase of this incident.
Primary Affected Service	The service affected by the registered issue. Only services the service recipient has a subscription for can be selected.
Affected CI	The configuration item (CI) the incident is registered for. Using Fill shows the CIs that are part the affected service. Other CIs can be entered manually.
CI is operational (no outage)	If selected (set to true), indicates the item is currently operational and there is no outage.
Outage Start Time	A date/time stamp for when the service outage started.
Outage End Time	A date/time stamp for when the service outage ended.
Requested By	The name of the operator who opens the incident.
Contact Person	The contact person for this incident.
Location	The service recipient's location
Major Incident	When this option is selected, the incident requires the Major Incident Review process.
Escalated	Select this option to mark the incident for escalation. When this option is selected, the **Escalation Team** section appears.
Incident Manager	An incident manager need be specified when the **Major Incident** or **Escalated** option is selected.
Parent Incident	This option indicates if the incident is a parent incident. You can link one or multiple child incidents to a parent incident if they are related in a certain way.
Link to Parent Incident	The parent incident of the current incident. This field is unavailable when the **Parent Incident** option is selected.

Field	Description
Category	The out-of-box system has four incident categories: Incident, Complaint, Request for Administration, and Request for Information. When you escalate an interaction into an incident, the new incident inherits the category from the interaction.
Subcategory	The subcategory of the incident.
Area	Depending on the selection of a category, a different list appears describing the area of concern for the incident.
Assignment Group	The support group assigned to work on this incident.
Assignee	The name of the person assigned to work on this incident. This person is a member of the assigned support group.
Impact	The impact the incident has on the business. The impact and urgency are used to calculate the priority.
Urgency	The urgency indicates how pressing the incident is for the organization.
Priority	The order in which to address this incident in comparison to others.
Source	The source of the incident.
Expected Solution Time	The expected time when the incident is resolved.

Note: When you view an existing incident, shaded fields are not available for more input. Incident Management populates these fields from information stored in associated records. You can update the associated record to increase the amount of information in these read-only fields.

Related Records in Incident Management

HP Service Manager lists all related records for the incident on the Related Records section. All information is read-only, but a user can click a record ID to view the related record. The related records are listed in alphabetic order by the module file name: Change (cm3r), Interaction (incidents), Incident (probsummary), Request (request), Problem (rootcause). Within each module the records are sorted by ID in ascending order.

The Related Records section contains the following fields.

Field	Description
ID	The related record number in the database.
Type	The link type between the related record and the incident.
Phase	The current phase of the related record.
Status	The current status of the related record.
Title	The title of the related record.

SLT section

HP Service Manager populates the information in the SLT section with one or more Service Level Agreement records associated with the asset. If no agreement exists, the section is blank. All the information is read-only.

The **Next Expiration** field displays the next immediate deadline from all matching SLTs. The SLT section contains the following subsections that list the details of the specific SLTs.

SLT type	Description
Process Targets	Lists all of the matching SLTs from all of the associated SLAs.
Uptime Targets	Lists the percentage of time that all SLTs are available.
Max Duration Targets	Lists the acceptable amount of time for an outage for all SLTs.
Upcoming Alerts	Lists the alerts for all of the SLTs.

Note: When you view an existing record, shaded fields are not available for more input. Incident Management populates these fields from information stored in associated records. You can update the associated record to increase the amount of information in these read-only fields.

Hover-over forms for incident records

In Incident Management, incident forms for open, update, and close include hover-over forms. A hover-over form opens for a field that supports hover-over forms when a user moves the mouse over the field. The hover-over form only opens when the field contains data. The data displayed on hover-over forms is read only.

The incident record forms (open, update, close) contain the following hover-over fields.

Field	Subform fields
Contact	Full Name, Telephone, Email
Affected CI	Critical CI, Pending Change

Posting outages

The Incident Management application can be used to post outage information about devices in the system into the SLA application when you open or close incidents. The system posts outages both manually and automatically.

When posting outages manually, Incident Management displays the Post Which Outages? form for the selected device when you open and close and incident. Use this form to specify the exact start and stop time of the outage instead of the time the outage was reported. Click **OK** to continue opening or closing the incident.

The current time is the default value in manual mode. You may accept the default or type the exact time.

Incident Management contract management records

Contract Management integrates service contract information and tracking into the service desk. You can enable the application or set automatic labor and parts calculation features for Contract Management in the Contract Management configuration record.

Incident Management and service level agreements

Incident Management supports the selection of more than one applicable SLA for an incident. When you create an incident, you can choose a Customer SLA for the contact, one or more applicable Service SLAs for the contact's subscriptions to a service, or no SLAs at all. Service SLAs only apply if the incident references a Business Service, the contact has a subscription to the service, and the subscription references an SLA. The following describes the system's process for adding SLAs to an incident.

- If one SLA is associated with the incident based on the contact, the Customer SLA is added to the incident.
- If the contact has an Individual Subscription for the CI, the Service SLA from that subscription is added to the incident.

- If the contact has a Department Subscription for the CI, the Service SLA from that subscription is added to the incident.
- If the contact has neither, then no Service SLA is added to the incident

The SLAs should contain all Service Level Targets (SLTs) that define the business rules for all response and availability metrics. You can choose as many SLTs as necessary to describe your response or availability commitment. If necessary, you can add more SLTs that meet your criteria.

When you view the new record, the **SLT** section lists the SLTs that apply to the incident.

Open the related topics to find the definitions for Customer SLA and Service SLA.

Parent and child incidents

The parent-child relationship allows you to link multiple incidents that are related in a certain way. For example, a network outage results in multiple similar incidents from different users. You can link these incidents under a parent incident. In this way, the activities that occur to the parent incident are automatically recorded under the **Activities** section in all child incidents and related Service Desk interactions (if there are any). In addition, you can also configure if the child incidents are automatically closed when the parent incident is closed.

Major incident

If the impact or priority of an incident increases, the incident may become a major incident. For a major incident, you may need problem management activities to identify the root cause, and take appropriate actions and plans to prevent future major incidents from occurring.

After you mark an incident as a major incident, the incident has a **Major Incident Review** section and the **Review Details** field in this section is mandatory in the Review phase. HP Service Manager also notifies the specified Incident Manager about the major incident.

Incident access control

The Incident Management module utilizes security roles and security rights to authorize users in creating, modifying, and closing records. These settings allows you to grant a user with proper rights. For example, a user can create and close records, but cannot modify records that are not assigned to this user.

Service Manager also provides a security control to segment data between multiple customers. The Mandantan controls identify which customer data a particular user or group can access or update.

Incident updates: Incident diagnosis details

HP Service Manager provides an audit trail capability that identifies each step in the diagnosis and resolution of an Incident record. Each time the record is updated, Service Manager creates a separate historical activity record for that specific Incident record, including which operators took what actions at what times. An authorized user may leaf through each historical activity record of an Incident record to develop a comprehensive understanding of the history and resolution of the Incident record.

The Incident record also includes a field to capture the resolution of the record.

Incident logging: manual

HP Service Manager allows the following approaches to manually create an Incident record:

- Authorized Service Desk users can create an Incident record directly within the HP Service Manager Incident Management module.
- Service Manager also includes a web-based, self-service interface that allows end users to create service requests through an easy-to-complete form. Once the form is complete, Service Manager routes the request through the Service Desk module to the appropriate Service Desk technician, who can then escalate the request to an Incident record. Users can track, update, or close their requests through this interface.
- An Incident record can be created through the web services and event services interfaces. These interfaces are used by existing integrations to network and systems management (NSM) tools (both HP's and third party's) and could be used in customer-created integrations to home-grown tools.

Incident logging: templates and related incidents

You can quickly create a new Incident record by copying an existing Incident record, or by applying templates. The HP Service Manager template functionality allows authorized users to create templates for common tasks in the Service Desk, Incident, and Change Management modules. Templates include predefined information for some or all fields of a record. A user can create an Incident record and apply a template, which can automatically fill in some or all fields of the record to save the user's effort.

Alerts and escalation

There are several ways of providing alerts and escalations in HP Service Manager:

1. Notifications: Service Manager provides a broad and deep solution to deliver notifications to incident stakeholders whenever the incident is opened, updated or closed. Administrators have complete control of the following areas in the notification engine:

    a. The notification vehicle (email, page, etc) and format

    b. The conditions on which the notification is sent

    c. The receiver of the notification

2. Alerts: The administrator can configure alerts in the incident workflow and SLM targets. When these targets are met, specified users receive alerts and notifications.

3. Escalation: The **Escalated** option in an incident record allows you to mark an incident for escalation. Once you select this option, you must specify an appropriate incident manager. After you save the incident, the incident manager and the incident assignee will then receive a notification about this escalated incident.

4. 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 Targets 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.

Incident escalation: Functional escalation

HP Service Manager includes pre-defined workflows reflecting HP's best practices based on ITIL 2011 guidance. These best practices come from HP's professional services organization and are developed through working with some of the HP's primary partner companies.

By default, Incidents are assigned to the service desk for acceptance as an Incident and assignment to the appropriate group.

Based on customer process requirements, assignment can be automated. Service Manager can be configured to automatically define record assignment based on values in any of the Incident record fields.

For example, escalations can be defined in the category record associated with an incident record or in SLAs that are applied to the record. Escalations include notifications and alerts (as the record passes through escalation levels). Service Manager can send alerts to different users, managers, and IT staff as the record is escalated.

SRC Support Catalog also allows automatic opening and routing of Incident records based on pre-defined categories and items.

Field-level controls

HP Service Manager provides two basic methods for setting field level controls including making the field mandatory. The system provides two methods to indicate that a field is mandatory in the UI.

If the field only needs to be mandatory on a screen-by-screen basis, you can set the field as mandatory via a RuleSet validation. This control can be visually indicated via a property in forms designer.

If the field needs to be mandatory for all access points throughout the system, you can set a workflow-level or table-level Rulset validations by using the supplied configuration tools. In this case, the visual indication is automatic.

Visually on the screen, the system identifies a mandatory field with a red asterisk.

Incident record data model

Incident Management enables you to track different types of information related to an incident, such as categorization, prioritization, description, contact information, and so on.

Incident data model: Contact details

HP Service Manager stores related contact information, including the operator who opened the incident and the contact person for the reported issue, with the preferred method of contact (email, phone, or other).

Incident data model: Categorization

HP Service Manager categorizes or classifies Incidents according to the following information:

- Category
- Subcategory
- Area

In an out-of-box Service Manager system, Service Manager automatically applies the Incident category to the new Incident that you create. If the Incident Management module has other customized categories, you need to select a category when you create a new Incident. Based on the selected category, Service Manager presents a filtered set of choices for Area and Subarea.

The Incident record also captures the ID of the failed CI or service, including the failing component.

Incident data model: Priority

The Incident record form includes fields to capture impact, urgency, and priority. HP Service Manager automatically derives the priority code based on the impact and urgency codes, but this mechanism can be manually overridden.

