BMC Service Desk

Version 8.1.00

Part of
BMC Remedy ITSM Suite version 8.1.00

For all the latest content, see https://docs.bmc.com/docs/display/servicedesk81.

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC™

www.bmc.com

BMC Software Inc.
2101 CityWest Blvd, Houston TX 77042-2827, USA
713 918 8800
Customer Support: 800 537 1813 or contact your local support center

Home

This space contains information about the BMC Service Desk 8.1 release, which is part of the BMC Remedy IT Service Management (BMC Remedy ITSM) Suite 8.1 release.

Featured content

- New features for this release
- Hub and Spoke capability overview
- Using the BMC Atrium Service Context
- Creating email generated incident requests
- Accessing BMC Knowledge Management
- Changes to the BMC Atrium CMDB for BMC Remedy ITSM
- Quickly Creating a Fully Qualified Incident Request (video)
- Quickly Resolving an Incident Request by Using Incident Matching (video)
- Known issues and workarounds
- Known issues for browsers

Where to start

- End users: Incident Management, Problem Management, Common Service Desk features
- Administrators: Configuring after installation
- Developers: Developing

About BMC Service Desk

BMC Service Desk uses automated, ITIL-compliant incident management and problem management processes to help IT organizations respond quickly and efficiently to conditions that disrupt critical services. The incident management process focuses on getting users up and running after disruptions. The problem management process focuses on determining the root cause of a problem, and on using the change management process to correct the root cause. BMC Service Desk provides a single point of contact for user requests, user submitted incidents, and infrastructure-generated incidents.

What's new

This section provides information about what is new or changed in this space, including urgent issues, documentation updates, maintenance releases, service packs, and patches. It also provides license entitlement information for the release.

✓ **Tip**
To stay informed of changes to this space, place a watch on this page.

No updates have been added since the release of Version 8.1.00.

License entitlements for BMC IT Service Management

This topic explains the entitlements that apply to licenses you purchase from BMC Software. For information about restrictions to those licenses, please see your Product Order Form.

You can download the components mentioned herein from the Electronic Product Distribution website. Use the user name and password that your BMC sales representative gave you. (This user name and password is different from the one you use to access the Customer Support site.)

If you do not have a current license for the components you want, contact a BMC sales representative by calling 800 793 4262. If you cannot download the components, contact a sales representative and ask for a physical kit to be shipped to you.

- BMC Atrium entitlements for BMC Remedy IT Service Management Suite
- BMC Remedy IT Service Management Suite - Base License

BMC Atrium entitlements for BMC Remedy IT Service Management Suite

This section describes the BMC Atrium license entitlements and any restrictions for BMC Remedy ITSM Suite, and contains the following topics:

- BMC Analytics for BSM license for BusinessObjects
- BMC Atrium CMDB licenses
- BMC Atrium Shared Components licenses

BMC Analytics for BSM license for BusinessObjects

BMC Analytics for BSM uses SAP BusinessObjects, a third-party business intelligence platform to administer and publish reports.

SAP BusinessObects Enterprise XI is shipped with BMC Analytics for BSM, and is available for download on the BMC Electronic Product Distribution (EPD) site. If you don't already have it installed in your environment, use the downloaded file to install it. If you already have it installed in your environment, you must have adequate licensing for both your SAP BusinessObjects Enterprise XI environment and the BMC Analytics for BSM content.

License Types: User vs. Premium User

There are two types of user licenses available for BMC Analytics for BSM: User and Premium User. Depending on the license type, users will have access to the capabilities of either the Professional or Premium edition of SAP BusinessObjects Enterprise. Non-premium users have full access to view and author Web Intelligence content, but may not use other content types such as viewing Crystal Reports. Premium users may use all the capabilities of the BusinessObjects Enterprise Premium suite, including viewing of any BusinessObjects document types including viewing Crystal Reports from the BMC Remedy Mid Tier.

Accessing non-BMC data

The BMC Analytics for BSM license provides the ability for the licensee to use the SAP Business Objects technology embedded in BMC Analytics for BSM for the purpose of accessing data from BMC products.   It does not provide the ability to use the product as a standalone enterprise Business Intelligence system outside the context of BMC products.   All data accessed by BMC Decision Insights must either come from BMC products directly or if there is data from non-BMC products, this data must be presented in context of BMC data.

For example:

- it would be acceptable to use BMC Analytics for BSM to create a report that shows incident ticket information (from BMC product) as well as the cost center of the person logging the ticket (from a non-BMC data source).
- It would NOT be acceptable to create a report of employees and their cost centers (from non-BMC data source and not in context of BMC data)

BMC Atrium CMDB licenses

The BMC Atrium CMDB Suite, BMC Atrium CMDB Enterprise Manager, and BMC Atrium CMDB Enterprise Manager - Enterprise Use licenses for BMC Atrium Core entitle you to use the following functions:

- BMC Atrium CMDB, including the following components:
  - Normalization Engine
  - Reconciliation Engine
  - Atrium Explorer
  - Atrium Impact Simulator
  - Common Data Model
  - Class Manager
  - Product Catalog and Definitive Media Library
  - Service Catalog
- BMC Atrium Integration Engine
- Atrium Integrator
- BMC Atrium Web Services
- BMC Atrium Web Services Registry

BMC Atrium Shared Components licenses

Because the BMC Atrium Shared Components (BMC Atrium SC) package includes zero dollar licenses, you may only use these licenses within the context of the solution provided. You cannot use the shared components as stand-alone products. The context of this limitation is as follows:

- BMC Remedy Action Request System (AR System) is supplied as a foundational component for other BMC Atrium SC products. Use of AR System is limited to running the other components within the BMC Atrium SC.
- Three fixed users are provided with AR System. Additional users may not be added until AR System and additional user licenses are purchased.
- Data from the BMC Atrium Integration Engine (Integration Engine) may only be used to populate BMC Atrium CMDB with other BMC products or external data sources. It may not be used to populate data into the AR System forms directly.
- BMC Atrium CMDB may only be integrated with external data sources or thirdparty discovery products if at least one BMC product is also integrated with BMC Atrium CMDB. It may not be used in a stand-alone configuration without integration with a BMC solution.
- SAP BusinessObjects Enterprise is required with BMC Analytics for BSM. Since this version of SAP BusinessObjects Enterprise is distributed under an OEM agreement, you must use SAP BusinessObjects Enterprise with BMC data sources. BMC Atrium SC includes a temporary key (30 day) in the distributions (both kit and EPD) to use with SAP BusinessObjects Enterprise. No license to SAP BusinessObjects Enterprise is conveyed directly as part of BMC Atrium SC delivery. The license conveys only when you

purchase BMC Analytics for BSM, or another BMC product which requires SAP BusinessObjects Enterprise (for example, BMC ProactiveNet Performance Manager).

Actions that would void the zero dollar licenses and require a full purchase of the components include, but are not limited to:

- Using the AR System server to develop a new application.
- Using the AR System server as a foundational component for a product that contractually requires the purchase of AR System.
- Using the BMC Atrium Integration Engine to directly integrate with AR System and not BMC Atrium CMDB.
- Using only third-party products to populate BMC Atrium CMDB, without integrating it with any BMC applications.
- Using more license capacity for BMC Atrium Orchestrator product components other than as listed above. Using non-BMC (AKA third-party) BMC Atrium Orchestrator Application Adapters.
- Using SAP BusinessObjects Enterprise exclusively with non-BMC data sources.

BMC Remedy IT Service Management Suite - Base License

- Includes unlimited use of the following BMC Atrium Orchestrator core product components. Test and development licenses are provided at no additional cost:
  - Repository
  - Access Manger
  - Grid Manager
  - Metrics and Reporting
  - Operations Actions Management Modules
  - Operations Actions Utility Modules.
- Includes license rights to use the following BMC Atrium Orchestrator product components for configuration of an initial Orchestration environment as detailed here:
  - One (1) Configuration Distribution Peer (CDP, a master peer/server that executes all workflows)
  - Three (3) Development Studio Licenses (the workflow authoring tool used to create and modify workflows)
  - Five (5) Operator Control Panel (OCP) Licenses (the web-based user interface designed to monitor and manage workflows and/or for semi-automation mode)
  - Application Adapters (the systems/interfaces/gateways/connectors used to talk to external applications) for BMC products.

Version 8.1.00

This topic contains information about enhancements in BMC Service Desk 8.1.00.

- Enhancements in version 8.1

Enhancements in version 8.1

This topic describes the following product enhancements available with version 8.1:

- Simplified installation
- UI updates

Simplified installation

The BMC Remedy IT Service Management 8.1 installation has been greatly simplified:

- To reduce manual user inputs, the number of panels in the installer are reduced. Information from the AR System server is intelligently leveraged by the installer to simplify installation.
- Related inputs are consolidated into single panels.
- The following configuration modules were removed from the installer, but their instructions are linked below:

Configuration module removed from installer	Where documented
BMC Atrium Service Context	Configuring BMC Atrium Service Context for BMC Remedy ITSM applications
Migrating BMC Knowledge Management permission mappings (during upgrades only)	Migrating user permissions from the 7.2 and 7.5 releases
Private port queues	Adding a private queue port number for Software License Management
Object modification logging	Using the object modification log
Crystal Reports	Showing or hiding Crystal Reports – the web-only reports are intsalled by default.
Thread setting	The installer automatically sets the Fast and List threads to 12 maximum and 8 minimum.

For additional instructions on configuring BMC Remedy IT Service Management, go to Configuring after installation.

UI updates

Numerous updates have been made throughout the Service Desk application to make the user interface (UI) behave consistently with other applications in BMC Remedy IT Service Management Suite. Key UI changes include:

- Incident matching
- Additional columns available in the console tables
- Menu structure simplified
- Refresh button consistency
- Knowledge search UI on the Incident form updated
- Hover-over UI updated
- Presentation of Incident and Problem details updated
- Incident form auto-complete feature updated
- Service field menu entries sorted alphabetically on Incident form
- View Service Request link in Incident Management

Incident matching

When you click Incident Matching while viewing an incident request, the Incident Matching dialog box now opens with a lists of possible matching records for you to select from. If you do not see an appropriate matching record, you can return to the Incident form without selecting a record. See Searching for matching records for more information.

Additional columns available in the console tables

There are now more columns that you can add to the Incidents and Problems tables on the Incident Management and Problem Management consoles. See the description of the Preferences button on Functional areas of the Incident Management console and Functional areas of the Problem Management console for information about adding columns to the application tables.

Menu structure simplified

The Navigation pane menu structure on the Incident Management and the Problem Management consoles and on the Incident and Problem forms has been flattened to simplify navigation through the menus. See Functional areas of the Incident Management console and Functional areas of the Problem Management console for a description of the new Navigation pane menu structure on the consoles.

Refresh button consistency

The Refresh button now appears in a consistent location on the main Service Desk forms and consoles: in the top right corner of the form or console, to the left of the Global search field.

Knowledge search UI on the Incident form updated

When you perform a knowledge search from the Incident form, the search results are now displayed in a format that is similar to that of the Global search results. The knowledge search results are also displayed in the same browser window as the Incident form, instead of a separate browser window.

Hover-over UI updated

The hover-over UI has been updated to include more, and more consistent information.

Presentation of Incident and Problem details updated

When viewing details related to an Incident or Problem record, for example: the Incident Matching dialog, or a Known Error record, the UI has been updated to more closely resemble the Best Practice view. This makes it easier to view information in the UI.

Incident form auto-complete feature updated

The auto-complete feature has been updated on the Incident form to make it more consistent with the auto-complete feature on other forms in the BMC Remedy ITSM suite of applications. For example, in the Service field, the auto-complete feature now performs a "match-anywhere" function on text typed into the field.

Service field menu entries sorted alphabetically on Incident form

The entries in the selection menu related to the Service field on the Incident form are now sorted alphabetically.

View Service Request link in Incident Management

If the Incident request that you are working on was generated from BMC Service Request Management, there is now a link (**View REQ00000000123**) to the originating service request in the Navigation pane of the Incident request form.

Corrected issues in version 8.1.00

The following issue has been corrected in release 8.1.00 of BMC Service Desk.