Service Manager automatically assigns urgency based on the Category of a record. However, system administrators can define additional rules for assignment based on any parameter, such as the CI that is the subject of the record, the caller who is the subject of the record, an SLA associated with the record, and so on.

An Incident record has the following impact and urgency codes.

Impact codes:

- 1 - Enterprise
- 2 - Site/Dept
- 3 - Multiple Users
- 4 - User

Urgency and priority codes:

- 1 - Critical
- 2 - High

- 3 - Average
- 4 - Low

Incident data model: Assignment

The Incident record stores the assignee group and an individual assignee within the group, if known. The Incident record also captures the name of the vendor/supplier to which the record has been assigned, if appropriate.

Incident data model: Symptoms

An Incident record has a field for the brief summary (the Title) of the issue and a free text field for the details of the problem or symptoms of the fault, which can be used as the search information for the built-in Knowledge Management capability.

Incident data model: Status

HP Service Manager tracks the status of an Incident in the **Status** field. Service Manager provides the following out-of-box status codes, other codes can be easily added to meet customer requirements.

- **Categorize**
- **Assign**
- **Work In Progress**
- **Pending customer**
- **Pending Evidence**
- **Pending Vendor/Supplier**
- **Pending Other**
- **Resolved**
- **Suspended**

Incident data model: Resolution

Help desk operators are prompted to enter record resolution information when they close records, including a Closure Code (this is a mandatory field). HP Service Manager provides out-of-box Closure Codes, which can be tailored to meet the customer's requirements. Resolutions can be promoted as candidates for the knowledgebase. Knowledgebase entries can also be used as the resolution for the Incident record.

Incident data model: Closure

HP Service Manager allows users to enter a Closure Code when a record is closed. The Closure Code can be compared to the category recorded at open time to report on trends. In addition, Service Manager automatically captures the time and date of Incident closure for reporting.

Incident data model: Incident source

When the source of the incident is a person, the Interaction record linked to the Incident record shows the basic information of the source. For example, the following information:

- Whether the Incident is opened through the self-service interface
- The Incident trigger
- The location of the issue

When the source of the incident is an event trigger, the Title and Description fields of the Incident record contain that information, which reference the source event displayed in the External ID field of the Event Browser in HP Operations Manager.

Incident and Service Request separation

Service Requests can be handled within the Service Desk module, supported by the Service Catalog module. Service Requests are tracked as Service Desk Interactions and can be fulfilled using Incident Management, Change Management, Request Management, or another fulfillment engine specified by in the Service Catalog configuration. Service Requests that do not originate from the Service Catalog and instead come directly to the Service Desk can be routed to the appropriate fulfillment mechanism by the Service Desk Analyst or they can be completed and closed at the Service Desk.

Incident data model: Configuration Item details

HP Service Manager has a Configuration Management module that captures information on CIs (individual, groups, and services). CIs can be captured as the subject of an Incident record, which links the records. Users can access a subject CI record from an Incident record, and can access all Incident records associated with a CI from the CI record.

When initiating an Incident, the user can attach a CI if known at the time. The user can, given the correct access rights, “drill down” to the CI details.

Through integration with HP UCMDB discovery capabilities, users can investigate and compare differences between the managed state of a CI and the discovered actual state. For example, if these are different, the difference could have been caused by an unsuccessful recent change to the CI.

Incident integration: Configuration Management system

HP Service Manager is fully integrated with the HP UCMDB CMS solution. This is a federated solution that integrates with the HP-provided discovery tools as well as those provided by other vendors.

Incident integration: Change Management

Out-of-box, the HP Service Manager Incident Management module is fully integrated with the Change Management module. Users can open Change request records from Incident records. Service Manager can pass relevant information from the Incident record to the Change request record. The two records are linked automatically.

Authorized users can access the Change Management module, create Changes associated with an Incident record, search for Change requests, view the Calendar, link an Incident record to an open Change request, and so on.

Incident integration: Incident matching with RFCs

HP Service Manager allows linkage between Incidents and Changes, and provides tools for users to establish the linkage. Users can link an existing Change or a newly created Change to an Incident. Service Manager can use business rules to manage the relationships. For example, Service Manager can use business rules to set all the related Incidents to “Resolved” when the related Change is resolved. Related users can then check if these Incidents can be closed.

Incident integration: Knowledge Management

The HP Service Manager Knowledge Management module allows end users and service-desk personnel to get speedy and accurate answers to their questions directly from any Service Manager application screen. End users can access the Knowledge Management module through the self-service interface to search for potential problem resolutions before contacting the service desk.

Knowledge can come from any Service Manager data source—Incidents, Known Errors and so on—or any external data source. Knowledge can also include Hot News.

However, the Knowledge Management module is more than just the technical components needed to store answers. Because knowledge articles are created via the Knowledge-Centered Support (KCS) process, users can be confident in the accuracy and "just-in-time" solution quality of the answers. The KCS process is an industry best practice for knowledge management for which Service Manager has received external certification.

Service Manager Knowledge Management is a fully integrated support-oriented knowledge management solution that supports KCS standards and guidelines. The Knowledge Management module provides a natural language search engine and rich-text authoring tools that enable users to search, update, and author knowledge articles. Knowledge Management integrates with Interaction, Incident, and Problem management modules so that users can search and use knowledge from existing incidents or problems while attempting to resolve a new incident or problem. Users can also use this integration with Interactions, Incidents, and Problems to create new knowledge. The rich-text editor allows users to include various types of images and documents as attachments that can be linked to other documents or included as part of an existing document.

As part of HP's Closed Loop Incident Process (CLIP) solution, the integration between Service Manager Knowledge Management module and HP Operations Orchestration (OO) allows automatic execution of run-books related to change management tasks in the context of Service Manager Knowledge Documents. This allows for better and higher levels of automation.

For example, a Service Desk user diagnoses an Incident (or an end user who does self-help diagnosis) and searches for a Knowledge Management document with matching symptoms to the issue. When the user finds such a document, the user can execute a script from a link on the Knowledge Management page itself. The Knowledge Management link triggers a web service action that tells the OO server to run a specific pre-defined script on a specific server. The OO server then sends appropriate commands to the specified server to execute the runbook commands. When the target server receives the runbook commands, the server executes operating system commands or database commands as pre-defined to accomplish the specified action. This action could be a workaround or a fix, applied to the environment selected by the Service Desk (or end) user.

Incident integration: Incident matching with Problem

Incident matching and association is a foundational function in HP Service Manager. When a user creates an Incident record, Service Manager prompts the user with a list of similar Incident and Problem records. Service Manager can automatically check for potentially similar records based on similar known errors, root causes, incident records, incident record duplicates on a device, or incident record duplicates on parents.

The user can then determine if the new Incident record is identical or similar to an existing Incident record (and can then link the records), or can be resolved based on the workaround information in an existing Problem record.

Incident integration: Request Fulfillment

Out-of-box, the HP Service Manager Incident Management module is fully integrated with the Request Fulfillment module. Users can open Request records from Incident records, and Service Manager can pass relevant information from the Incident record to the Request record. The two records will be linked automatically.

Service Manager also includes a web-based, self-service interface that allows end users to create service requests through an easy-to-complete form. Once the form is complete, Service Manager routes the request through the Service Desk module to the appropriate Service Desk technician, who can then escalate the request to an Incident record. Users can track, update, or close their requests through this interface.

Incident integration: Service Level Management

Service Level Agreements (SLA), Operational Level Agreements (OLA), and Underpinning Contracts (UC) are created in the HP Service Manager Service Level Management module. Each SLA has multiple Service Level Targets (SLT), which can define required response or resolution timeframes associated with Incident records, or required uptime for CIs or services. When an Incident record is created, Service Manager applies the applicable SLA (based on the business unit for which the Incident is created, the CI that is the subject of the record, or other parameters) and populates response and resolution time SLT, as well as availability SLTs, in the Incident record.

This information can be used to prioritize record resolution, and Service Manager displays upcoming SLT deadlines, escalations, and alerts in the Incident record.

Incident Management user roles

There are specific roles associated with Incident Management. Service Manager uses role-based permissions to enable you to complete a task that is appropriate to your role. System Administrators manage and assign these permissions.

The Incident Management module has the following user roles:

Role	Responsibilities
Operator	• Register incident based on an event and assign to the correct support group.
Incident Analyst	• Review and accept or reject assigned incidents. • Investigate and diagnose the incident. • Document incident resolution or workaround in the Service Management application. • Implement incident resolution. • Verify that the incident is resolved and close the incident.
Incident Coordinator	• Review and accept or reject incidents assigned to the support group. • Handle incidents escalated by an Incident Analyst of the support group. • Monitor Operational Level Agreements (OLA) and Underpinning Contracts (UC) targets of the support group.
Incident Manager	• Handle incidents escalated by the Incident Coordinator or by the Service Desk Agent. • Determine and execute the appropriate escalation actions. • Request an Emergency Change if required.
Service Desk Agent	• Open interactions based on contact with the user • Match user interaction to incidents, problems, known errors, or knowledge documents • Solve and close interactions • Provide status updates to users on request • Register incidents based on user interactions and assign them to the

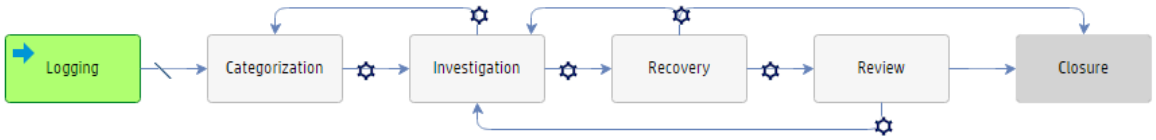
Role	Responsibilities
	correct support group • Register requests for change, based on user interactions • Register service requests, based on a user interactions • Validate solutions provided by support groups • Report and verify solution to users • Monitor the Service Level Agreement (SLA) targets of all registered incidents and escalate the incidents if required • Communicate service outages to all users
Service Desk Manager	• Handle incidents that are categorized as Complaints.

Incident Management workflows and user tasks

Incident Management enables you to categorize and track various types of incidents (such as service unavailability or performance issues and hardware or software failures), and ensures that incidents are resolved within agreed-on service level targets.

The incident workflow is a sequence of connected steps in the life cycle of an incident. In the workflow, an incident goes through several phases to complete the life cycle.

Incident Management workflow and its phases

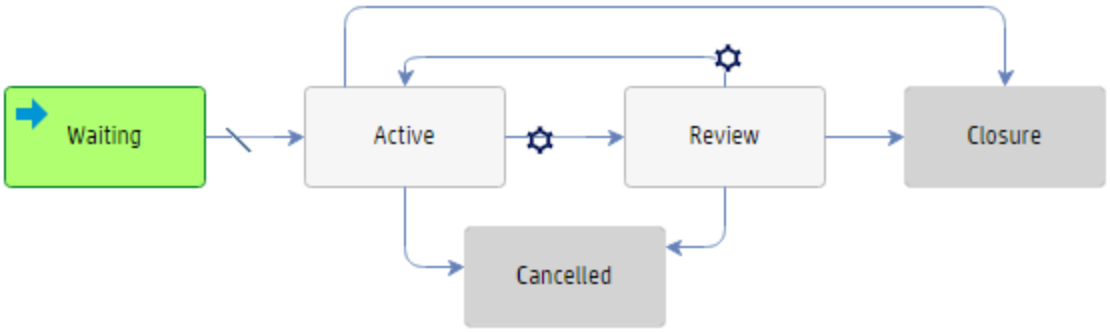


The following tasks are associated with the Incident Management workflow:

Workflow Phase	User Tasks
Logging	• "Create a new incident from a user interaction" on page 32 • "Create New Incidents from Monitoring System Notifications" on page 34 • "Review and Update Incident Information" on page 35 • Open an incident
Categorization	• "Reassign an Incident" on page 37 • "Assign an Incident" on page 36
Investigation	• "Change Incident Status to Pending User Information" on page 38 • "Change Incident Status to Pending Vendor/Supplier Investigation" on page 39 • "Document an Existing Solution or Workaround in an Incident" on page 40 • Handle User Requests for Information • Escalate an incident

Workflow Phase	User Tasks
	• Reassign an incident for additional support
Recovery	• "Test the Incident Resolution" on page 40 • "Change Incident Resolution" on page 41 • "Reassign Incident Resolution" on page 42
Review	• Reject an Incident Resolution • Reject an Incident Resolution with an Associated Change or Service Request • Close an Incident • Close an Incident with an Associated Interaction or Event • Handle complaints
Closure	None

Incident task workflow



Workflow phases can consist of one or multiple tasks to be completed to proceed to the next phase. You can use Incident Management tasks to categorize, investigate, resolve, or review an incident.

The following tasks are associated with incident tasks:

Incident Task Phase	User Tasks
Waiting	Create an incident task
Active	None
Review	• Cancel an opened task for an incident record

Incident Task Phase	User Tasks
	• Close an opened task for an incident record
Closure	None
Cancelled	None

Note: Incident Task can be created by clicking the **Link New Task** button at any Incident phases except the Logging and Closure phases. All the tasks must be closed before Incident closure.

You need to perform some minimum steps to resolve an out-of- box incident. The following example demonstrates these steps:

Phase:	User Actions:	Options
Logging	1. Enter a title in the **Title** field. 2. Provide a description of the problem in the **Description** field. 3. Click the **Fill** button and then select an appropriate value to specify the **Primary Affected Service** field. 4. If necessary, set the **Impact** and **Urgency** fields. 5. Click **Save**. 6. If you want to link an existing incident record, select the incident in the solution candidates and then click **Link Selected Record**. Otherwise, click **Continue** to create a new incident.	• This is the phase that is initiated when an end user Opens a New Problem (**Incident Management > Create New Incident**)
Categorization	1. Click the **Fill** button to specify the **Subcategory**. a. Select an appropriate subcategory. b. Select an appropriate area. 2. Click the **Fill** button for the **Assignment Group**, and then select an appropriate assignment group. 3. Click the **Fill** button for the **Assignee**, and then select an appropriate assign person. 4. Set the Status field to **Work In Progress**. 5. Click **Save**.	

Phase:	User Actions:	Options
Investigation	1. Enter the **Solution** field in the **Proposed Solution** tab. 2. Click **Save**.	From the Investigation Phase, you can also move to any of the following: • Return to the Categorization Phase.
Recovery	1. Set the Status field to **Resolved**. 2. Click **Save**.	From the Recovery Phase, you can also move to any of the following: • Return to the Investigation Phase. • Jump directly to the Closure Phase.
Review	1. Review the data entered for the Incident.	From the Review Phase, you can also move to any of the following: • Return to the Investigation Phase.
Closure	1. Click **Close** Button. 2. Select the appropriate **Closure Code**. 3. Click **Finish**.	

Access Incident Management reports

Applies to User Roles:

Incident Manager

Incident Coordinator

The Reporting tool in HP Service Manager provides a number of out-of-box reports on the incident data in your system. You can view these reports through a dashboard named Incident Overview (Global). You can also create your own dashboards to display other reports of your interest.

To access Incident Management reports, follow these steps:

1. Click **Change Management** > **Incident Overview**.

   By default, the **Incident Overview (Global)** dashboard is displayed.

2. View the reports on the dashboard. For descriptions of these reports, see "Report descriptions and usage" on page 1.

3. Add your own dashboards as needed. For details, see "Update a dashboard" on page 1.

   Your custom dashboards are added to the dashboard list on the toolbar of the dashboard page.

   Tip: You can click **Export** to export the reports on a dashboard to PDF format.

4. Click the **Open dashboard settings** icon on a dashboard to set its properties, or click the **Set as Default Dashboard** button to set it as your default one.

Create a new incident from a user interaction

Part of Workflow(s):
Incident Management: Logging
Applies to User Roles:
Service Desk Agent
You can create an incident from a user interaction. You can also update an incident from a user interaction that has already been triggered to an incident.

Create an incident from a user interaction

To create an incident from a user interaction, follow these steps:

1. Click **Service Desk** > **Create Streamlined Interaction**. The New Interaction form is displayed.

2. Specify the **Contact** for the interaction.

3. In the **Service Recipient** field, select the service recipient.

4. In the **Notify By** field, select the user's preferred notification method.

5. Type a description for the interaction.
6. In the **Category** field, select the **incident** or **request for information** category.
7. (Optional) In the **Subcategory** and **Area** fields, select the subcategory and area for the interaction.
8. In the **Affected Service** field, select the affected service.
9. Click the **Continue** button. The New Incident form is displayed, with fields populated with the values from the interaction.
10. Proceed with opening a new incident by updating fields such as **Primary Affected Service**, and then click **Save**.
11. Search possible solutions in the form that appears. If matching solutions are found, select the corresponding record, and then click **Link Selected Record**.

    Note: You can also perform this step after an incident is created. To do this, open the incident and then select **Solution Matching** from the **More** menu in the Detail List toolbar.

12. Complete the incident form with any other relevant information.
13. Click **Save & Exit**.

Update the new incident

To update the incident from the related user interaction, follow these steps:

1. Click **Service Desk** > **Interaction Queue**. Service Manager opens the Interaction queue.
2. Click the interaction in the queue to display the details of the record.

   Those items with a status of **Dispatched** are user interactions that have been triggered to Incident Management (or another module).

3. On the record details page, click the **Related Records** tab, and then click the related incident that you want to update.
4. Proceed with updating the incident. After closing the incident form, you are returned to the user interaction list.

Create New Incidents from Monitoring System Notifications

Part of Workflow(s):
Incident Management: Logging
Applies to User Roles:
Operator
You can create an incident when notified by a monitoring system of an event in the Information and Communication Technology (ICT) infrastructure.

To create an incident from a monitoring system event notification:

1. Click **Incident Management** > **Create New Incident**.
2. Select the incident category.

   Note: If a default category is specified in the Incident Settings, HP Service Manager directly assigns the incident to the default category and skips this step. For more information, see "Configure Incident Management settings" on page 68.
3. Click **Apply Template**.
4. Select the appropriate template. The template automatically fills in some fields with predefined values.
5. Type a title and description for the incident.
6. In Incident Detail, verify or complete the following required entries. Use the Fill button when available to display a list of values for the field.
   - **Category**
   - **Subcategory**
   - **Area**
   - **Impact**
   - **Urgency**

7. Click **Fill** to select an Assignment Group.
8. Click **Fill** or **Find** to select the applicable Service affected by the incident.
9. Complete the form with any other relevant information.
10. Click **Save & Exit**.

Incident Management opens a new incident, assigns a unique number with the prefix IM, and places the incident in the queue for the Incident Coordinator.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Review and Update Incident Information

Part of Workflow(s):
Incident Management: Logging
Applies to User Roles:
Service Desk Agent
To update incident information:

1. Click **Incident Management > Incident Queue**.
2. Use search or advanced search to find one or more records.
3. Double-click the target record.
4. Review the information in the record to verify that it is complete and correct.
5. For incident records that are complete:
   a. Click **Fill** to select the applicable Assignment Group for the incident.
   b. Follow the procedures defined by your company to provide the interaction number and the SLA target to the customer.

- To see a list of the related interactions,open the **Related Records** section.
- To see information about the SLA, Open the **SLT** section.

6. For incident records that are incomplete or incorrect, gather the required information and update the form. The required information includes:
   - The title and description of the incident
   - The service provided by the affected item (for example, email)
   - The Incident details: Category, Area, Subarea, Impact, Urgency, Priority
7. Click **Fill** to select the applicable Assignment Group for the incident, if it is not already assigned to a group.
8. Use internally-defined procedures to provide the interaction number and the SLA target to the customer. The incident is now assigned to the assignment group you selected.
9. Click **Save & Exit** to return the incident queue.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Assign an Incident

Part of Workflow(s):
Incident Management: Categorization
Applies to User Roles:
Incident Coordinator
The Incident Coordinator reviews open status incidents and assigns the record to an Incident Analyst for further investigation and diagnosis.

Assigning an incident is a two-step process. First, review an incident to determine if it can be resolved by your group. Next, assign the incident to an Incident Analyst.

To review and assign an incident:

1. Click **Incident Management** > **Incident Queue**.
2. Select the **Incidents by Assignment Group** view.
3. Review the incident records in the list to determine which ones can be assigned to your group for further investigation.
   a. Review each incident record and look at the contents of the Affected CI and Description fields.
   b. Determine to whom an incident record can be assigned.
4. Open the **Categorization and Assignment** section.
5. Click **Fill** to select an assignment group from the Assignment Group field and then click **Fill** to select an assignee from the Assignee field.
6. Click **Save & Exit**.

Reassign an Incident

Part of Workflow(s):
Incident Management: Categorization
Applies to User Roles:
Incident Analyst
Incident Coordinator
At times you will need to reassign incident records when an Incident Analyst is unavailable.

To reassign an incident:

1. Click **Incident Management** > **Incident Queue** > **By Assignment Group**.
2. Select a list of Incident Analyst assignments for a particular analyst.
   a. Click the list in the **View Records for which Assignment Group?** field, and then select an assignment group.
   b. Click **OK**.
3. To complete the reassignment of an incident:
   a. Select the incident record to be reassigned.
   b. Clear the assignee in the **Assignee** field, and then click **Fill** to select an operator from the list

of names to reassign the incident to that person.

c. Click **Save & Exit**.

Change Incident Status to Pending User Information

Part of Workflow(s):
Incident Management: Investigation
Applies to User Roles:
Incident Analyst
If you need additional information from the user, contact the user directly. While waiting for information from the user, change the incident status to pending user information status.