Issue number	Description
SW00430698	In the Incident Management Best Practice view, the **Categorization** and **Tasks** tabs are not visible by default after you upgrade from one of the following versions of BMC Remedy Incident Management: 7.0.3 Service Pack 8 (and later) 7.6.04 Service Pack 1 (and later)

Key concepts

This section provides a high-level overview of the product and includes information about:

- Business Service Management (BSM)
- Business value
- User goals and features
- ITIL processes
- End-to-end processes
- User roles
- Architecture

Business Service Management (BSM)

BSM provides a comprehensive and unified platform that simultaneously optimizes IT costs, demonstrates transparency, increases business value, controls risk, and assures quality of service. Delivering an "ERP for IT," BSM simplifies, standardizes, and automates IT processes so that you can manage business services efficiently across their lifecycle -- *across distributed, mainframe, virtual, and cloud-based resources*. With BSM, your organization has the trusted information it needs, can prioritize work based on business critical services, and can orchestrate workflow across your core IT management functions.

BSM has been architected so that you can adopt it incrementally and in a low-risk fashion based on the top initiatives you are already most likely pursuing, such as Cloud Computing, Data Center Automation, and IT Service Management.

In this site, we use the following terms to explain how you can realize BSM in your organization using BMC Software products and services:

- *BSM Initiatives* describe the most common strategic initiatives that organizations are undertaking to address their IT management challenges.
- For each BSM Initiative, a set of *value paths* have been defined that capture the most common ways to get started on an initiative with the highest impact and shortest time to value based on BMC customer

experiences.

- A value path prescribes the steps, or *required capabilities*, that an organization will need to realize value around a key project within each initiative.
- Required capabilities map to BMC products or service offerings to address the required capabilities for each value path.

Business value

BMC Service Desk acts as a single point of contact for user requests, user-submitted incidents, and infrastructure-generated incidents. BMC Service Desk is the anchor product that enables you to get started with Service Desk Optimization.

An organization must address everyday, immediate incidents to carry out its business. These immediate incidents are the focus of the incident management process. In addition, it is essential to detect, analyze, and resolve problems in the infrastructure.

The BMC Service Desk consists of two features:

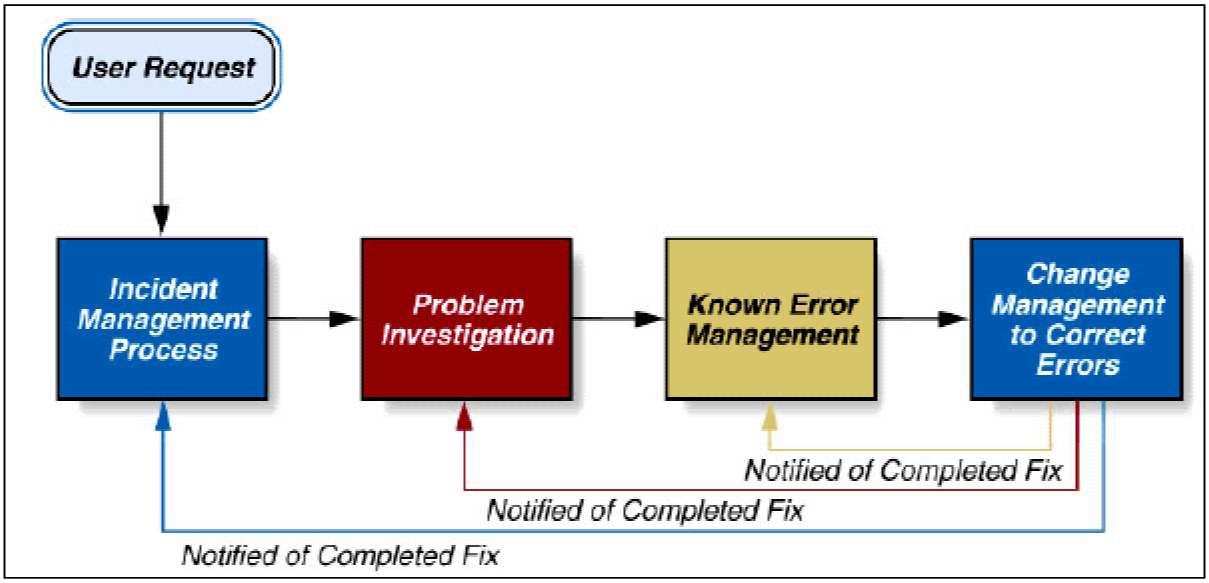
- Incident Management
- Problem Management

These ITIL compliant applications automate the incident and problem management processes to enable IT to respond quickly and efficiently to conditions that disrupt critical services.

Incident Management focuses on getting users up and running after disruptions.

Problem Management focuses on determining the root cause of a problem, and on using the BMC Change Management processes to correct the root cause.

Relationship between incident, problem, and change management processes for user requests


User Request
Incident Management Process
Problem Investigation
Known Error Management
Change Management to Correct Errors
Notified of Completed Fix
Notified of Completed Fix
Notified of Completed Fix

Related topics

Incident management user roles
Problem management user roles
Using

Incident Management

The mission of the incident management process is to resolve incident requests as quickly as possible in a prioritized fashion. The Incident Management module is designed to support this goal.

When dealing with incident requests, Incident Management is typically initiated in response to a customer call, a service request, or an automated event. An example of an automated event might be an alert from a monitoring system, such as BMC ProactiveNet Performance Management (BMC BPPM). The primary goal of the incident management process, according to ITIL standards, is "to restore normal service operation as quickly as possible with minimum disruption to the business, thus ensuring that the best achievable levels of availability and service are maintained."

When dealing with incident requests, the following best practices are critical for success:

- Prioritization, so that incidents that cause the organization the most pain, such as lost sales or work stoppage, are fixed first.
  This approach conserves your resources, and uses them where they are most needed.
- Consistent recording of incident request details. These details are then made available to other applications, such as BMC Change Management.
  This means that entries can be searched, analyzed, and communicated throughout the organization.
- Integration with BMC Atrium Configuration Management Database (BMC Atrium CMDB).
  This information can be used both to resolve the immediate incident and to determine whether other systems might be affected.

> ⚠ **Note**
> An incident is any event that is not part of the standard operation of a service and that causes an interruption to or a reduction in the quality of that service. Normal service operation is the operation of services within the limits specified by the service target. BMC Service Level Management, when integrated with Incident Management, monitors service targets.

The incident management process also handles customer requests for service, such "I need a new laptop," or "I need access to this network resource." Customers can use BMC Service Request Management to enter service requests. If BMC Service Request Management is not available, your organization can use Incident Management.

Overview of incident ownership

Incident ownership is determined automatically by Incident Management when the incident request record is created. Incident Management assigns incident ownership based on the following criteria:

- The support group of the person who submits the incident request record.
- The support group the incident request record is assigned to.

For example, consider the following support groups:

- **Support Group A** has a support group role of Help Desk. Person A is in Support Group A.
- **Support Group A2** also has a support group role of Help Desk. Person A is not a member of Support Group A2.
- **Support Group B** does not have a support group role of Help Desk; for example, it might have a support group role of Tier 2. Person B is in Support Group B.
- **Support Group C** does not have a support group role of Help Desk; for example, it might have a support group role of Tier 3.

Based on these support groups, the following example events show how the incident owner is set when no incident owner assignment event is predefined:

- Person A submits an incident and assigns it to Support Group A2 with the role of Help Desk. Ownership of the incident is set to Support Group A2 because the Assigned Group has the role of Help Desk. Otherwise, ownership of the incident is set to Support Group A.
- Person B submits an incident and assigns it to Support Group A. Ownership of the incident is set to Support Group A because the group has the role of Help Desk.
- Person B submits another incident, and assigns the incident to Support Group C. Support Group B becomes the owner, because Person B is the submitter.

Problem Management

The mission of the problem management process is to minimize the number of incidents. The Problem Management module supports this goal by managing problem investigations, known errors, and solution database entries. Problem management can proactively prevent the occurrence of incidents, errors, and additional problems.

This topic includes information about:

- Problem investigation
- Known error
- Solution database

Problem investigation

An important ITIL objective is investigating and resolving problems in a continuing effort to cut costs and improve services. A problem investigation helps an IT organization get to the root cause of incidents.

It initiates actions that help to improve or correct the situation, preventing the incident from recurring. For example, if computers are running low on disk space, ideally the problem can be resolved before it becomes an incident. Problem investigations are usually triggered by either an incident review or by an application such as BMC Event Manager. BMC Event Manager can generate an event about a capacity threshold being reached. This might cause the problem coordinator to create a problem investigation to prevent a capacity shortage from causing outages.

After a problem investigation identifies the cause, this information can result in:

- A known error, which describes the root cause as well as the proposed structural solution to remove the root cause
- A solution entry that describes how to work around the issue

Known error

A known error is a problem that has been successfully diagnosed and for which a permanent solution has been proposed.

After the root cause analysis of a problem investigation is completed and a structural solution has been proposed, a known error is created to request that the proposed solution is implemented. The implementation of the proposed solution is part of the change management process. A known error process can have one of the following results:

- A change request to implement the needed fix
- Closing the known error as an accepted issue, with updates to the knowledge database containing steps to avoid the issue

Solution database

The solutions database provides a simple repository of potential solutions or workarounds to infrastructure issues. A solution database entry contains information that might be required to provide or restore a service.

The data from the solutions database becomes input into a full knowledge management system with the use of the BMC Knowledge Management application.

For more information about BMC Knowledge Management, see the BMC Knowledge Management documentation.

Tasks overview

A task is a unit of work that needs to be completed as a step in resolving an incident request. If the solution to an incident request involves more than one action, procedure, or process, consider dividing the solution into separate tasks. Dividing the solution into separate tasks can help you to better manage and to monitor the incident request as it moves toward resolution.

You can assign the tasks to the same person, to several people, or to a support group. The person or support group to whom the task is assigned is the task implementer. When the group coordinator sets the task status to **In Progress**, the task implementers are notified of the tasks assigned to them by email, pager, or some additional means. After a task is assigned to the task implementers, they can log their progress as they complete each task.

> ⚠ **Note**
> Tasks can have an **Assigned** status only if the associated incident request also has the status of **Assigned**.

You can use a task template to add a task to an incident request, or you can create an ad hoc task. Task templates are predefined tasks that you can quickly add to an incident request. For information about how to do this, see Adding tasks using task templates. An ad hoc task is any task that is not included in the list of task templates and, therefore, you must create it manually. For information about how to do this, see Creating ad hoc tasks.

When using task templates, you can also add tasks that are divided into sub-tasks. A task that has sub-tasks is called a task group. The sub-tasks of the task group are called "children" of the task group.

Although tasks and task groups are related to specific incident request records, information about the tasks and task groups is stored on a separate Task form. You can relate an unlimited number of tasks or task groups to an incident request.

After a task or task group is assigned to a task implementer, the task implementer receives notifications to perform each of the assigned tasks.

Calbro Services company example

In the BMC Remedy IT Service Management (BMC Remedy ITSM) documentation set, a fictional company named Calbro Services helps explain how BMC Remedy ITSM principles and procedures are used in practice.

Although Calbro Services is a fictional company, it is based on research of actual BMC customers. Learning how Calbro Services manages common IT Service Management scenarios should prove useful as you use the BMC Remedy ITSM applications in your own environment.

Calbro Services, a large, global company, is headquartered in New York City and publicly traded on the New York Stock Exchange. The company has 27,000 employees in 240 offices located in 20 countries. The following table describes key business services in Calbro Services:

Key business services

Service	Description
Online banking	500 ATMs in major cities
WWW presence	Corporate site and online brokerage services
Discount equity brokerage	Online and storefront services
Sales force automation	Automated sales activities such as leads, orders, reports, and so on
Customer support	Support centers in the United States, Europe, and Asia
Mass marketing	World-wide marketing campaigns aimed at making Calbro Services a household name

User goals and features

This topic provides an overview of the service desk user goals, especially those related to solving business problems, and how they are addressed by the features in the product.

Incident Management

The goal of the incident management process is to restore normal service operation as quickly as possible with minimum disruption to the business, to ensure that the highest levels of availability and service are maintained.

To help you achieve this goal, the Incident Management documentation describes the following work flows, which are designed to help you manage incident request from beginning to end:

- Registering and assigning incident requests
- Resolving, closing, and canceling incident requests with open tasks
- Working with incident requests as a manager

Problem Management

The purpose of problem management is to reduce the number of incidents; either proactively, by preventing them from happening, or reactively, by preventing them from happening again.

To help you achieve this goal, the Problem Management documentation describes the following work flows, which are designed to help you manage problem investigations from beginning to end:

- Performing the incident request review
- Performing the root cause analysis
- Performing the analysis review
- Closing the problem investigation

ITIL processes

BMC Service Desk supports the following ITIL processes:

- Incident management, through the Incident Management feature
- Problem management, through the Problem Management feature

For information about how BMC Service Desk supports these processes, see User goals and features and Business value.

End-to-end processes

This section describe various incident and problem management processes that you can manage from start to finish using the Incident Management and Problem Management features of BMC Service Desk.

- Incident management processes
- Problem management processes

Incident management processes

This topic describes some of the incident management process that you can manage using the Incident Management feature of BMC Service Desk.

- Process flow status and the lifecycle of an incident request
- Incident management use cases

Incident management process flow video

Watch the following video to learn about the basic flow of the incident management process.

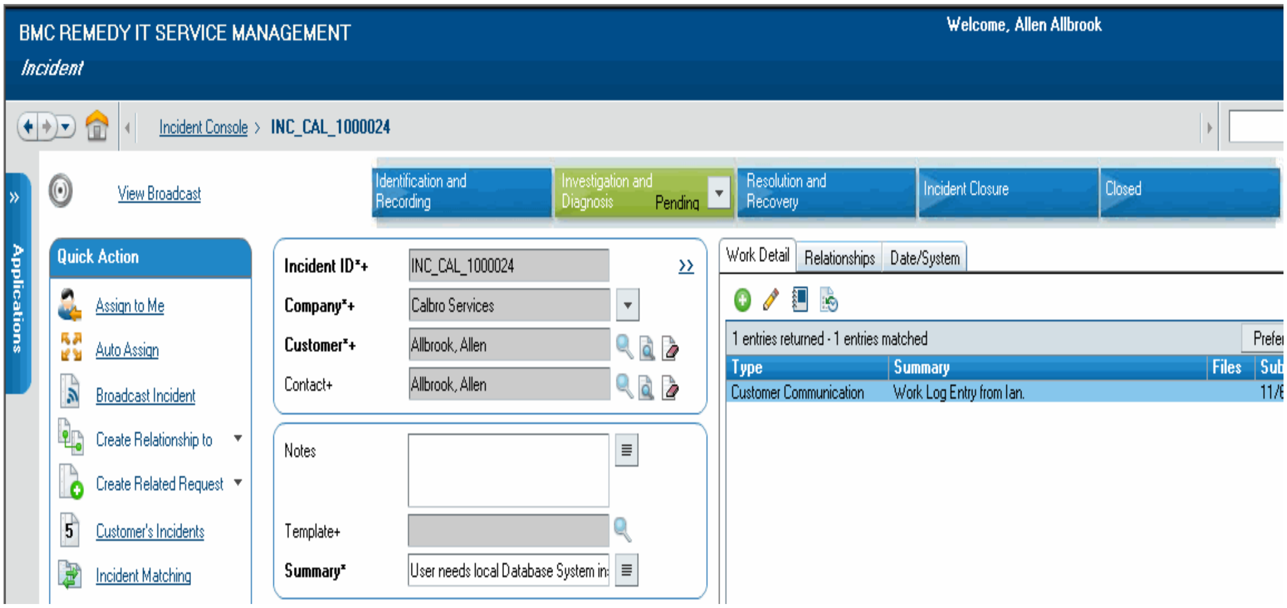
> **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

Process flow status and the lifecycle of an incident request

The Process Flow Status area displays the flow of the incident request through the stages of the process in blue. The current stage of the incident is highlighted in green. The status of the incident is indicated by both color and text.

The Process Flow Status area (Best Practice view)



Incident ID*+ INC_CAL_1000024

Company*+ Calbro Services

Customer*+ Allbrook, Allen

Contact+ Allbrook, Allen

Notes

Template+

Summary* User needs local Database System in:

1 entries returned - 1 entries matched

Type	Summary	Files	Sub
Customer Communication	Work Log Entry from Ian.		11/8

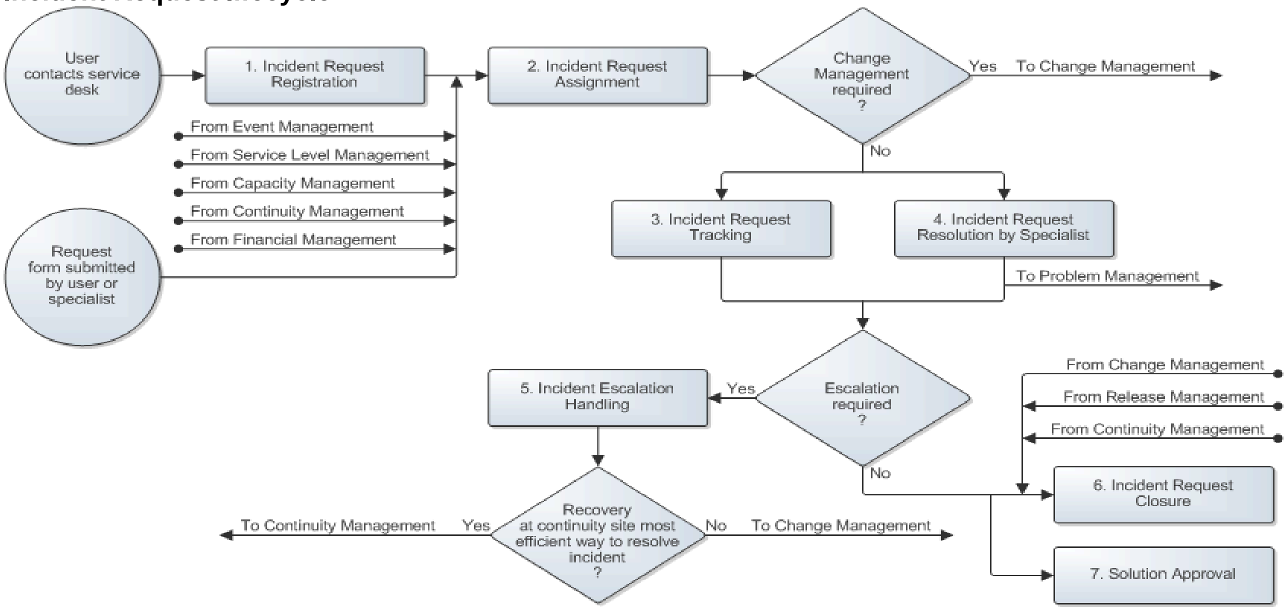
Disclaimer
Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

The Process Flow Status area also guides you through the stages of the incident lifecycle. At each stage, the diagram provides applicable accelerators. When you select an accelerator, you are prompted to enter the data required to complete the task. You can also enter optional recommended data in the dialog box.

The following figure provides an overview of the incident request lifecycle, as described by the BMC Service Management Process Model. Each of the major steps in the diagram corresponds to sections in Registering and assigning incident requests as support staff, Resolving and closing incident requests as support staff, and Working with incident requests as a manager, where the steps and their associated tasks are explained in more detail.

Incident Request lifecycle


User contacts service desk
1. Incident Request Registration
2. Incident Request Assignment
Change Management required ?
Yes
To Change Management
No
From Event Management
From Service Level Management
From Capacity Management
From Continuity Management
From Financial Management
Request form submitted by user or specialist
3. Incident Request Tracking
4. Incident Request Resolution by Specialist
To Problem Management
5. Incident Escalation Handling
Yes
Escalation required ?
No
From Change Management
From Release Management
From Continuity Management
6. Incident Request Closure
7. Solution Approval
To Continuity Management
Yes
Recovery at continuity site most efficient way to resolve incident ?
No
To Change Management

Incident management use cases

This topic describes common incident management use cases that you typically encounter as IT support staff. The Calbro Services user personas help to illustrate the use cases and ITIL good practices workflow, however, the use cases do not necessarily make reference to specific Calbro Service sample data.

- Incident resolution with first call resolution
- Incident resolution with assignment to specialist
- Incident request resolution with an emergency change request

Incident resolution with first call resolution

Francie Stafford is a service desk analyst who works on the Calbro Services service desk. She receives a call from Joe Unser, a Calbro Services benefits agents who cannot access one of his key applications, because he is locked out of his user account. Francie creates an incident request, resolves the incident for Joe, and then closes the incident request.

Incident resolution with first call resolution

Role	Tasks and actions	Explanation
Customer	**Contacting the service desk** Joe Unser, the service desk customer, phones Francie Stafford on the service desk	Joe Unser needs to have one of his user accounts unlocked, and calls the service desk to open an incident request.

Service desk analyst	**Registering the incident request record** 1. On the Incident Management console, Francie clicks **Create**, to open a new incident request record. 2. Francie enters the first few letters of Joe's email address on the incident request form and then presses **Enter**. The application matches the email address and fills in part of the incident request record based on the contents of Joe's People record. 3. Francie selects the appropriate template to populate the new incident request record with basic information common to all requests of this type. 4. In the template, Francie sees a set of work instructions that describe how to unlock Joe's account.	Francie Stafford receives Joe's call and, using the Incident Management Best Practice view, creates a new incident request record using the applicable template. For detailed information about how to do this, see Creating an Incident request record using a template. Francie is able to unlock Joe's account while he is on the phone. For detailed information about first call resolution, see First call resolution .
Service desk analyst and Service desk customer	**Closing the incident request** 1. After unlocking Joe's account, Francie asks him to confirm the account has been unlocked successfully by logging into his application. 2. Joe is able to log in, and confirms this to Francie. 3. Francie then enters the resolution in the Work Details tab (Work Info when using the Classic view), makes sure that all other required fields on the incident request record are completed, and then moves the incident request record's **Status** to **Closed**.	While Joe is still on the phone, Francie asks him to confirm that his account is unlocked and that he can log in to his system. Joe confirms this, so Francie updates the resolution field on the incident request record to indicate this. Francie closes the incident request record. For detailed information about closing incident request records, see Closing incident requests.

Incident resolution with assignment to specialist

Francie Stafford receives another call from Joe Unser who, this time, cannot send documents to his local printer. Francie creates an incident request, but cannot resolve it herself. The incident request is automatically assigned to a specialist, Ian Plyment, who accepts the assignment and restores Joe's printer connection. Ian then closes the incident request.

Incident resolution with assignment to specialist

Role	Tasks and actions	Explanation
Service desk customer	**Contacting the service desk** Joe Unser, the service desk customer, phones Francie Stafford on the service desk	Joe Unser cannot send documents to his local printer.

Service desk analyst	**Registering the incident request record** 1. On the Incident Management console, Francie clicks **Create**, to open a new incident request record. 2. Francie enters the first few letters of Joe's email address on the incident request form and then presses **Enter**. The application matches the email address and fills in part of the incident request record based on the contents of Joe's People record. 3. Francie selects the appropriate template to populate the new incident request record with basic information common to all requests of this type. 4. After Francie completes the incident request registration and saves it, the incident request is assigned to an assignment group as specified in the template.	Francie Stafford receives Joe's call and, using the Incident Management Best Practice view, creates a new incident request record from the applicable template. For detailed information about how to do this, see Creating an Incident request record using a template.
Specialist	**Accepting the assignment** 1. On the Incident Management console header, Ian selects his company in the Company field and his support group from the **View By** field. 2. From the Defined searches area, he runs **All Open Unassigned - All Priorities**, which returns all of the open, unassigned incident requests for his support group. 3. Ian selects Joe's incident request and opens it. 4. In the Navigation pane, Ian selects **Assign to Me** and then changes the record's status to **In Progress**.	Ian Plyment is a specialist who works for the support group to which Joe's incident request is assigned. From the Incident Management console, Ian runs a defined search for all open, unassigned incident request for his support group. Joe's incident request is one of the records found by the search. Ian opens the record and accepts the assignment. For more information about how to run a defined search, see Using Search. For more information about how to accept an assignment see Accepting an incident request.