> **Note:** You can configure the **Suspend processing for these states** option in the corresponding Service Level Target (SLT) of the Incident so that the SLT stops time interval tracking for a pending incident. Otherwise, the SLT continues to track the incident as an open incident.
>
> In a pending status, the assignment group remains the same.

1. Click **Incident Management** > **Incident Queue**.
2. Select the **Open incidents assigned to my group** view, which is sorted on the service level agreement (SLA) target date. The view is sorted by target date with the oldest date listed first.
3. Select an open incident, and then look at the category in the Category field. The category is inherited from the Service Desk interaction process. Valid entries are complaint, incident, or request for information. The Area and Subarea fields are also populated according to the selected category.
4. Click the list in the **Status** field and change the status to an applicable pending status.
5. When the user delivers the requested information, change the status to accepted or work in progress. Click the list in the **Status** field and update the status.
6. Click **Save & Exit**.

Change Incident Status to Pending Vendor/Supplier Investigation

When you determine that a vendor needs to investigate and diagnose the cause of an incident, you are required to update the status of the incident record to indicate that the investigation is pending vendor feedback.

Part of Workflow(s):
Incident Management: Investigation

Applies to User Roles:
Incident Analyst
To update an incident record status to pending vendor information:

1. Click **Incident Management** > **Incident Queue**.
2. Select the **Open incidents assigned to my group** view, which is based on the service level agreement (SLA) target date. The view is sorted by target date with the oldest date listed first.
3. Select an open incident, and then look at the category in the Category field. The category is inherited from the Service Desk interaction process. Valid entries are complaint, incident, or request for information. The Area and Subarea fields are also populated according to the selected category.
4. Click the list in the **Status** field and change the status to **Pending Vendor/Supplier**.
   - **Note**: When an incident record is at a status of pending vendor, the service level agreement clock continues to track the incident as an open incident. The assignment group remains the same.
5. Open the **Activities** section.
6. Click **Fill** in the Vendor/Supplier field to generate a list of vendors/suppliers and choose one.
   - **Note**: The Vendor/Supplier field is only valid when the incident Status is Pending Vendor/Supplier.
7. Enter the reference number (obtained from the vendor/supplier) in the **Vendor/Supplier Record** field.
   - **Note**: When the vendor/supplier provides the requested information, you can change the status to work in progress.
8. Click **Save & Exit**.

Document an Existing Solution or Workaround in an Incident

Part of Workflow(s):
Incident Management: Investigation

Applies to User Roles:
Incident Analyst
When you find an existing solution that resolves an open incident, you can verify the effectiveness of the solution and then use the solution to resolve the incident.

After you verify that the solution works, perform the following steps to attach the solution to the incident record:

1. From the knowledgebase document or record that contains the solution, do the following:
   a. Click **Use Solution** to add the solution to the Solution field of the incident record..

   b. View the published document, and then select it as a solution. The system reopens the record with the Solution field updated.

      Note: For information about attaching a file, see the related topics.

2. Update the incident detail:
   a. Open the Activities section.

   b. Select the applicable update type in **New Update Type**.

   c. Add other necessary information and notes in **New Update**.

   d. Check **Visible to Customer** to make the information available to customers.

3. Click **Save & Exit**.

Test the Incident Resolution

Part of Workflow(s):
Incident Management: Recovery

Applies to User Roles:
Incident Analyst

One of the tasks of the Incident Analyst is to review and test the resolution described in the Solution field of an incident record. When the test is successful, the incident is assigned for incident closure. When the resolution test fails, the Incident Analyst returns the incident to incident investigation and resolution or assigns it to incident escalation.

To update tested incident resolutions:

1. Click **Incident Management > Incident Queue** or view your To Do Llst.
2. View and identify any incidents whose resolution (Solution field) can be tested.
3. Test the resolution described in a test environment that mimics the production environment.
4. When the resolution fails:
   a. If the incident requires an escalation, update the **Assignment Group** and **Assignee** fields with the Incident Coordinator responsible for the Incident Escalation process.
   b. If the incident does not require an escalation, update the **Assignment Group** and **Assignee** fields with the applicable Incident Analyst responsible for the investigation and diagnosis process or incident escalation.
   c. In both cases, in the Activities section, select a **New Update Type** and then in **New Update** type an explanation of the test failure.
5. When resolution testing is successful:
   a. Update the **Assignment Group** and **Assignee** fields with the applicable Incident Analyst responsible for the incident closure process.
   b. In the Activities section, select the **New Update Type** and then in **New Update** type a description of the test results.
6. Click **Save & Exit**.

Change Incident Resolution

Part of Workflow(s):
Incident Management: Recovery

Applies to User Roles:
Incident Analyst
One of the tasks of the Incident Analyst is to review and identify incidents received from the incident investigation and diagnosis process that need to be escalated to the Incident Coordinator because the implementation of the resolution requires a change.

To initiate a change for an incident:

1. Click **Incident Management > Incident Queue** or view your To Do list.
2. View and identify any incidents whose resolution (shown in the Solution field) can only be accomplished with a change.
3. Update the **Assignment Group** and **Assignee** fields with the applicable group and Incident Coordinator.
4. In the Activities section, select the **New Update Type** and then in **New Update** type a description of the change required to implement the resolution.
5. Click **Save & Exit**.

Reassign Incident Resolution

Part of Workflow(s):
Incident Management: Recovery

Applies to User Roles:
Incident Analyst
One of the tasks of the Incident Analyst is to review and identify incidents received from the incident investigation and diagnosis process that need to be reassigned to another group, because the Incident Analyst does not have the necessary permissions to implement the resolution.

To reassign an incident:

1. Click **Incident Management > Incident Queue** or view your To Do list.
2. View and identify any incidents with a resolution (shown in the Solution field) that cannot be accomplished because you do not have the applicable permissions.
3. Update the **Assignment Group** and **Assignee** fields with the applicable group and operator.
4. In the **Activities** section, do the following:
   a. From the **New Update Type** field list, select an update date.
   b. In the **New Update** field, type a description of the permissions required to implement the resolution.
5. Click **Save & Exit**.

Reject an Incident Resolution

Part of Workflow(s):
Incident Management: Review

Applies to User Roles:
Incident Analyst
If the solution assigned to an incident is found to not resolve the incident completely, the incident must be returned to the incident investigation and diagnosis process for additional analysis. For example, a solution may appear to solve the problem, but when the customer uses the solution, the problem persists. Incidents that have associated service requests or changes require additional processing.

To reassign an incident for additional investigation and diagnosis:

1. Click **Incident Management > Incident Queue** or view your To Do queue.
2. Select an incident for review.
3. Review the incident resolution description in the Solution field to verify that it is correct and complete. Verify that all information in the detail record is complete.
4. When the solution does not resolve the incident and the incident does not include an associated service request or change:
   a. Update the **Status** field to Work In Progress.
   b. Update the **Assignment Group** and **Assignee** fields with the applicable group and Incident Analyst.
   c. In the Activities section, do the following:
      i. From the **New Update type** field list, select an update type.
      ii. In the **New Update** field, type an explanation that describes the problem with the proposed solution.
   d. Click **Save & Exit** to return to your To Do queue.
5. If the incident includes an associated service request or change, the incident requires additional processing.

Reject an Incident Resolution with an Associated Change or Service Request

Part of Workflow(s):
Incident Management: Review

Applies to User Roles:
Incident Analyst
If the solution provided for an incident is found to not resolve the incident completely, then the Incident Analyst must review the incident for necessary changes or requests. When incident closure rejects the incident solution and the incident has an associated change, incident closure updates the status of the incident to pending change and requests that Change Management reopen the change. When incident closure rejects the incident solution and the incident has an associated service request, incident closure updates the status of the incident to pending change and requests that the Service Desk reopen the request.

To reassign a rejected incident solution with an associated change or service request:

1. Click **Incident Management > Incident Queue** or view your To Do queue.
2. Select an incident for review.
3. Review the incident resolution description in the Solution field to verify that it is correct and complete.
4. When the solution does not resolve the incident and the incident includes an associated service request:
   - Update the **Status** field to Pending Change.
   - Update the **Assignment Group** and **Assignee** fields with the applicable Service Desk group and Service Desk Agent.
   - In the **Activities** section, do the following:
     - From the **New Update Type** field list, select an update type.
     - In the **New Update** field, type an explanation that describes the problem with the proposed solution and that also mentions any associated requests that must be reopened.
   - Click **Save & Exit** to return to your To Do queue.

5. When the solution does not resolve the incident, and the incident includes an associated change:
   - Update the **Status** field to Pending Change.
   - Update the **Assignment Group** and **Assignee** fields with the applicable Change Management group and Change Coordinator.
   - In the **Activities** section, do the following:
     - From the **New Update Type** field list, select an update type.
     - In the **New Update** field, type an explanation that describes the problem with the proposed solution and that also mentions any associated changes that must be reopened.
   - Click **Save & Exit** to return to your To Do queue.

Escalate an Incident

Part of Workflow(s):
Incident Management: Investigation

Applies to User Roles:
Incident Coordinator
If the Incident Coordinator determines that the incident can be solved by escalating an incident, the Incident Coordinator proceeds as follows:

1. Click **Incident Management** > **Incident Queue** or view your **To Do** queue.
2. Click the open incident record.
3. Click the **Related Records** tab.
4. Select an appropriate link type from the **Link Type** drop-down list box.
5. Click **Link New Record**.
6. Select an appropriate category on the page that appears.
7. Follow the instructions to continue creating a new record.

Reassign an Incident for Additional Support

Part of Workflow(s):
Incident Management: Investigation

Applies to User Roles:
Incident Manager
After an Incident Manager is notified that an incident is not going to be resolved on time and that the service level agreement (SLA) is breached or in danger of being breached, the Incident Manager reassigns the incident for additional support.

The Incident Manager reviews the SLA target times and determines that the incident requires reassignment to another level of support. The Incident Manager reassigns the incident to another support group.

To reassign an incident for additional supports:

1. Click **Incident Management** > **Incident Queue** or view your **To Do** list.
2. Click the open incident.
3. Clear the assignment group in the **Assignment Group** field, and then click **Fill** to select the new assignment group.
4. Click **Save & Exit**.

   Note: You can contact the Service Desk to request that the Service Desk send an information bulletin to affected users and stakeholders.

Monitor Interaction Queue for Service Level Agreement Breaches

Part of Workflow(s):
Service Level Agreement Monitoring

Applies to User Roles:
Service Desk Agent
The Service Desk Agent monitors the interaction queues for interactions with associated incidents that have not been resolved in the time specified by the Service Level Agreement (SLA). When this occurs, the Service Desk Agent begins the escalation procedure for the incident by assigning the incident to the applicable Incident Manager and assignment group based on the services affected by the incident.

To reassign breached incidents for additional analysis and diagnosis:

1. Click **Service Desk > Interaction Queue** or view your To Do queue.
2. In the View list, select Monitor SLA Interaction - Breached.

3. From the list, select an interaction record with a linked incident (Open - Linked) record.
4. To view the related incident, click **More** or the More Actions icon and select **Related > Incidents > View**.
5. Double-click the **Incident ID**.
6. Update the **Assignment Group** and **Assignee** fields based on the information in the Service and Affected CI fields.
7. In the Activities section, do the following:
   a. In the **New Update Type** field list, select an update type.
   b. In the **New Update** field. type an explanation to describe the reason for the escalation and any relevant details.
8. Click **Save & Exit** to return to the Interaction queue.

Monitor Interaction Queue for Potential Service Level Agreement Breaches

Part of Workflow(s):

Service Level Agreement Monitoring

Applies to User Roles:

Service Desk Agent

The Service Desk Agent monitors the interaction queues for interactions with associated incidents that are within a few hours of breaching as specified by the Service Level Agreement (SLA) for the type of incident. For those items that are within one hour of breaching, the Service Desk Agent coordinates with the Incident Coordinator who escalates the incident associated with the escalation and communicate the expected resolution to the applicable users and user groups. For those items that are within four hours or one day of breaching, the Service Desk Agent monitors the applicable queues until the interactions are resolved or escalated.

To monitor the interaction queues for potential breached interactions:

1. Click **Service Desk > Interaction Queue** or view your To Do queue.
2. In the View list, select the **Monitor SLA Interaction - Breach within 1 hour** queue.

3. To view the incident details for an interaction in the queue:
   a. View the related incident.

   b. Click **More** or the More Actions icon and select **Related > Incidents > View**.

   c. Double-click the **Incident ID**.

4. Contact the Incident Coordinator assigned to the related incident, and either begin the Incident Escalation process or contact the affected users and groups with the expected resolution details.

5. For any interactions in the other Monitor SLA Interaction queues, continue to monitor the queues until the items are resolved or require escalation.

Handle Complaints

Part of Workflow(s):
Complaint Handling

Applies to User Roles:
Service Desk Manager

The Service Desk Agent assigns an incident containing a user complaint to the Service Desk Group. When the incident is saved, it is automatically assigned to the Service Desk Manager. The Service Desk Manager reviews and accepts the incident to research and resolve the complaint.

To manage an incident based on a user complaint:

1. Click **Incident Management** > **Incident Queue** or view your **To Do** queue.

2. Click the open incident record and review the contents of the User complaint.
   Note: Investigate the complaint by reviewing the relevant information and talking to the people involved.

3. When you have finished searching for an answer or solution to satisfy the user, select the Activities section to add appropriate notes.

4. Enter the resolution in the **Solution** field and verify that the information is correct and complete.

5. Select **Resolved** from the Status field.

6. Click **Close** to close the incident.

7. Select an appropriate code from the **Close Code** field in the form that appears.
8. Click **Finish**. The status changes to Closed.

Open an incident

Applies to User Roles:
Configuration Auditor
Incident Coordinator
Incident Manager
You can open incident records as part of many Service Management processes, including interaction management, event management, configuration verification and audit, and incident management.

Note: For information on opening or creating incident records in the interaction management process and event management process, see the related topics.

To open an incident record:

1. Click **Incident Management** > **Create New Incident**.
2. Select the incident category.

   Note: If a default category is specified in the Incident Settings, HP Service Manager directly assigns the incident to the default category and skips this step. For more information, see "Configure Incident Management settings" on page 68.
3. Type an appropriate title in the **Title** field and then give appropriate description in the **Description** field.
4. Click **Fill** to select an Assignment Group.
5. Click **Fill** to select the applicable **Affected Service**.
6. Click **Fill** to select the **Affected CI**.

   Note: The **Default Impact** and **Priority** values of the affected CI are automatically populated to the **Impact** and **Urgency** fields of the incident record. You can manually change these auto-populated values if needed.

7. Click **Save**.
8. Search possible solutions in the form that appears. If matching solutions are found, select the corresponding record, and then click **Link Selected Record**.

   Note: You can also perform this step after an incident is created. To do this, open the incident and then select **Solution Matching** from the **More** menu in the Detail List toolbar.

9. Complete the incident form with any other relevant information.
10. Click **Save & Exit**.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

View a list of services potentially affected by an outage

Applies to User Roles:
Incident Coordinator
Incident Manager
The View Affected Services menu option enables you to view a list of services that are potentially affected by an outage relating to CIs that are specified in an incident or change record. By viewing the affected services list, you can determine the potential impact of an outage related to critical, dependent services when you open an incident. You can also use the affected services list to plan when opening a change.

Note: The list of CIs generated does not include the CIs specified in the primary incident or change record.

To view a list of affected services:

1. Perform one of the following actions.
   - Open an existing incident or change record. Use search or advanced search to find one or more records.
   - Proceed as if you are going to add a new incident or change record.
2. If you are in the process of adding a new record, fill in the **Affected CI**.
3. Click **More** or the More actions icon and select **View Affected Services**. The CI Identifier record opens.
4. Open the **Affected Services** section. A list of affected services opens or a message, stating that there are no services affected by the outage.

   Note: For change records, a list of all affected business services is returned in all cases, whether the record has one primary CI or multiple CIs.
5. Select a CI from the list for detailed information from the Configuration Management record.
6. When you finish viewing the affected services, click **Cancel**.

Apply a template to complete an incident

Applies to User Roles:
Incident Analyst
Incident Coordinator
Incident Manager
Templates enable users to quickly complete an incident record by automatically populating fields with the applicable information.

Note: Make sure that the user profile is enabled to use templates. For additional information on enabling a profile to use templates, see the related topics.

To apply a template to complete an incident:

1. Click **Incident Management** > **Incident Queue** or view your **To Do** queue.
2. Select an incident record.
3. Click **Apply Template**. The Select Incident Template wizard opens.

4. Double-click the template that you want to apply to the selected incident. You are returned to the selected incident record and the fields are automatically filled in with the values set in the template.
5. Modify other fields, as needed.
6. Click **Save & Exit**.
   Note: Users authorized to use this template can also modify the template to meet their needs.

Access Incident Management views

Applies to User Roles:
Incident Analyst
Incident Coordinator
Incident Manager
Incident Management views contained in the Favorites and Dashboards navigation pane enable you to easily and quickly access specific types of records. When the database changes, the dashboard contents change to reflect current activity.

To view your favorites, click **Favorites and Dashboards** > **Incident Management**. HP Service Manager provides the following default Incident Management views:

- (1) Monitor OLA-UC Incident - Breached
- (2) Monitor OLA-UC Incident - Breach within 1 hour
- (3) Monitor OLA-UC Incident - Breach within 4 hours
- (4) Monitor OLA-UC Incident - Breach within 1 day
- All Open Incidents
- Incidents by Assignment Group
- Open Incidents Assigned to Me
- Open Incidents I Own

Note: The Monitor OLA-UC breached views contain incident records that measure the performance of individual support groups and applicable vendors. The records that are close to breaching an agreement or that already have breached an agreement can be seen in these views.

Relate a record to an incident record

Applies to User Roles:
Incident Analyst
Incident Coordinator
Incident Manager
As part of incident processing, you can relate or associate an existing incident, change, request, or problem to an incident. Use related records to associate an incident with any applicable incidents, changes, requests, or problems so that status changes or updates that you make will also be made to associated records.

To relate a record to an incident record:

1. Click **Incident Management** > **Incident Queue** or view your To Do queue.
2. Select a target record.
3. Click the **Related Records** tab.
4. Select an appropriate type from the **Link Type** drop-down list box.
5. Click **Link Existing Record**.
6. When the Associating Records form opens, type the ID of the record.

   You can also use **Search** in the Associating Records dialog box to locate the applicable ID number.
7. Click **OK**.

Update an incident

Applies to User Roles:

Incident Analyst

Incident Coordinator

Incident Manager

Sometimes you need to update an existing incident record for reasons, such as reassigning the incident to another group or changing the priority of the incident record. When you update the incident record, you can also include helpful information in the Update field of the Activities section.

To update an incident:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Select a record to display it.
4. Make any necessary changes. For example, if you want to reassign the incident record to another group:
   - Clear the assignment group in the **Assignment Group** field, and then click **Fill**. A list of assignment groups is displayed.
   - Select the new assignment group from the list.
5. Open the Activities section to do the following:
   - Add notes in the **Update** field with the reason why the incident has been updated or to add other helpful information.
   - If necessary, click the **New Update Type** list to categorize the activity update.
6. When you are finished with your updates, click **Save & Exit**.

Note: When you view an existing incident, shaded fields are read-only fields. Incident Management populates these fields from information stored in associated records. You can update the associated record to increase the amount of information in this incident record.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Resolve an incident

Applies to User Roles:
Incident Analyst
Incident Coordinator
Incident Manager

When you find an existing solution that resolves an incident, you can attach the solution to the incident record and close the record. You can also save the resolution as a candidate for the knowledgebase.

To resolve an incident:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Double-click a record to display it in the Incident form.
4. Click the **Activities** tab and then do the following:
    a. In the **Update Type** field list, select an update type.
    b. In the **Update** field, type a note to explain how you resolved the incident.
5. Click the **Proposed Solution** tab and then type the solution in the **Solution** field.

    If the incident is a potential problems candidate, select the **Problem Candidate** check box.
6. Select **Resolved** from the **Status** drop-down list box.
7. Click **Save**.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Close an Incident

Part of Workflow(s):

Incident Management: Review

Applies to User Roles:

Incident Analyst

Incidents that have been resolved satisfactorily and have no associated events, interactions, or changes are closed by specifying a closure code and updating the status to closed. Incidents that have associated events, interactions, or changes require additional processing.

To close an incident:

1. Click **Incident Management > Incident Queue** or view your To Do queue.
2. Select an incident that is ready to be closed.
3. Click **Close**. The Close Incident form is displayed.
4. Set the following fields:

   Subcategory and **Area**: You can change the **Subcategory** and **Area** fields, and the change will be saved to the incident when you click **Finish**.

   Closure Code: Select the code that best describes the closure.

   Problem Candidate: Select this check box if you want to mark this incident as a problem candidate.

   Completion Comments: Enter your comment for the closure.
5. Click **Finish**. The status changes to Closed.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Close a first-time resolved incident

Applies to User Roles:

Service Desk Agent, Incident Coordinator

When you create a new incident, you can close the incident directly if you are able to resolve the user request on the first intake in the Logging phase of the incident. If the incident is triggered from an interaction, the associated interaction record is closed automatically.

To close a first-time resolved incident, follow these steps:

1. Open the incident record that is in the Logging phase.
2. In the **Solution** filed, type a solution for the incident.
3. Click the **Resolve Directly** button on the toolbar.

   Service Manager displays the **Close Incident** page.
4. Specify information for the **Subcategory** and **Closure Code** fields.
5. Specify information for other optional fields such as **Completion Comments**.
6. Click **Finish**. The status of the incident changes to Closed.