Specialist	**Using Incident Matching to resolve the incident** 1. From the Navigation pane on the incident request record, Ian opens the Incident Matching window. 2. On the Search Criteria Page 1 tab, Ian types **Printer** in the **Summary Keyword Search** field and selects **Connectivity** from the **Operational Categorization Tier 1** menu. 3. He clicks **Search**. Any matching incidents, problem investigations, known errors, and solutions appear in the tabs at the bottom half of the dialog box. 4. Ian views details of the matching records and finds information that helps him resolve incident request. 5. From the **Relationship Type** list on the Incident Matching window, Ian selects **Resolved By** and then clicks **Relate With Solution**. This copies the solution from the matching record to the **Resolution** field of the incident request record.	Ian uses the Incident Matching feature to determine the cause of Joe's incident and resolves it by restoring Joe's printer connection. For more information about using the Incident Matching feature, see To search for matching records-Classic view. This section also discusses other methods to search for possible solutions.
Specialist	**Completing the incident request** 1. On the incident request record, Ian makes sure that all other required fields on the incident request record are completed 2. Ian then moves the incident request record's status to **Resolved** and provides a status reason of **Customer Follow-Up Required**.	Ian is unable to contact Joe directly to determine that his printing service is successfully restored, so he completes the incident request by moving the status to **Resolved** with a status reason of **Customer Follow-Up Required**. Incident Management sends Joe an email asking him to contact the Service Desk to confirm that the incident is resolved. If Joe does not respond within a specific period of time, which is configurable for each installation, the auto close rule moves the incident request's status to **Closed**. For more information about Closing an incident request, including Completing an Incident Request, see Closing incident requests.

Incident request resolution with an emergency change request

This user scenario describes how to resolve an incident request with an emergency change request.
Joe Unser, a Calbro Services benefits agent, cannot access the local area network. He contacts the Calbro Service desk, and Francie Stafford, a service desk analyst, creates an incident request.

The incident request is assigned to Ian Plyment, a specialist in the support group assigned to Joe's company. Ian determines that Joe's data port is broken, and an emergency change is required to restore Joe's service.

Ian contacts Allen Allbrook, the owner of the service, to let him know that an emergency change is required. Allen assesses the risk and authorizes Ian to perform the work.

Ian then replaces Joe's data port and documents his actions in the incident request. Ian verifies with Joe that he can now access the local area network.

Ian closes the incident request and notifies Mary Mann, the change coordinator, of the emergency change so she can register the change. This ensures everyone can see what was changed, should the emergency change cause other incidents to occur. It also ensures that BMC Atrium CMDB is updated.

⚠ **Note**
Incident Management and BMC Change Management must be installed to follow this user scenario.

The following table describes the typical steps involved in this user scenario.

Resolving an incident request with an emergency change

Role	Actions	Explanation
Service desk customer	The customer contacts the service desk.	Joe cannot access the local area network.
Service desk analyst	1. On the Incident console, the service desk analyst registers the incident request record. 2. The analyst uses Incident Matching to search for a solution. 3. When the specialist does not find a solution, the specialist completes the incident request registration and saves the record. The incident request is assigned to an assignment group as specified in the template.	Francie Stafford receives Joe's call and, using the Incident Management Best Practice view, creates a new incident request record from the applicable template.
Specialist	The specialist accepts the assignment: 1. On the Incident console, the specialist searches for incident requests that are assigned to his support group, but not to an individual. 2. The specialist opens the customer's incident request and assigns it to himself. In the work details, the specialist specifies that the incident request is being handled according to the emergency change protocol.	Ian Plyment is a specialist working for the support group that supports Joe's company. Ian searches for all open, unassigned incident requests for his support group. Joe's incident request is one of the records found by the search. Ian opens the record and accepts the assignment. Ian investigates Joe's incident request and determines that his data port is broken. The fix requires an emergency change. Ian contacts Allen Allbrook, the owner of the affected service, to tell him this incident request requires an emergency change. Ian also notes this in the Work Detail tab of the incident request. Allen analyzes the risk and impact of the emergency change request and then authorizes Ian to implement the emergency change.

Specialist	The specialist implements the change and records all work in the incident request. The specialist contacts the customer to verify that the affected service has been restored. The specialist closes the incident request.	After the change is implemented and verified, Ian closes the incident request and asks Mary Mann, the change coordinator, to register a change for this emergency change. This ensures everyone can see what was changed, in case the emergency change causes incidents to occur. This also makes sure that Allen, the service owner, is informed and BMC Atrium CMDB is updated.
Change coordinator	1. The change coordinator creates an emergency change request. 2. From the Incident form, the change coordinator creates a change request. This opens the Change Request form and copies information from the incident request record to the change request record.	From Joe's incident ticket, Mary creates the emergency change request. By creating the request from the incident request, much of the information is copied directly from the incident request record to the change request record. This saves time and ensures accuracy. While creating the emergency change request, Mary creates a relationship between Joe's incident request and the emergency change request.

Problem management processes

This topic describes some of the problem management process that you can manage using the Problem Management feature of BMC Service Desk.

- Process flow and the lifecycle of a problem investigation
- Problem management use cases

Problem management process flow video

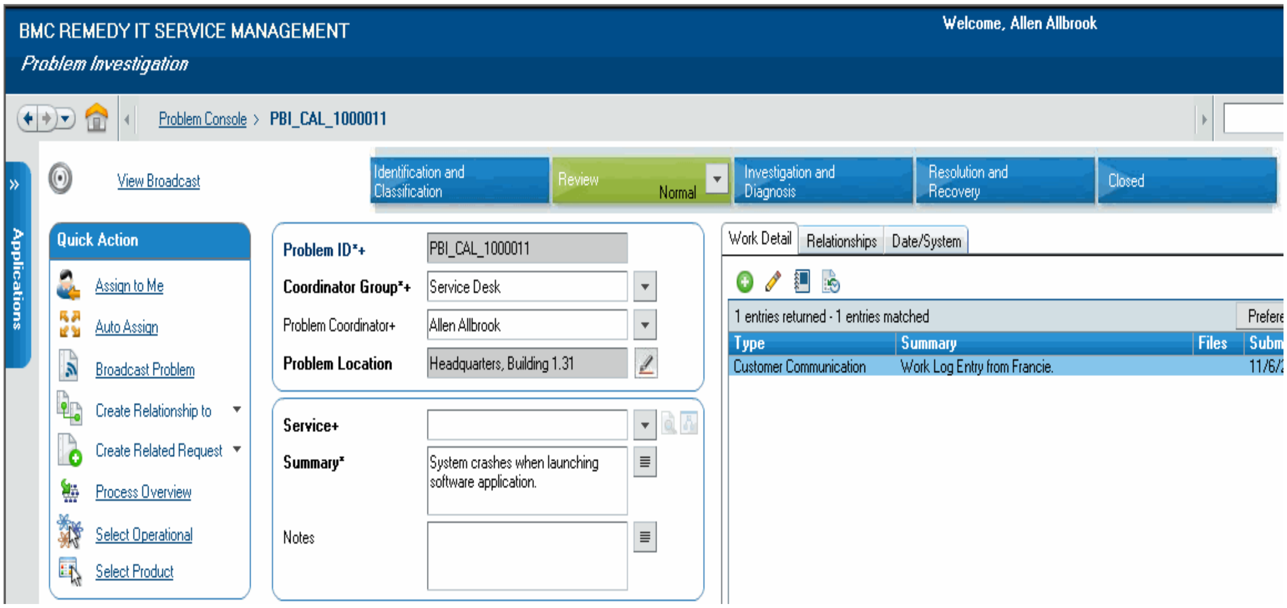
Watch the following video to learn about the basic flow of the problem management process.

> **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

Process flow and the lifecycle of a problem investigation

The Process Flow Status area displays the process flow of the problem investigation within the Problem Investigation form. A diagram shows the stages of a problem investigation in blue. The current stage of the investigation is highlighted in green. The status of the investigation is indicated both by color and text. Process Flow Status area on the Problem Investigation form

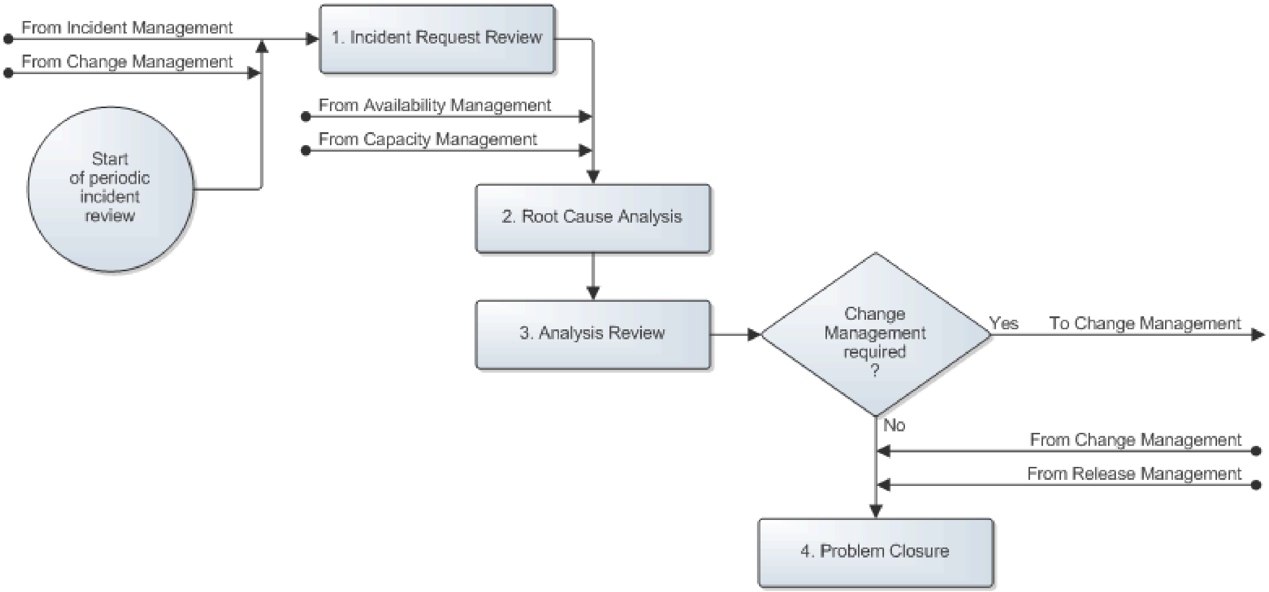


Problem ID*+	PBI_CAL_1000011
Coordinator Group*+	Service Desk
Problem Coordinator+	Allen Allbrook
Problem Location	Headquarters, Building 1.31
Service+	
Summary*	System crashes when launching software application.
Notes	

1 entries returned - 1 entries matched

Type	Summary	Files	Subm
Customer Communication	Work Log Entry from Francie.		11/6/

The following figure provides an overview of the problem investigation lifecycle.



Problem management use cases

This topic describes common problem management use cases that you typically encounter as IT support staff. The Calbro Services user personas help to illustrate the use cases and overall ITIL good practices workflow; however, the use cases do not necessarily make reference to specific Calbro Service sample data.

- Problem investigation resolution with a change request
- Problem investigation resolution without a change request
- Problem investigation resolution using a change request roll back
- Indicating a problem investigation at an impasse

Problem investigation resolution with a change request

This user scenario describes how to resolve a problem investigation with a change request.
Bob Baxter, the Calbro problem coordinator, conducts an incident request review on the Calbro Order Processing System (OPS). In the course of the review, Bob discovers that several similar incidents related to the OPS occurred over the past six months. The resulting problem investigation determines that a change to the IT infrastructure is required. A known error is created making a request for change (RFC), which is assigned to Mary Mann, the change coordinator. The change is approved by Mary, executed and verified by Ian Plyment, the specialist. The status of the Known Error is automatically marked as **Corrected**.
Bob is notified that the change request has been completed. He notes the permanent corrective action in the problem investigation and changes its status to **Closed**.

> ⚠ **Note**
> Incident Management, Problem Management, and BMC Change Management must be installed to follow this user scenario.