Close an Incident with an Associated Interaction or Event

Part of Workflow(s):
Incident Management: Review

Applies to User Roles:
Incident Analyst
Incidents that are resolved satisfactorily that have associated events or interactions are closed by specifying a closure code and updating the status to closed. Incidents that have associated changes require additional processing.

To close an incident with an associated interaction or event:

1. Click **Incident Management > Incident Queue** or view your To Do queue.
2. Select an incident that is ready to be closed.
3. Review the incident resolution description in the Solution field to verify that it is correct. Make sure that all information in the detail record is complete.
4. If this incident has an associated interaction, update the **Assignment Group** and **Assignee** fields with the Service Desk group and Service Desk Agent responsible for the Close Interaction process.
5. If this incident has an associated event, update the **Assignment Group** and **Assignee** fields with the Group and Operator responsible for Event Management.
6. Click **Close**. The Close Incident form is displayed.

7. Use Fill to select an applicable code for the **Closure Code** field.
8. Enter your comments in the **Completion Comments** field.
9. Click **Finish**. The status changes to Closed.

Add an attachment to an incident record

To add an attachment to a record, follow the steps below:

1. Open the record to which you want to add an attachment. To do this, select a record from the queue or search for a specific record.

   Note: You can also add an attachment when you create a new record.

2. Scroll down to and click the **Attachments** tab.
3. Click **Add files**, and then browse to the file or files that you want to attach to the record.

   After you confirm your selection, a progress bar in the **File Name** column displays the progress of the file upload process.

   Note: The multiple file upload and progress bar functionality is only available in browsers that support the HTML5 File API (for example, Mozilla Firefox, Google Chrome, or Windows Internet Explorer 10).

   The file is now uploaded. However, the file is not attached to the record until you click **Save**. To remove a file that is uploaded in error, click the **X** icon in the **Remove** column before you click **Save**.

   Note:

   - The size limit for individual attachments and the space that is available for storing attachments are displayed in the upper-right corner of the **Attachments** section.
   - If you try to attach a file that exceeds the size limit for individual attachments or the total available space, you receive an error message, and the attachment is not uploaded.

- If you try to attach a type of file that is not permitted (for example, an .exe file), you receive a message that prompts you to remove the attachment. If you do not remove the attachment, it is removed automatically when you click **Save**.
- There is no limit to the number of files that you can attach to a record, provided that they do not exceed the size limit. However, we recommend that you do not attach more than 20 files to a single record.
- If you refresh the browser or click certain comfill buttons that refresh the browser before the file upload process is complete, the file is not uploaded.
- Whether you can attach a file with a duplicated name against the attachment list depends on the setting of the **preventDuplicatedAttachmentName** parameter.

4. Click **Save**.

Open an attachment in an incident record

To open a file that is attached to a record, follow these steps:

1. Open the record to which the file that you want to open is attached. To do this, select a record from the queue or search for a specific record.
2. Scroll down to and click the **Attachments** tab.
3. To open a single file, click the file name or the download icon in the **Download** column.

   To open multiple files, select the files that you want to open by using the check-boxes next to the file names, and then click **Download**.

   Note: When you download multiple attachments concurrently, HP Service Manager packages the files in a compressed (zipped) folder. Some third-party unzipping tools may not correctly handle file names that contain non-Roman characters. In this situation, the name of the unzipped file may change unexpectedly. We recommend that you use WinRAR to unzip the compressed folder.

4. Click **Save**.

View the details of an attachment in an incident record

To view the details of the files that are attached to a record, scroll down to and expand the **Attachments** section of the appropriate record.

> **Note:** The number of attached files is displayed on the **Attachments** tab heading. This enables you to identify whether a record has attachments quickly without having to expand the **Attachments** section.
>
> However, the number of attached files is not displayed if a custom dynamic view dependency is configured for the section or tab title. This is because the custom dynamic view dependency may include file count information.

If a file is attached to the record, the following information is displayed in the table in "Attachments" section:

- The name of the attached file
- The size of the attached file (in KB)
- The login name of the person who attached the file
- The date when the file was attached to the record

Attached files are displayed in the order in which they were uploaded.

Delete an attachment from an incident record

Applies to User Roles:
Incident Coordinator
Incident Manager
To delete an attachment from a record, follow these steps:

1. Open the record from which you want to delete an attachment. To do this, select a record from the queue or search for a specific record.
2. Scroll down to and click the **Attachments** tab.
3. To delete a single file, click the **X** icon in the **Remove** column.

To delete multiple files, select the files that you want to delete by using the check-boxes next to the file names, and then click **Remove**.

4. In the dialog box that appears, confirm the deletion.
5. Click **Save**.

Create an incident task

Applies to User Roles:

Incident Coordinator

After an incident is created, you can create the tasks for categorizing, investigating, resolving, and reviewing the incident.

To create an incident task:

1. Select an incident that is not closed.
2. Click the **Link New Task** button in the **Tasks** tab of this incident.
3. Select a category for the new task.

   Service Manager opens a task information form.
4. Complete the form with all required information.
5. Click **Save** or **Save & Exit**.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

Cancel an opened task for an incident record

Applies to User Roles:

Incident Coordinator
Incident Manager
Incident Analyst

If an incident record has an opened task, you can cancel the open task by using the Cancel Task feature.

To cancel an opened task for an incident record:

1. Click **Incident Management** > **Search Incidents**, enter your search criteria, and then click **Search**.
2. Select an incident and then click the **Tasks** tab.

   A task list appears if this change contains opened tasks.
3. Double-click the task that you want to cancel.
4. Click **Cancel Task** from the **More** drop-down list.
5. Enter the Task Outcome and then click Finish.

The opened task is now cancelled:

- The status of the opened task is set to Cancelled.
- The automatic transition moves the workflow phase to Cancelled.
- The Completion Code is set to Cancelled.

Close an opened task for an incident record

Applies to User Roles:

Incident Coordinator
Incident Manager
Incident Analyst

If an incident record has opened tasks, you can close them by using the Close Task feature.

> **Note:** You cannot close a high priority (priority is High or Critical)
> incident task if this incident task is not in the Review phase.

To close an opened task for an incident record:

1. Click Incident **Management** > **Search Incidents**, enter your search criteria, and then click **Search**.
2. Select an incident and then select the **Tasks** tab.

   A task list appears if this change contains opened tasks.
3. Double-click the task that you want to close.
4. Provide necessary information for task completion.
5. Click **Close Task**.
6. Enter the Completion Code and Task Outcome, and then click **Finish**.

Note: You can add parts and labor costs tracking to an incident, problem, change, or request or to any associated task of a record. To do this, navigate to the **Cost** tab, specify the currency, and then specify the date, part number, and quantity for any parts used. Alternatively, specify the date, technician name (used to derive the rate from the operator record), and hours worked for any labor. Service Manager will automatically calculate and roll up costs from any sub tasks into the **Total cost** field on the **Costs** tab.

The opened task is now closed:

- The status of the opened task is set to Closed.
- The task is moved to the Closure phase.
- The Completion Code is set to the value you provided.

Create other types of record from an incident

You can create other types of record from an incident record, and the created record is automatically linked to the incident record.

To do this, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Open the incident from which you want to create another type of record.

4. In the **Related Records** section, select one of the following options from the **Link Type** drop-down list. These options defines the type of the new record and the relation between the new record and the incident.
   - Caused By Changes
   - Caused Changes
   - Caused By Incidents
   - Caused Incidents
   - Related Requests
   - Related Known Errors
   - Related Problems
5. Click **Link New Record**.
6. Follow the on-screen instructions to complete the creation of the new record.

After you create the new record, the new record is automatically linked with the incident.

Set a parent incident

Before you can create a parent-child relationship between incidents, you must set an incident as the parent incident.

To do this, follow these steps:

1. Open the incident record that you want to use as the parent incident.
2. In incident details, select the **Parent Incident** check box.
3. Click **Save**.

The **Child Incidents** section then appears under **Related Records**.

If you clear the **Parent incident** check box, the **Child Incidents** section then disappears. When you save the change, the parent incident ID is removed from the **Link to Parent Incident** field in all child incidents. That is, the parent-child relationships between these incidents are dismissed. In addition, if

the **Notify incident owner if Parent Incident flag was unchecked** option is selected in incident settings, a notification is sent to all assignees of the child incidents.

Set a child incident

Follow these steps to set and link a child incident to a parent incident:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Open the incident that you want to make as the child.
4. Specify the parent incident in the **Link to Parent Incident** field. To do this, you can use one of the following methods:

   Note: The incident that you specify in this field must be a parent incident. That is, the **Parent Incident** option of this incident is selected.

   - Enter the ID of the parent incident. By this method, you can specify any incident that is marked as a parent.
   - Click the **Fill Field Link to Parent Incident** button. A list of parent incident candidates then appears. Select a parent incident and then click **Link Selected Record**.

     By this method, you can only specify a parent incident that matches one of the following criteria, which you can use to filter existing parent incidents.

     - An incident with a matching title
     - An incident with a matching related service or configuration item
     - An incident with a matching service or configuration item
5. Set the **Subcategory**, **Area** and **Assignment Group** fields.
6. Click **Save**.

After you link a child incident to a parent incident, the child incident appears in the **Child Incidents** section in the parent incident.

Unlink a child incident

To unlink a child incident from the parent incident, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Open the parent incident.
4. In the **Child Incidents** section, select the child incident that you want to unlink, and then click **Unlink Selected Record**.

   Note: You can also select and unlink multiple child incidents, or simply click **Unlink All** to unlink all child incidents.

5. Click **Save**.

Mark an incident as a major incident

Applies to User Roles:

Incident Analyst

To mark an incident as a major incident, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Double-click a record to display it in the Incident form.
4. Select the **Major Incident** check box and then specify an incident manager.

   A new **Major Incident Review** section then appears in incident details.

5. Click **Save**.

The specified incident manager receives an email about the creation of the major incident.

Mark an incident for escalation

Applies to User Roles:

Incident Coordinator

To mark an incident for escalation, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Use search or advanced search to find one or more records.
3. Double-click a record to display it in the Incident form.
4. Select the **Escalated** check box and then specify an incident manager.
5. Specify an escalation team in the **Escalation Team** section.
6. Click **Save**.

The incident assignee and the incident manager then receive an email about the incident escalation.

Incident Management administrator tasks

You can access Incident Management administration from the Central Administration Utilities. A System Administrator can access the Operator record for the following information types and functions:

- User and contact information
- Application profile privileges
- Mandanten utility

Configure Incident Management settings

Applies to User Roles:

System Administrator

To configure Incident settings:

1. Click **Incident Management** > **Administration** > **Settings** in the System Navigator.
2. Click **Incident** and then configure the following settings for the Incident application:

Setting	Description
Notify incident owner if Parent Incident flag was unchecked	When the Parent Incident flag is unchecked, a notification is sent to all the assignees of the child incidents that were related to this parent incident
Default Category	The default category when you register a new Incident. The out-of-box value for this parameter is "none".
Parent to Child Incident Default Status	When any of the following scenarios occurs, the status of the child incident changes to the default status that is specified in this setting. ◦ The parent-child relationship is dismissed from the parent incident ◦ The parent incident is closed and the **Parent Incident Relationship Model** is **Parent Incident and Child Incidents close independently**
Parent Incident	Whether to close a child incidents when its parent incident is closed

Setting	Description
Relationship Model:	
Post back link to Child	The link file that posts the changes of certain fields in the parent incident to the corresponding fields in child incidents. This function works only when you select **Close Child Incidents when Parent Incident closed** in **Parent Incident Relationship Model**. You can customize the fields that are posted back to the child incidents. For more information about links, see Links.

3. Optionally, click the **Incident Task** and then configure the following settings for an incident task:

Setting	Description
Default Category	The default category when you register a new incident task. The out-of-box value for this parameter is "none".

4. Click **Save** and then click **OK**.

Configure the Incident Management environment

Applies to User Roles:

System Administrator

Incident Management provides an environment record in which you define the operational environment for the application by allowing or disallowing specific operator actions. Administrators can modify the environment parameters to match the operational requirements of their organization.

To configure the Incident Management environment:

1. Click **Incident Management** > **Administration** > **Environment** in the System Navigator.
2. Select or clear the parameters for your Incident Management environment.

> **Tip:** You can use the field help to view the description for each setting. To view the help on field:

- Web client: Select a field, and then press **F1**.
- Windows client: Select a field, and then press **Ctrl+H**.

3. Click **Save**.
4. Click **OK**.

Create a template to complete incident records

Applies to User Roles:
System Administrator
Templates enable users to quickly complete incident records by automatically populating various fields with necessary information. You can create as many templates as you need while authorizing select user roles for each template. The users authorized to use a particular template will then be able to apply that template when completing an incident.

Note: Make sure that the user profile is enabled to use templates.

To create a template, follow these steps:

1. Click **Tailoring** > **Templates**, and then click **New**.
2. Type a name in the **Template name** field.
3. Select Incident in the **Table name** field, and then click **Next**.
4. Click **Fill** for each user role that you are authorizing to use this template.
5. Modify the fields as required to meet the needs of your template by double-clicking in the field to assign a value to each field you select.
6. Click **Add** to exit the template wizard.
7. Click **Save**.
8. Click **OK**. The roles authorized for this template can now use or modify this template.

Alternatively, you can create a template from an existing record. To do this, follow these steps:

1. Click **Incident Management** > **Search Incidents**.
2. Enter an Incident number in the **Incident ID** field, and then click **Search**.
3. Click the incident record.
4. Click **More** or the More Actions icon and select **Create Template from Record**.
5. Modify the name in the **Template name** field.
6. Click **Fill** for each user role that you are authorizing to use this template.
7. Modify the fields as required to meet the needs of your template by double-clicking in the field to assign a value to each field you select.
8. Click **Add** to exit the template wizard.
9. Click **Save**.
10. Click **OK**.

Assignment groups

An assignment group is a list of users who are responsible for an Incident record. Incident Management notifies the group when an Incident record opens or escalates. Assignment groups make the routing and escalation of Incident records easier.

For example, the Service Desk Agent receives a service request to fix a disabled workstation. The agent creates an Incident record, and then assigns the incident to the Hardware assignment group. The hardware technician determines that the hard drive must be replaced. Because the drive must be purchased, the technician assigns the Incident record to a Request Fulfillment assignment group for acquisition. If the hard drive purchase is delayed, and the delay impacts the closure of the Incident record in a reasonable amount of time, Incident Management automatically escalates the Incident record and assigns it to the Request Fulfillment manager.

HP Service Manager administrators create Assignment groups as part of the Ongoing Maintenance process.

Add an Incident Management assignment group

Applies to User Roles:
System Administrator

Incident Management assignment groups specify the Incident Coordinator and Operators in the group so that when someone creates a new incident it can be assigned to the applicable group. Typically, assignment groups are organized by location and expertise. To facilitate incident response, new assignment groups can be added to the out-of-box assignment groups for Incident Management.

To add an Incident Management assignment group:

1. Click **Incident Management** > **Configuration** > **Assignment Groups**.

   Alternatively, you can click **System Administration** > **Ongoing Maintenance** > **Groups** > **Assignment Groups**.

2. Type the name of the group in the **Assignment Group** field.

3. Provide the applicable information for the remaining fields on the **Group** tab.

4. Click the **Members** tab.

5. Insert the cursor in a blank line and use the Fill button to select the operators you want to assign to the group. There is no limit to the number of operators in an assignment group. However, consider how many users should respond to an incident when you create and populate a new assignment group.

6. Click **Add**.

7. Click **OK**.

Using mass update with Incident Management record lists

Mass update enables you to select multiple records from a list of records and then to update the value in a field or several fields in the selected records. The system provides a template form that displays the fields for the selected records and allows a user to change the value of any of the displayed fields. The Mass Update template form does not display all fields in the records. For example, fields marked read only in the data policy do not display. You can also do a Complex Update on the selected records. A Complex Update uses RAD expressions containing variables and concatenated fields to populate another field in the records.

When doing a mass update, you should remember that the value you enter for a particular field becomes the value for that field for all of the selected records. Whenever you update incident records, you must also update the incident activity data.

Mass update is available for incident records and incident queue records. The ADMIN and SYSADMIN profiles in the out-of-box system provide the Template Mass Update and Complex Mass Update capability

A System Administrator can edit the datadict table and probsummary file so that a field does not appear in the list of fields displayed by the Mass Update wizard. On the Data Policy form, change the Usage Type column for the field to System.

Update multiple incident records

Applies to User Roles:
System Administrator
You can use mass update to update a value in one or more fields for multiple incident records. For example, if you want to update multiple high priority incident records, select the high priority view of the Incident queue. The value you enter for a particular field becomes the value for that field for all the records you selected for mass update.

You can use complex update to enter expressions as instructions for actions to be performed on multiple incident records.

To update multiple incident records by using **Mass Update**:

1. Click **Incident Management** > **Search Incidents**.

2. Use search or advanced search to find one or more records. Select the View list of incident records that you want to update. For example, select High Priority Incidents to update multiple high priority incident records.

3. Use the arrow keys to move to a row and then use the space bar to select individual records. A range of records can be selected using **Shift**+Spacebar. You can also use the scroll bar and the **ctrl** key to select individual records.

4. Click **Mass Update**.

5. Update the fields to be included in the mass update:
   a. Double-click the field that you want to update, and then type the value for the field in the box or use the Fill feature to display a list of potential values for the field.

   b. Click **Next**.

   c. Continue updating the fields that you want included in the mass update.

d. Click **Next** after each update.

e. Click the **Activity Update** field to document what is included in the mass update. When the mass update is complete, these notes display in the Journal Update of the Activities section for each record.

6. Click **Execute**. Mass update starts, and then displays each incident number as it is updated.

7. If an incident record cannot be included in the mass update, you can choose to:
   - **Retry**: Retry the mass update.
   - **Skip**: Skip the incident record to exclude it from the mass update and continue with the next record.
   - **End**: End the mass update, and retry later.

To update multiple incident records, using **Complex Update**:

1. Click **Incident Management** > **Search Incidents**.

2. Use search or advanced search to find one or more records. Select the View list of incident records you want to update. For example, select High Priority Incidents to update multiple high priority incident records.

3. Click **Mass Update**.

4. Click **Complex Update**.

5. Follow the instructions in the complex update form and type the expressions in the **Instructions to be executed ONCE at the beginning of mass add/update** field and the **Instructions for action on EACH RECORD** field.

6. Click **Execute**.

7. If an incident record cannot be included in the complex update, you can choose to:
   - **Bypass**: Bypass the invalid message and include the incident record in the complex update.
   - **Skip**: Skip the incident record to exclude it from the complex update and continue with the next record.
   - **End**: End the complex update, and retry later.

Incident Management downtime records

You can access Incident Management downtime records by using the Incident Management Security Administration Utility to show the availability of a selected device. Availability measures the ability of a device or component to provide service within a measured time frame. There are three downtime measurements.

Type of availability	Description
Explicit unavailability	The downtime experienced by the failing device.
Implicit unavailability	The downtime experienced because of the failure of a parent or controlling device.
Perceived unavailability	The explicit or implicit downtime during normal business hours. The total reflects only working hours.

Create a downtime record

Applies to User Roles:
System Administrator
As part of monitoring the availability of devices in the system, a System Administrator creates downtime records for a specific device.

To create a downtime record:

1. Click **System Administration** > **Base Configuration** > **Monitoring** > **Downtime**.
2. Type the applicable data in the **Logical Name**, **Location**, **Contact Name**, **Type**, and **Table Name** fields.
3. Click **Add**.
4. Click **OK**.

Reset downtime

Applies to User Roles:

System Administrator

To reset downtime:

1. Click **System Administration** > **Base Configuration** > **Monitoring** > **Downtime**.
2. Click **More** > **Reset**.
3. Click **Schedule** to set a time for the reset to occur.
4. Click **OK**.

Create a note

Applies to User Roles:
System Administrator
Any note that an Administrator or Operator user creates is saved with the associated HP Service Manager records. You can add more notes each time you select the Notes option. Each set of notes has a time stamp and the name of the operator who created the note set.

You must have notes enabled by your Service Manager System Administrator to use this feature. To enable notes for an Incident Management operator, select notes on the Incident Management Security Profile form. For the out-of-box system, only the System Administrator has notes enabled.

To create a note:

1. Do one of the following to locate a record:
   a. Select an incident record from a queue.
   b. Use search or advanced search to find one or more records.
2. Click **More** or the More Actions icon and select **Notes**.
3. Type the information in the **Add New Note** box.
4. Click **Save**.
5. Click **Back**.
6. Click **Save & Exit**.

Incident configuration

Incident configuration enables you to configure alert, Incident categories, workflow, solution matching, and so on.

Create an incident category

Applies to User Roles:

System Administrator

If you are an HP Service Manager Administrator, you may want to create an incident category. To do this, you can modify an existing category record, or you can create a new category record. HP Service Manager provides out-of-box category records that you can use or modify.

> **Note:** When a category is set as the default category in settings, do not delete it to avoid unpredictable issues.

To create new category record:

1. Click **Incident Management**.
2. Click **Configuration** > **Incident Categories**.
3. Click **New**.
4. Type the name of the incident category.
5. Clear the **Active** check box if you do not want the new category to appear in the category list.

   > **Note:** If you clear the **Active** check box, this category cannot be used to create new incidents.

6. Type the category description.
7. Select a workflow for the category.
8. Click **Save**.

9. ***Optional***: Click the **Link New Subcategories** button to create a new subcategory for the incident category.

Note: The **Apply To** flag indicates whether the category is shared across different modules.