The following table describes the typical steps involved in this user scenario:
Resolving a problem investigation with a change request

Role	Actions	Explanation
Problem coordinator	The problem coordinator performs an incident request review: From the Incident console, the problem coordinator creates a custom search that has the following characteristics: • `Service = OPS` • `Impact => 2-Significant/Large OR 1-Extensive/Widespread` • `Last Resolved Date >= 07/19/2009`	For the purpose of this example, assume today's date is 01/19/2010. The Last Resolved Date used in this example, therefore, is six months ago. After running the search, the problem coordinator looks for incident request records that have not yet been linked to a problem investigation. The problem coordinator, Bob Baxter, performs an incident request review on the OPS by querying the Incident Management system for incidents or recent changes related to the OPS. Bob discovers that over the past six months there were several similar incidents related to the OPS.
Problem coordinator	1. From one of the incident request records that is related to the OPS server issue, the problem coordinator creates a problem investigation. 2. The incident record's details are copied from the incident request record to the Problem form, and a relationship is created between the problem investigation record and the incident request records. 3. The problem coordinator completes the Problem form.	Bob wants to determine the root cause of these incidents, so he creates a problem investigation from one of the incident request records. Creating the problem investigation from an incident request record ensures that all of the relevant details are copied over from the incident request to the problem investigation.

Problem coordinator	1. From the Problem form, the problem coordinator creates relationships between the problem investigation and all related incident requests. 2. The problem coordinator creates a relationship between the problem investigation and the OPS server.	Bob then relates the remaining OPS incidents and the OPS CI to the problem investigation.
Problem coordinator	The problem coordinator assigns the problem investigation to the specialist.	Bob assigns the problem investigation to the specialist, Ian Plyment, to conduct a root cause analysis.
Specialist	The specialist accepts the assignment and performs the root cause analysis.	Ian accepts the problem investigation assignment and begins a root cause analysis. During the root cause analysis, he determines the physical server on which the OPS runs needs a memory upgrade and sends his root cause analysis to Bob.
Problem coordinator	The problem coordinator performs the analysis review by opening the problem investigation and independently verifying that the specialist's assessment of the root cause is correct.	Bob reviews and verifies Ian's analysis. Bob then creates a Known Error, which serves two purposes: to identify the best workaround (temporarily routing the users to a redundant server) and to request a change for the memory upgrade on the primary OPS server.
Problem coordinator	The problem coordinator creates a known error: 1. On the problem investigation form, the problem coordinator sets the **Status** field to **Completed** and the **Status Reason** field to **Known Error** . 2. This opens the Known Error form and creates a relationship between the known error and the problem investigation. 3. The problem coordinator completes the form. The problem coordinator assigns himself as the problem coordinator. The problem coordinator assigns the change coordinator for the known error assignment.	Bob creates the known error directly from the problem investigation, which transfers all pertinent information to the known error. Bob assigns the known error to Mary Mann, the change coordinator.

Change coordinator	1. From the Known Error form, the change coordinator creates a change request. This opens the Change Request form and creates a relationship between the known error and the change request. It also copies information from the known error record to the change request record. 2. The change coordinator saves the change request and moves the request through the change request lifecycle until the change request is approved and has a date.	Mary receives the known error and reviews it. She agrees that the change is required and creates a change request from the known error. Mary moves the record through the change request lifecycle.
Change coordinator	1. The change coordinator assigns the change request to a specialist. 2. The change coordinator adds a task to the change request and relates the CIs to the change request. 3. The change coordinator moves the change request to the Implement stage.	On the change request record, Mary creates a task to implement the change, and assigns the change request to Ian Plyment, the specialist who will perform the work. The coordinator also relates the CI to the change request.
Specialist	The specialist performs the tasks and closes them: 1. On the Change Management Support console, the specialist searches for assigned tasks. 2. The specialist opens the task record and performs the task. Then the specialist records information about performing the task and changes the status of the task to **Closed**.	Ian implements the change. When he finishes the last task, the system notifies Mary that the tasks are closed.

Change coordinator	The change coordinator completes the change request: 1. From the Change form, the change coordinator moves the change request to the Close stage. 2. The change coordinator enters the performance rating and the actual start and end dates.	After Mary coordinates the change implementation, she reassigns the known error to Bob for verification.
Problem coordinator	The problem coordinator confirms that the change has solved the problem. Then, the problem coordinator sets the status of both the problem investigation and the known error to **Closed**.	Bob is notified that the change was completed and verifies that it fixed the problem. He then changes the status of the problem investigation and known error to **Closed**.

Problem investigation resolution without a change request

This user scenario describes how to resolve a problem investigation without a change request.
Bob Baxter, the problem coordinator for the Calbro Services Payroll service, conducts a incident request review on this service. In the course of the review, Bob discovers that multiple incidents related to performance have occurred over the past six months. Bob assigns the problem investigation to a specialist, Ian Plyment. Ian's problem investigation determines that the anti-virus software on the Payroll service server runs a complete scan of the server every ten minutes. Ian reconfigures the anti-virus software to run only once an hour. Ian then notifies Bob that he has implemented a corrective action to solve the root cause. Bob verifies the corrective action and closes the problem investigation.

> ⚠ **Note**
> Incident Management and Problem Management must be installed to follow this user scenario.

The following table describes the typical steps involved in this user scenario: **Resolving a problem investigation without a change request**

Role	Actions	Explanation

Problem coordinator	The problem coordinator performs an incident request review. From the Incident console, the problem coordinator creates a custom search with the following characteristics: • `Service = Payroll` • `Impact => 2-Significant/Large OR 1-Extensive/Widespread` • `Last Resolved Date >= 07/19/2008` For the purpose of this example, assume today's date is 11/19/2008. The Last Resolved Date used in this example, therefore, is six months ago.	Bob performs an incident request review by searching incident requests registered against the services for which: • He is the problem coordinator. • That have not yet been linked to a problem investigation. • That have been resolved with a workaround.
Problem coordinator	The problem coordinator opens one of the incident request records related to the Payroll service performance issue, and creates a problem investigation. The incident record's details are copied from the incident request record to the Problem form, and a relationship is created between the problem investigation record and the incident request records. The problem coordinator completes the Problem form.	Bob spots a trend-numerous performance-related incidents have been reported against the Payroll service. Bob creates a problem investigation record directly from one of the incident request records. Creating a problem investigation directly from an incident request record transfers all relevant information from the incident request and automatically establishes the relationship between the incident request and the problem investigation.
Problem coordinator	The problem coordinator relates all the related incident requests to the problem investigation.	Bob then relates the other incident requests to the problem investigation.
Problem coordinator	The problem coordinator assigns the problem investigation to a specialist.	After creating the problem investigation, Bob assigns it to the specialist, Ian Plyment.
Specialist	The specialist accepts the assignment and performs the root cause analysis.	Ian accepts the problem investigation assignment and begins a root cause analysis. During the root cause analysis, he determines the anti-virus software on the server runs every ten minutes, which is causing the performance issues. Ian determines the more appropriate frequency for the anti-virus software to run is once an hour.
Specialist	1. The specialist implements the solution by changing the problem investigation status to Completed and changing the status reason to Enhancement Request. 2. The specialist then records details about the investigation.	Because the changes to the anti-virus software configuration do not meet the criteria for the change management process, Ian makes the necessary changes himself and then changes the status of the problem investigation to Completed. To complete the problem investigation, Ian must select a status reason.

Specialist	1. The specialist notifies the problem coordinator. 2. The specialist confirms that the problem coordinator is set as the assigned problem coordinator. Then the specialist changes the status of the problem investigation to Assigned.	Ian notifies Bob about the results of the problem investigation and the corrective action he performed.
Problem coordinator	The problem coordinator performs the analysis review: On the problem investigation form, the problem coordinator reviews the work information and independently verifies that the changes have corrected the problem.	Bob performs an analysis review and double-checks that the problem has been corrected.
Problem coordinator	The problem coordinator closes the problem investigation: The problem coordinator reviews the problem investigation form to verify that the details are complete. When the problem coordinator is satisfied that the problem investigation form is complete and correct, the problem coordinator changes the status to Closed.	Bob closes the problem investigation.

Problem investigation resolution using a change request roll back

This user scenario describes how to resolve a problem investigation by rolling back a change request.
Bob Baxter, the problem coordinator at the Calbro Service Desk, performs an incident request review by searching incident requests registered against the payroll service. He reviews the history of the associated CIs and recognizes a trend in problems that are related to common changes to a specific CI. He creates a change request to roll back changes that affect that CI. A Request for Change (RFC) is submitted to Mary Mann, the change manager in Front Office Support, for approval.
The change is approved and successfully implemented by Ian Plyment, the Specialist. The change manager creates a Broadcast to alert users. Future incidents are successfully averted.

> **Note**
> Incident Management, Problem Management, and BMC Change Management must be installed to follow this user scenario.

The following table describes the typical steps involved in this user scenario: **Rolling back a change**

Role	Actions	Explanation

Problem coordinator	The problem coordinator performs an incident request review: From the Incident console, the problem coordinator creates a custom search with the following characteristics: • `Service = Payroll` • `Impact => 2-Significant/Large OR 1-Extensive/Widespread` • `Last Resolved Date >= 07/19/2009` For the purpose of this example, assume today's date is 11/19/2009. The Last Resolved Date used in this example, therefore, is four months ago. The problem coordinator looks for incident request records that have not yet been linked to a problem investigation.	Bob performs an incident request review by searching incident requests registered against the payroll service, for which he is the problem coordinator.
Problem coordinator	1. The problem coordinator opens an incident request that is related to the payroll service and creates a problem investigation. 2. The incident record's details are copied from the incident request record to the Problem form, and a relationship is created between the problem investigation record and the incident request records. 3. The problem coordinator completes the Problem form.	Bob spots a trend-numerous incidents have been reported against the payroll server CI, which is critical to making that service available. He also discovers that the server recently was the subject of a change. Bob reviews the change related to the server and determines that the recent change to the CI was the root cause of those incident requests. Bob creates a problem investigation record directly from one of the incident request records, which transfers all relevant information from the incident request and automatically establishes the relationship between the incident request and the problem investigation.
Problem coordinator	1. The problem coordinator creates relationships between the problem investigation and all of the related incident requests. 2. The problem coordinator creates a relationship between the problem investigation and the original change request that is responsible for triggering the incident requests.	Bob then relates the other incident requests, the original change request, and the CI to the problem investigation.

Problem coordinator	The problem coordinator creates a known error: 1. The problem coordinator sets the **Status** field to **Completed** and the **Status Reason** field to **Known Error**. 2. This opens the Known Error form and creates a relationship between the known error and the problem investigation. 3. The problem coordinator completes information on the form. The problem coordinator enters his name as the assigned problem coordinator. The problem coordinator enters the change coordinator's name as the known error assignee, and sets the status to Assigned.	Bob determines that the best way to prevent similar incident requests from recurring is to roll back the original change. To request the rollback, Bob creates a known error from the problem investigation. He assigns the known error to Mary Mann, the change coordinator.
Change coordinator	1. The change coordinator opens the known error record and creates a change request. 2. This opens the Change Request form and creates a relationship between the known error and the change request. It also copies information from the known error record to the change request record. 3. The change coordinator completes the required information and saves the change request. 4. The change coordinator moves the change request through the lifecycle until it is approved and the dates are set. 5. To alert users about the rollback, the change coordinator creates a broadcast.	Mary receives the known error and reviews it. She agrees that the rollback is required and creates a change request from the known error. Mary moves the record through the change request lifecycle. As part of the change request, the change coordinator creates a broadcast alerting users to the incorrect original change and the symptoms in the defective CI. The broadcast mentions the new change and the time when the CI will be unavailable-while the change is being executed. Finally, the broadcast explains that the change was necessary to avoid further incoming related incidents.

Change coordinator	1. The change coordinator assigns the change request to a specialist. 2. The change coordinator adds a task to the change request. 3. The change coordinator relates the CIs to the change request. 4. The change coordinator moves the change request to the Implement stage.	On the change request record, Mary creates a task to roll back the CI and assigns the change request to Ian Plyment, the specialist who will perform the work. The coordinator also relates the CI to the change request.
Specialist	The specialist closes the tasks after performing them: 1. From the Change Management Support console, the specialist searches for assigned tasks. 2. After performing the task, the specialist records information about performing the task and changes the status to Closed.	Ian rolls back the change to the CI. When he finishes the last task, the system notifies Mary that the tasks are Closed.
Change coordinator	The change coordinator completes the change request: 1. The change coordinator moves the change request to the Closed stage. 2. The change coordinator enters the performance rating and the actual dates of the change.	Mary completes the change request record and removes the broadcast, because it is no longer relevant.

Problem coordinator	The problem coordinator closes the problem investigation and known error: 1. The problem coordinator confirms that the rollback has solved the problem with the payroll server. 2. The problem coordinator opens the problem investigation record and checks that the details are all correct, and then sets the status to **Closed**. 3. The problem coordinator opens the known error and sets the status to closed. The problem coordinator records a summary of how the known error was resolved.	Bob is notified that the rollback was completed. Bob verifies that the rollback fixed the problem, and then changes the status of the problem investigation and known error to closed.

Indicating a problem investigation at an impasse

This user scenario describes how to indicate a problem investigation at an impasse.
During Bob Baxter's incident request review of the Calbro Payroll service, he discovers also that over the past six months multiple incident requests have been registered related to slow searches against the Payroll service database. Bob assigns the problem investigation to Ian. Ian's problem investigation finds a defect in the database management software that might be corrected by a future patch. Ian notes the root cause, but because a permanent solution in not yet available, he moves the problem investigation status to Pending. Bob performs periodic checks against problem investigations with a status of Pending, to see if permanent solutions have become available.

> ⚠ **Note**
> Incident Management and Problem Management must be installed to follow this user scenario.

The following table describes the typical steps involved in this user scenario:
Indicating a problem investigation at an impasse

Role	Actions	Explanation

Problem coordinator	The problem coordinator performs an incident request review: From the Incident console, the problem coordinator creates a custom search that has the following characteristics: - `Service = Payroll` - `Impact => 2-Significant/Large OR 1-Extensive/Widespread` - `Last Resolved Date >= 07/19/2009` For the purpose of this example, assume today's date is 11/19/2009. The **Last Resolved Date** used in this example, therefore, is six months ago.	Bob performs an incident request review by searching incident requests registered against services with the following characteristics: - For which Bob is the problem coordinator. - That have not yet been linked to a problem investigation. - That were resolved with a workaround.
Problem coordinator	1. The problem coordinator opens an incident request record that is related to the Payroll service search issue and creates a problem investigation. 2. The incident record's details are copied from the incident request record to the Problem form, and a relationship is created between the problem investigation record and the incident request records. 3. The problem coordinator completes the Problem form.	Bob spots another trend-numerous incidents have been reported against the Payroll service related to the length of time it takes to run a search against the database. Bob creates a problem investigation record directly from one of the incident request records. Creating a problem investigation directly from an incident request record transfers all relevant information from the incident request and automatically establishes the relationship between the incident request and the problem investigation.
Problem coordinator	The problem coordinator relates all the related incident requests to the problem investigation.	Bob then relates the other incident requests to the problem investigation.
Problem coordinator	The problem coordinator assigns the problem investigation to a specialist.	After creating the problem investigation, Bob assigns it to Ian.
Specialist	The specialist accepts the assignment and performs the root cause analysis.	Ian accepts the problem investigation assignment and begins a root cause analysis. During the root cause analysis, he determines that the problem is with a defect in the database management software. Ian also determines that none of the database management software patches fixes this problem. The problem might be fixed in a future release.

Specialist	1. The specialist notifies the problem coordinator. 2. The specialist verifies that the problem coordinator is assigned as problem coordinator. 3. The specialist changes the problem investigation status to Assigned.	Ian notifies Bob that he has completed the root cause analysis and determined the problem is with the database management software. He also tells Bob that, currently, no patch from the database software vendor fixes the problem.
Problem coordinator	1. The problem coordinator performs the analysis review by reviewing the work information recorded on the problem investigation. 2. The problem coordinator independently verifies that the specialist's assessment of the impasse is correct.	Bob performs an analysis review and double-checks that Ian's assessment of the situation is correct.
Problem coordinator	1. The problem coordinator indicates that the problem investigation is at an impasse. 2. The problem coordinator indicates why no further action can be taken against the investigation and changes the problem investigation status to **Pending**.	Because no current fix for the root cause is available, Bob determines that the problem investigation is at an impasse.
Problem coordinator	Periodically, the problem coordinator checks the problem investigations with a status of **Pending**. • If a solution is now available, the problem coordinator reassigns the problem investigation to a specialist for follow-up and implementation. • If a solution is still unavailable, the problem coordinator records information about the periodic check.	Bob performs periodic checks of all problem investigations with a status of Pending to determine if a solution has become recently available.

User roles

This section provides a list of various user types and how they interact with the product.

- Incident Management user roles
- Problem Management user roles

Incident Management user roles

This topic describes end user roles for the Incident Management feature of the BMC Service Desk application. It contains information about the following roles:

- Support staff
- Manager
- User
- Requester Console

Support staff

For the incident management process, the BMC Service Management Process Model defines the following support staff roles.

Service Desk Analysts are usually first-line support staff. A Service desk analyst's responsibilities include:

- Providing the interface between the service owner organization and its customers
- Obtaining accurate and complete information from the user when creating the incident request, and doing so efficiently and accurately
- Resolving as many of their registered incident requests as possible within the limitations of their access rights and their time constraints
- Ensuring that the incident requests that they have registered, but which they are unable to resolve, are assigned to the most appropriate group for resolution
- Validating incident request resolutions with their users

Specialists are usually second-line and third-line support staff. They are considered subject matter experts. Their main responsibility is to provide an accurate analysis and a diagnosis of their assigned incident requests to restore service to the affected users. A specialist's responsibilities include:

- Resolving incident requests
- Updating incident requests with relevant information and status changes
- Escalating incident requests, for which resolutions can be implemented only through the change management process, to the owner of the affected service

Manager

For the incident management process, the BMC Service Management Process Model defines the following management roles.

Group coordinators are responsible for the quality and integrity of the incident management processes and for the work of their support group members. They coordinate the assignment of incident requests to support staff. The group coordinator's other responsibilities include:

- Monitoring incidents
- Monitoring open incidents requiring assignment
- Managing the assignment of incidents to their appropriate support groups for resolution
- Receiving notifications of incident assignments and escalations
- Facilitating the resolution of escalated incidents in accordance with the escalation policy
- Ensuring the resolution of incidents within the support group's service targets
- Ensuring the overall completeness and accuracy of closed incidents
- Reviewing reports
- Ensuring that incidents requiring root cause analysis are copied into Problem Management
- Managing support group membership
- Managing scripts, templates, and decision trees

On-Duty managers take over the responsibility from service owners when the owner is not available to perform the incident escalation handling procedure. In these situations, the on-duty manager decides whether an escalated incident must be resolved by implementing an emergency change, by recovering the affected service at its continuity site, or by continuing the resolution of the incident within the incident management process.

Service owners create and assign incident requests. They also decide whether an escalated incident needs to be resolved by implementing an emergency change, by recovering the affected service at its continuity site, or by continuing the resolution of the incident within the incident management process.

User

A user is usually an employee who needs assistance from the IT support staff to resolve an incident or implement a change. Anyone in your organization can be a user.

The incident user's responsibilities include:

- Requesting support when necessary and providing the required information to help resolve the incident requests. They submit requests by filling out the Request form, or by contacting the service desk by email or telephone.
- Verifying the solution provided by the service owner organization and reopening the incident request if the solution is not acceptable

Requester Console

Users of the Requester Console are usually employees who need assistance from the IT support staff. The user or requester is typically an employee in the organization who must have a change implemented or an incident resolved. But any member of your organization can be a requester.

However, the user *might* not be an employee. Non-employees can also be requesters, since non-registered users can also submit service requests. Traditionally, after a requester made a telephone call to a central help desk, a support staff member logged the request.

BMC Service Desk: Incident Management and BMC Change Management provide user self-provisioning. Using the Requester Console, requesters can submit, track, and (in some cases) resolve their own requests, and, as a result, improve the overall efficiency.

BMC Change Management and BMC Service Desk: Incident Management are preconfigured to work with the Requester Console. However, an organization can set an option to make the Requester Console unavailable.The Requester Console is the primary interface for requesters to define and view their requests. From the Requester Console, you can define a request that is submitted to BMC Change Management or BMC Service Desk: Incident Management. You can also view requests and respond to a survey after the request has been resolved.

Problem Management user roles

This section describes the end user roles for the Problem Management feature. It contains information about the following roles:

- Problem coordinator
- Specialist

Problem coordinator

Problem coordinators are responsible for the quality and integrity of the problem management process. Problem coordinators have full access to problem investigations, known errors, and solution entries assigned to their support groups.

> ⚠ **Note**
> Problem coordinators require at least the permission of Problem User to access Problem Management. In addition, they must have the functional role of Problem Coordinator to perform the problem coordinator's duties.

Their responsibilities include:

- Reviewing the incident requests that have been related to the services for which they act as the problem coordinator, to help identify problems
- Ensuring that the problems for which they are responsible, including the ones that have been identified within the Availability and Capacity Management processes, progress through the problem management process in a timely and prioritized fashion
- Ensuring that the information entered in the problem investigations and known errors that they manage is accurate and complete
- Reviewing periodically their problem investigations for which a practical structural solution can not be found
- Verifying structural solutions and closing the known errors and problem investigations that they manage

Specialist

Specialists work on problem investigations, known errors, and solution entries as assigned. Their responsibilities include:

- Suggesting workarounds for problems
- Establishing the root causes of identified problems
- Proposing structural solutions (that is, permanent solutions) for problems
- Implementing structural solutions for problems if the Change Management process is not required
- Updating the problem investigation with relevant information and status changes

Individuals fulfilling the role of a specialist require Problem User permissions to access the Problem Management feature. Permissions are assigned to individuals by the system administrator.

For more information about Problem Management permissions, see Problem Management permissions.

Architecture

This section describes the BMC Remedy IT Service Management (BMC Remedy ITSM) architecture, including its relationship to BMC Remedy Action Request System server (BMC Remedy AR System server) and BMC Atrium Core. It also provides the following information:

- Organization of modules, applications, and subsystems
- Deployable application structure model
- Foundation
- Categorization
- Assignment architecture
- Required Resolution Date and Target Date fields
- Requester console architecture
- Command Automation Interface
- Notification engine
- Changes to the BMC Atrium CMDB for BMC Remedy ITSM

A database forms the underlying element of the BMC Remedy ITSM architecture. The BMC Remedy AR System server is on top of the database. BMC Remedy AR System server processes all data entered by BMC Remedy ITSM applications. In addition, the BMC Remedy AR System server is the workflow engine between the BMC Remedy ITSM applications and the database. It also verifies that a user has permission to perform each action, thereby enforcing any access control defined in the applications.

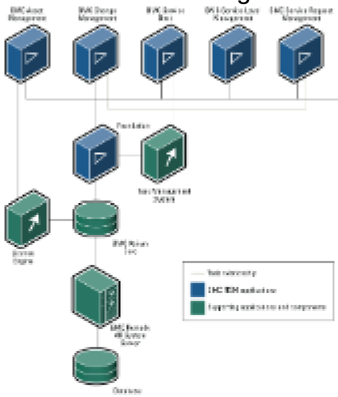
In this capacity, the BMC Remedy AR System server is the interface between the database and the BMC Atrium Core, which includes the Product Catalog and BMC Atrium Configuration Management Database (BMC Atrium CMDB). BMC Atrium CMDB stores information about the configuration items (CIs) in your IT environment and the relationships between them. BMC Atrium CMDB makes this information available to the BMC Remedy ITSM applications and their various shared application components, such as the Task Management System.

The BMC Remedy AR System server also manages the following:

- The BMC Remedy Approval Server is a self-contained, shared module that enables you to automate any approval or signature process. For more information about BMC Remedy Approval Server, see Adding approvals to an application.
- The BMC Remedy Assignment Engine enables you to automatically assign requests to individuals. For more information about BMC Remedy Assignment Engine, see Assigning requests with the Assignment Engine.

The relationships among the database, BMC Remedy AR System server, BMC Atrium Core, shared application components, and the BMC Remedy ITSM applications are shown in the following illustration.