For example, if the **Apply To** is set to "Interaction/Incident", then this category will be created in both the interaction category table and the incident category table.

Typical shared categories in the out-of-box configuration include Complaint, Request for Information, Incident, and Request for Administration.

For the **Apply To** flag in Incident Category:

When creating an incident category, the **Apply To** option is predefined as "Incident" only and cannot be modified. However, an incident category can also be created when creating an interaction category with the **Apply To** option set as "Interaction/Incident" or "Interaction/Incident/Problem".

When searching for an incident category, all the **Apply To** values that include Incident can be used.

The following list is used in Incident Category:

1 - Incident

3 - Interaction/Incident

4 - Interaction/Incident/Problem

Note: Incident category name is read-only after the category is created.

Create an incident task category

Applies to User Roles:

System Administrator

If you are an HP Service Manager Administrator, you may want to create an incident task category. To do this, you can modify an existing category record, or you can create a new category record. HP Service Manager provides out-of-box category records that you can use or modify.

To create a new incident task category record:

1. Click **Incident Management**.
2. Double-click **Configuration** > **Incident Task Categories**.
3. Click **New**.
4. Type the name of the incident task category.
5. Type a description of the problem task category.
6. Clear the **Active** check box if you do not want the new category to appear in the category list.

   Note: If you clear the **Active** check box, this category cannot be used to create new incident tasks.

7. Select a workflow for the category. The **Workflow** tab is displayed.
8. Click **Save**.

Note: Incident task category name is read-only after the category is created.

Add a new subcategory to an incident category

User Roles: System Administrator and Implementer

You can add a new subcategory directly for an incident category.You can view a list of subcategories and their record details associated with the current category.

To add a new subcategory for an incident category:

1. Click **Incident Management** > **Configuration** in the System Navigator.
2. Click **Incident Categories** and then click **Search** in the form that appears.
3. Select the Incident Category for which you want to add a subcategory.
4. Click the **Subcategories** tab in the Incident Category Definition page, and then click the **Link New Subcategories** button.
5. Type a subcategory name.
6. Type a description for the subcategory.

7. Click **Save** to add the new subcategory.
8. ***Optional***: Click the **Link New Areas** button to create areas for the incident subcategories. When you have finished, click **Save**.

Add a new area for an incident subcategory

Applies to User Roles:

System Administrator and Implementer

You can add a new area directly for an incident subcategory.You can view a list of areas and their record details associated with the current subcategory.

To add a new area for an incident subcategory:

1. Click **Incident Management** > **Configuration** in the System Navigator.
2. Click **Incident Categories** > **Search**.
3. Select the Incident Category for which you want to add an area.
4. Under the **Subcategories** section in the Incident Category Definition page, select the subcategory for which you want to add an area.
5. Type an area name.
6. Type a description for the area.
7. Click **Save** to add the new area.

Incident solution matching

When you create an incident, a list of potentially related incidents appears based on the pre-defined solution matching configuration. You can then select the matched records and update them directly. You can also run solution matching for an existing incident that is not closed. To do this, select the incident and then click **More** > **Solution Matching** from the Detail List toolbar.

In an out-of-box system, the following options are provided for Incident solution matching:

- Find an incident with a matching service or configuration item
- Find an incident with a matching related service or configuration item
- Find an incident with a matching title
- Find a known error with a matching service or configuration item
- Find a known error with a matching title
- Find a problem with a matching service or configuration item
- Find a problem with a matching title

To configure Incident solution matching options, navigate to **Incident Management** > **Configuration** > **Solution Matching**.

Note: If you create an incident from Service Desk escalation or link to a new incident from the Related Records section, the above incident solution matching will be ignored.

Incident management downtime record

You can access Incident Management downtime records by using the Incident Management Security Administration Utility to show the availability of a selected device. Availability measures the ability of a device or component to provide service within a measured time frame. There are three downtime measurements.

Type of availability	Description
Explicit unavailability	The downtime experienced by the failing device.
Implicit unavailability	The downtime experienced because of the failure of a parent or controlling device.
Perceived unavailability	The explicit or implicit downtime during normal business hours. The total reflects only working hours.

Add a downtime record

Applies to User Roles:

System Administrator

As part of monitoring the availability of devices in the system, a System Administrator adds downtime records for a specific device.

To add a downtime record:

1. Do one of the following:
   - Click **Incident Management** > **Configuration** > **Downtime Records**.
   - Click **System Administration** > **Base System Configuration** > **Monitoring** > **Downtime**.
2. Type the applicable data in the **Logical Name**, **Location**, **Contact Name**, **Type**, and **Table Name** fields.
3. Click **Add**.
4. Click **OK**.

Security

The following sections explain the Incident Management security roles, security areas, and rights.

Incident security areas

The security areas for Incident are Incident, Incident Tasks, and Incident Management Configuration. These areas contain the default security rights and settings for the Incident Management module. The security right settings will be inherited by the new roles created in an area when no settings are specified in the security role.

These security areas are used to set permissions to operators to provide access to particular area of Incident. The following table lists the areas and the relevant Incident menu items the operators can access.

Area	System Navigator menu items for this area
Incident	This area contains the default security rights and settings for Incident. The rights will be copied to new roles created for this area. However, the settings will only be inherited if there are no settings specified on the Role.
Incident Task	This area contains the default security rights and settings for Incident Tasks. The rights will be copied to new roles created for this area. However, the settings will only be inherited if there are no settings specified on the Role.
Incident Management Configuration	This area contains the default security rights and settings for Incident Management administration and configuration.. For example, Settings, Incident Categories, Incident Task Categories, and Solution Matching. The rights will be copied to new roles created for this area. However, the settings will only be inherited if there are no settings specified on the Role. **Note:** When you set the security rights for a security role in the Incident Management Configuration area: • The **View** right is to view the settings defined in the **Administration** menu and the **Configuration** menu. • The **Update** right is to update the values of existing settings defined in the **Administration** menu and the **Configuration** menu. • The **New** and **Delete** rights are to create and delete a setting in the **Configuration** menu, such as category.

Area	System Navigator menu items for this area
	• The **Admin** right is to add, edit, or delete the settings in the following menus: ◦ **Administration** > **Settings**. ◦ **Administration** > **Configuration** > **Solution Matching**

Default rights

The default rights defined in areas will be inherited when you create new security roles. The following table shows the out-of-box default rights defined in the Incident, Incident Tasks, and Incident Management Configuration areas.

Area Name	View	New	Update	Delete/Close	Expert	Admin
Incident	TRUE	FALSE	Never	Never	FALSE	FALSE
Incident Tasks	TRUE	FALSE	Never	Never	FALSE	FALSE
Incident Management Configuration	FALSE	FALSE	Never	Never	FALSE	FALSE

Default settings

The default settings defined in areas will be inherited when you create new security roles. In an out-of-box system, none of the default settings is checked or set in the Incident, Incident Tasks, and Incident Management Configuration areas.

Incident security roles and settings

The out-of-box security roles for the Incident module include the following:

- Incident process owner
- Incident coordinator
- Incident analyst
- Incident manager
- Incident task assignee
- Configuration auditor
- Operator

Mapping between previous security profiles and current PD security roles

The following table lists the mapping relationship between previous Incident security profiles and current PD security roles in the Incident module.

Security Profile	Security Role/Area
DEFAULT	DEFAULT/Incident
configuration auditor	configuration auditor/Incident
incident analyst	incident analyst/Incident
incident coordinator	incident coordinator/Incident
incident manager	incident manager/Incident
initiator	initiator/Incident
operator	operator/Incident
problem manager/coord	problem manager/Incident
	problem coordinator/Incident
service desk agent	service desk agent/Incident

Security Profile	Security Role/Area
service desk manager	service desk manager/Incident
service tech	service tech/Incident
sysadmin	sysadmin/Incident
N/A	incident task assignee/Incident
N/A	incident process owner/Incident

Field mapping between security profiles and PD security rights/settings

The following table lists the mapping of fields in legacy Incident security profiles and Process Designer security roles.

Security profile settings	Process Designer security rights and settings
New	New
Close	Delete/Close
Inactivate	
Mass inactivate	
Update	Update
Change category	
View	View
Log	
Can notify	
Search for duplicates	
Alternate views	
Can use callback list	
Advanced search	
Reopen	Reopen

Security profile settings	Process Designer security rights and settings
Mark problem candidate	Expert
Can suspend	
Can unsuspend	
Notes	
Override	
Tempate Mass Update	
Complex Mass Update	
Allow inefficient query	Allow Inefficient Query
Skip query warning	Skip Inefficient Query Warning
Can create personal views	Can Create Personal Views
Can create system views	Can Create System Views
Lock on display	Lock On Display
Modify Template	Modify Template
Allowed statuses	Allowed Statuses
QBE format	List Format
Search format	Search format
Manage format	Manage Format
Initial view	Initial View
Auto-notify format	Notify Format
Incident macro mail format	N/A
Default template	
Default category	
Assignment groups	Assignment groups
Authorized categories	Allowed Categories
New thread: View -> Search	New thread: View -> Search
New thread: Search -> List	New thread: Search -> List

Security profile settings	Process Designer security rights and settings
New thread: List -> Edit	New thread: List -> Edit
New thread: View -> Edit	New thread: View -> Edit

Note: N/A means the previous fields are obsolete and are not mapped to PD security rights/settings.

Out-of-box role rights

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

Area Name	Role Name	View	New	Update	Delete/Close	Modify Template	Expert	Admin
Incident	incident process owner	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE
	system administrator	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE
Incident Tasks	configuration auditor	TRUE	TRUE	Never	Never	FALSE	FALSE	FALSE
	incident analyst	TRUE	TRUE	Always	Always	FALSE	TRUE	FALSE
	incident coordinator	TRUE	TRUE	Always	Always	FALSE	TRUE	FALSE
	incident manager	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE
	incident process owner	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE
	incident task assignee	TRUE	FALSE	When assigned to workgroup	When assigned to workgroup	FALSE	FALSE	FALSE
	initiator	TRUE	TRUE	Never	Never	FALSE	FALSE	FALSE
	operator	TRUE	TRUE	When assigned	When assigned	FALSE	FALSE	FALSE
	problem	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE

Area Name	Role Name	View	New	Update	Delete/Close	Modify Template	Expert	Admin
	manager							
	SD agent/manager	TRUE	FALSE	When assigned	Never	FALSE	FALSE	FALSE
	service tech	TRUE	TRUE	Always	Always	FALSE	FALSE	FALSE
	system administrator	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE
Incident Management Configuration	incident manager	TRUE	TRUE	Always	Always	FALSE	FALSE	FALSE
	incident process owner	TRUE	FALSE	Never	Never	FALSE	FALSE	FALSE
	system administrator	TRUE	TRUE	Always	Always	TRUE	TRUE	TRUE

For information about the out-of-box role rights in the Common Configuration area, see Out-of-box role rights in the Common Configuration area

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 Incident Management 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!


Java™
COMPATIBLE