BMC Remedy ITSM architecture
Click on the following illustration to enlarge it.



Related topics

BMC Atrium Core architecture and features

BMC Remedy AR System and components architecture

Organization of modules, applications, and subsystems

The overall organization of the BMC Remedy IT Service Management (BMC Remedy ITSM) Suite has three layers: modules, applications, and supporting subsystems.

The top layer consists of modules that provide the interface to users, such as the Requester console. The Requester console interacts with a back-office application, such as the Incident Management feature of BMC Service Desk or BMC Change Management.

Applications include the main BMC Remedy ITSM applications: Incident Management feature of BMC Service Desk, BMC Change Management, Problem Management feature of BMC Service Desk, and BMC Asset Management. These applications contain logic and user interfaces specific to those application areas.

The final layer consists of supporting systems. This common set of systems supports the applications. Supporting systems contain generic logic that is specific to an application's function without embedding functionality from other applications that use its services. Examples of supporting systems include Task Management System, Cost module, and Contract Management.

The following figure illustrates the relationships among the BMC Remedy ITSM applications and modules.

BMC Remedy ITSM applications and modules
Click the following image to expand it.

Deployable application structure model

The BMC Remedy Action Request System (BMC Remedy AR System) platform provides the structural component used in the BMC Remedy IT Service Management (BMC Remedy ITSM) applications to define the *deployable application* architectural structure. Deployable applications provide functions that support a component architectural model:

- Licensing enforcement
- Encapsulation of permissions
- Definition of entry points
- Ability to import and export as a whole component

Deployable applications are used to wrap each of the different applications and modules that are provided in BMC Remedy ITSM applications. Deployable applications contain applications, modules, and helper components.

Applications:

- BMC Incident Management (licensed)

- BMC Problem Management (licensed)
- BMC Change Management (licensed)
- BMC Asset Management (licensed)

Modules:

- Cost Module (licensed)
- TMS
- BMC Change Management Dashboards (licensed)
- Application Administration Console
- Reporting Console
- Requester console

Helper components:

- Foundation elements
- Foundation components, such as message boxes and so on
- Site
- Company
- BMC Atrium Product Catalog

Foundation

The Foundation module contains the common forms, workflow, and data that are needed to support the applications.

It also provides a repository for the following data structures used by each BMC Remedy IT Service Management (BMC Remedy ITSM) application:

- Organization
- People
- Support groups
- Categorization (both organizational categorization and general categorization)

> ⚠ **Note**
> With version 7.5, the following structures were moved from BMC Remedy ITSM to BMC Atrium Core:
>
> - Company (tenancy definition and external company definition)
> - Location
> - Categorization (product categorization)

Categorization

Categorization structures in BMC Remedy IT Service Management (BMC Remedy ITSM) are divided into two distinct components: *operational categorization* and *product categorization*.

Operational categorization is a three-tier structure that helps you to define the work that is being done for a particular incident, problem, known error, change request, release request, or task. This structure is also used to qualify reporting in the system, qualify how groups and support staff get assigned, and route approvals.

Product categorization is a three-tier structure that helps you to define a description of the object or service on which you are performing the work (for example, Hardware, Peripheral Device, Monitor).

Assignment architecture

The assignment architecture for the BMC Remedy IT Service Management (BMC Remedy ITSM) Suite is based on a two-phase concept. The first phase is assignment of the support group; the second phase is assigning the support technician using load balancing technology built into the BMC Remedy Action Request (BMC Remedy AR System) Assignment Engine.

Phase 1: Support groups

The support group assignment phase is done using BMC Remedy AR System workflow on back-end forms, using four different inputs:

- Organization
- Location
- Operational categorization
- Product categorization

The Assignment form defines the events in which assignment needs to occur. These events are based on the calling application's assignment needs. For example, the BMC Remedy Change Management application requires assignment for the change coordinator and the change manager.

Assignment rules are partitioned based on tenancy that has been defined. Each operating company can have its own set of assignment rules.

Phase 2: Individual assignment

Individual assignment is done using the Assignment Engine. Assignment rules are provided to support Number of Tickets Assigned, Round Robin, and Capacity process rules:

- **Number of Tickets Assigned** assigns the request based on the person who has the lowest number of requests assigned.
- **Round Robin** assigns the request to the next person in line.
- **Capacity** uses a formula of the number of requests assigned and a capacity factor to determine total capacity, and assigns the request to the user with the lowest capacity rating.

Related topic

Assigning requests with the Assignment Engine

Required Resolution Date and Target Date fields

The Required Resolution Date field on the Help Desk form maps to the Date Required field on the Requester console. The customer can use this field to specify the date or time by which they need the request to be fulfilled. This is the suggested date or time that the customer would like the request to be fulfilled. There is no service level workflow related to this field.

The Target Date field is the date or time by which the request must be resolved, according to the service level agreement targets. The Target Date field is set by the BMC Service Level Management application when service level agreement targets are defined. If service level agreement targets are not defined, then you must set the Target Date manually.

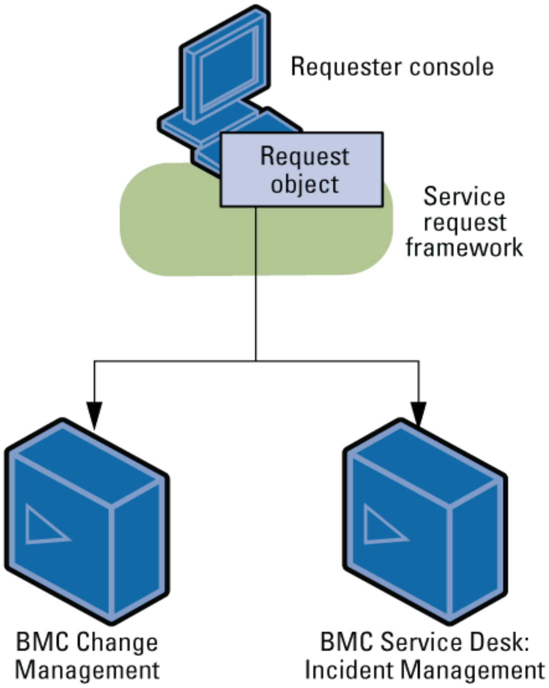
Requester console architecture

If BMC Service Request Management is not available, the Requester console is the customer-facing, user interface of the BMC Change Management and Incident Management feature of BMC Service Desk applications. It is a single entry point where users of these applications can submit a change request or report an incident.

⚠ **Note**
The BMC Service Request Management application provides a richer set of features and functions than the Requester console. If BMC Service Request Management is implemented, it is used instead of the Requester console as the customer-facing interface.

The service request entity serves as a bridge and is not designed to be managed by service desk personnel. It is a "slave" to the back-end change request or incident with its lifecycle completely driven by the back-end. The Requester console is the front-end entry point for users to submit requests. The following figure illustrates the underlying Requester console framework.

Requester console diagram


Requester console
Request object
Service request framework
BMC Change Management
BMC Service Desk: Incident Management

The Requester console is a simplified interface for users to submit change requests and incident requests. This enables users to submit requests into the system from a single console, without having to access the BMC Change Management or BMC Incident Management consoles directly. The targeted audience is non-IT user requesters.

Service request framework

The Requester console is supported by the service request framework, which implements the service request component for integration with the BMC Change Management and Incident Management applications.

The service request framework provides a bridge between the front-end user requests and the back-end operations. In BMC Remedy IT Service Management (BMC Remedy ITSM), integrations are implemented to BMC Change

Management and BMC Service Desk: Incident Management. In addition, the service request framework provides a structure that can be connected to other open back-end solutions.

The service request framework:

- Segments front-end transactions from back-end transactions
- Acts as a bridge between the Requester console front-end interface and BMC Change Management and BMC Service Desk: Incident Management back-end applications
- Supports synchronization between the front-end interface and back-end object life cycle
- Establishes a foundation to support integration with back-end applications
  - Integrates to BMC Change Management and BMC Service Desk: Incident Management as the back-end applications
  - Provides a mechanism for establishing field mappings between the request entity and change request or incident, for request creation
  - Provides CAI as a bi-directional communication mechanism for back-end integrations
- Integrates with BMC Service Level Management for requester-focused service level agreements (SLA) tracking

Date Required and Target Date fields

The Required Resolution Date field on the Help Desk form maps to the Date Required field on the Requester console. The customer can use this field to specify the date or time by which they need the request to be fulfilled. This is the suggested date or time that the customer would like the request to be fulfilled. There is no service level workflow related to this field.

The Target Date field is the date or time by which the request must be resolved, according to the service level agreement targets. The Target Date field is set by the BMC Service Level Management application when service level targets are defined.

Command Automation Interface

The Common Automation Interface (CAI) module provides a common infrastructure that can be shared across applications including BMC Remedy IT Service Management (BMC Remedy ITSM) applications and the BMC Configuration Automation for Clients application.

This section provides the following information:

- CAI plug-in
- Phases of use with TMS

The CAI provides event delivery to the target applications. CAI is a back-end component that does not provide a front-end user interface. Additional user dialogs can be defined for each integrated component to push data into the CAI forms. The functionality of CAI is based on the current implementation for SRMS framework command events and the requirements of the Task Management System (TMS) and Data Management.

The following table lists the functionality that CAI provides for each application or module:

Functionality provided by the CAI

Application or module	Functionality provided by CAI

Task Management System (TMS)	- Communication with BMC Remedy ITSM applications - Integration with the BMC Configuration Automation for Clients application
BMC Change Management	Integration with BMC ProactiveNet Performance Management
Service request framework (support for the Requester console)	Communication with BMC Remedy ITSM applications
Data Management	Multi-threading

CAI plug-in

The primary purpose of the CAI plug-in is to transmit events to other back-end applications.

Due to the dynamic nature of the field mappings for each command, and because it is not possible to use workflow to push values to dynamic fields, the CAI plug-in provides a mechanism to dynamically map data to fields. For example, the command to generate a back-end request consists of dynamic field values that can be mapped to any field on the back-end interface forms. Additionally, the CAI plug-in helps address problems that arise with incompatible permission models.

Phases of use with TMS

This topic provides an overview of how the CAI module is used by the Task Management System (TMS).

Definition phase: Application registration and command definition

Application registration defines the integration attributes to the external applications, such as application name, connection information, and interface form names.

Command definition describes the commands and the command parameters for each integrated component. For example, the Requester console has defined a set of commands for interaction with back-end applications. In TMS, a set of commands is defined for interaction with BMC Configuration Management. In addition, the CAI can include command parameter mappings to the registered applications.

Construction phase: Instantiation of the command definition as events

Command events are instantiated based on the command definitions. The event is constructed using the specific command name, and the command parameter values are populated by the integrated components. CAI provides the form structure and generic workflow for command instantiation. Each integrating component must implement the workflow to control its specific commands.

Execution phase: Event delivery

The mechanism that delivers the command events to the target system depends on the protocol used.

- AR protocol — The target is another BMC Remedy Action Request System (BMC Remedy AR System) application. This plug-in generates the appropriate records as specified in target information of the event.
- UR protocol — Workflow sets the URL string to the appropriate view field for the browser.

CAI provides the generic event plug-in and each integrating component must implement the workflow to control the invocation of the plug-in, or use specific workflow for the delivery.

Notification engine

The BMC Remedy IT Service Management (BMC Remedy ITSM) Notification Engine provides a back-end workflow model for defining which notifications should be sent, based on events in the application. To configure notifications, the primary option provided with the BMC Remedy ITSM Suite is exposed on the People form for support staff. Additional behind the scenes configuration is available through back-end forms, but you must understand how all of the pieces fit together before attempting these types of changes.

Primary functions

The Notification Engine provides the following primary functions:

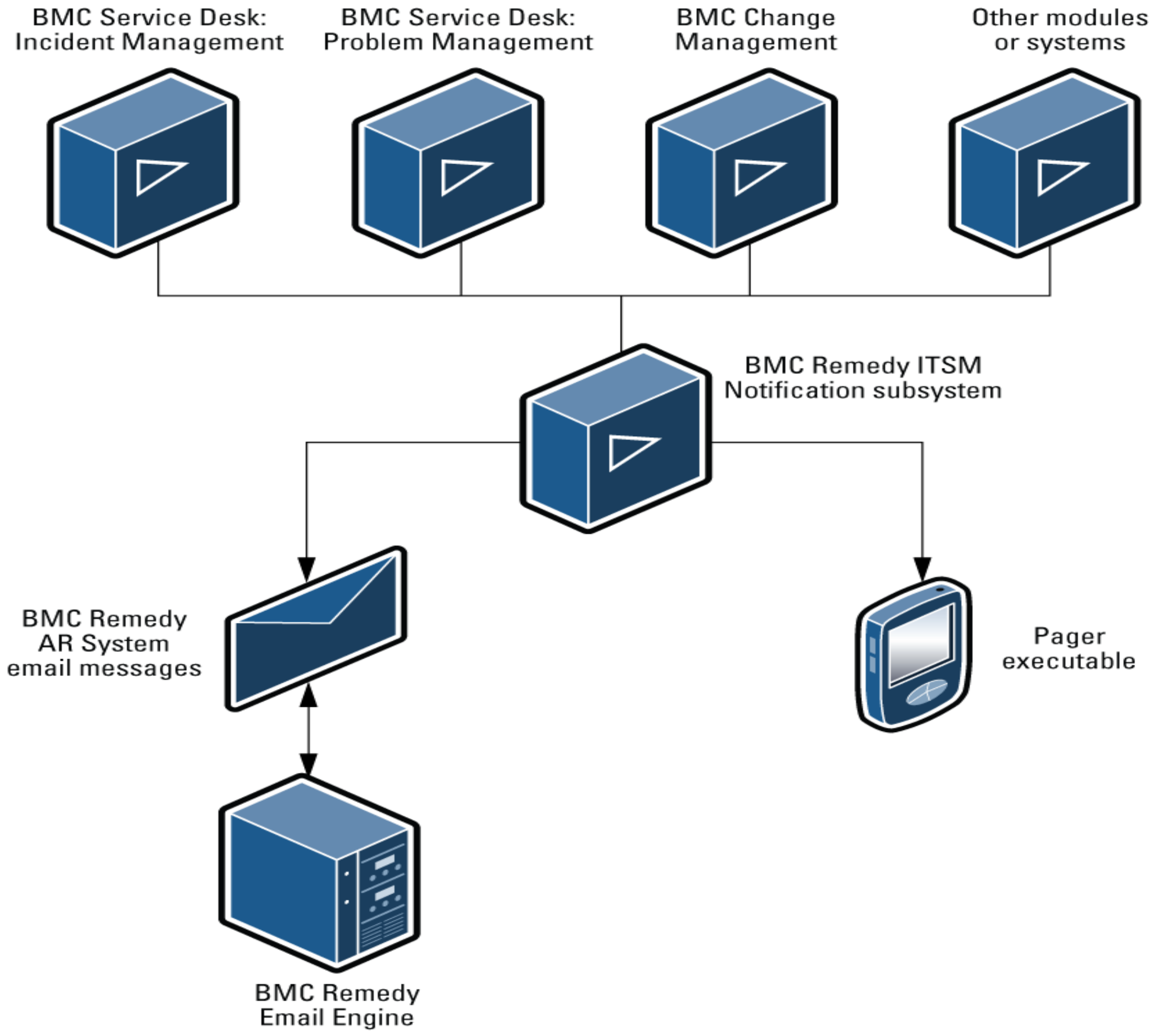
- Determines notification recipients (group or individual)
- Specifies the notification text
- Initiates the notification delivery (email or pager)
- Logs the notification details

For more information about the Notification Engine, see Notification Engine configurations.

Architecture

The BMC Remedy ITSM notification subsystem is available to all BMC Remedy ITSM applications and is connected to the BMC Remedy Email Engine provided with BMC Remedy Action Request System (BMC Remedy AR System).

Notification Engine architecture



The following major components make up the notification subsystem architecture:

- System Events and Message Catalog — Defines notification events and notification text
- System process control — Processes each notification event received from various BMC Remedy ITSM modules
- Notification interface — Sends the formatted notification (alert, email, pager)
- Notification audit — Audits each notification that is visible from the BMC Remedy ITSM modules
- Configuration settings and user preferences — Manages system default notifications and user notification preferences.

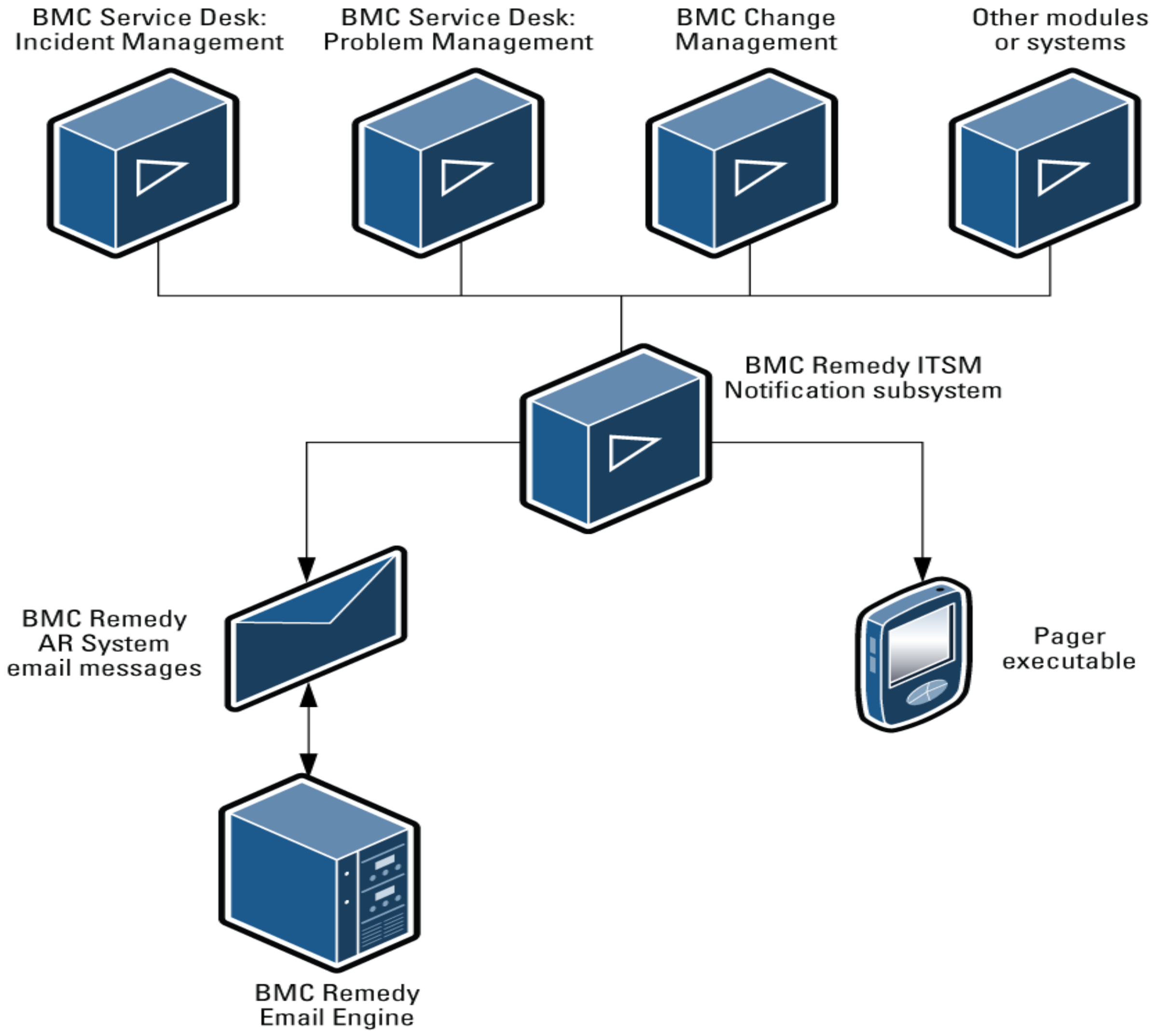
Related topic

Controlling BMC Remedy AR System through email

Notification Engine architecture

The BMC Remedy ITSM notification subsystem is available to all BMC Remedy ITSM applications and is connected to the BMC Remedy Email Engine provided with BMC Remedy Action Request System (BMC Remedy AR System).

Notification Engine architecture


BMC Service Desk: Incident Management
BMC Service Desk: Problem Management
BMC Change Management
Other modules or systems
BMC Remedy ITSM Notification subsystem
BMC Remedy AR System email messages
Pager executable
BMC Remedy Email Engine

The following major components make up the notification subsystem architecture:

- System Events and Message Catalog — Defines notification events and notification text
- System process control — Processes each notification event received from various BMC Remedy ITSM modules
- Notification interface — Sends the formatted notification (alert, email, pager)
- Notification audit — Audits each notification that is visible from the BMC Remedy ITSM modules
- Configuration settings and user preferences — Manages system default notifications and user notification preferences.

Changes to the BMC Atrium CMDB for BMC Remedy ITSM

Version 8.0 of BMC Remedy IT Service Management (BMC Remedy ITSM) made important changes in the way BMC Remedy ITSM stores the attributes that it uses to describe configuration items (CIs).

Earlier versions of BMC Remedy ITSM extended the BMC Atrium Configuration Management Database (BMC Atrium CMDB) data model by adding a number of attributes that were used to track Asset Management CI data. These attributes included information about costs, and foundational data such as company and location. BMC Atrium CMDB also included lifecycle information. Lifecycle information, however, was not discovered and you did not need to reconcile it across multiple sources. As a result, the system did not need to store lifecycle information in multiple BMC Atrium CMDB data sets.

For this reason, and because some customers needed to maintain separate permissions on these attributes, the 8.0 release of BMC Remedy ITSM introduced a new data model for the Lifecycle data.

Standard integration points and application forms were redesigned to accommodate the updates, so most customers who upgraded to version 8.0 or later were not directly affected by this change. However, you should read this topic to ensure that you understand how the change might have an impact on your environment.

⚠ **Note**
If you have customized functions or integrations that use lifecycle data, read this section.

Also, review the compatibility matrix for supported versions of BMC products at http://www.bmc.com/support/product-availability-compatibility.

For more information about the changes, see the following topics in the BMC Remedy ITSM Suite 8.0 online technical documentation:

- Data structure change
- Code changes
- Understanding how upgrades occur
- Integration and customization impact
- Updates to CI lifecycle data attributes
- BMC Remedy ITSM attributes that remain in the BMC Atrium CMDB
- Join architecture
- Backward compatibility for the BMC Atrium CMDB API

For information related to fields used in the system, see Finding whether and where fields are used in the system

Planning

This section contains information about the following planning issues:

- BSM environment recommendations
- User permissions
- Sample data - Incident templates

For more information on planning for your installation, localization, and system requirements, see Planning in the BMC Remedy IT Service Management Suite online documentation.

BSM environment recommendations

This topic provides information about the environments in which you should install the BMC Remedy IT Service Management suite, version 8.1, as certified by the BSM Reference Stack and BSM Interoperability programs. These programs provide information about validated use cases involving multiple BMC products and the third-party products that support them. BMC recommends that you install software versions that have been validated to work together by these programs, but the stacks validated by the programs do not represent the only possible combinations of products. For complete compatibility information about BMC Remedy IT Service Management Suite, version 8.1, see Product Availability and Compatibility (requires Customer Support logon credentials).

BSM Interoperability

The BSM Interoperability program helps you install compatible versions of BMC products together by testing an *application stack* of specific releases and verifying that they work together to demonstrate key use cases. The BMC Remedy IT Service Management suite, version 8.1, was certified with BSM Interoperability 8.5.1 SP 2 and some earlier releases of the application stack.

This section lists the products and applications tested in BSM Interoperability 8.5.1 SP 2. For more information such as a certified installation order, see the documentation for that release.

Application stack
The following products and applications have been validated in BSM Interoperability 8.5.1 SP 2:

- Atrium products
- Cloud products
- Service Operations - Application Program Management products
- Service Operations - Data Center Automation products
- Service Operations - Proactive Operations products
- Service Support products
- Compliance pending

The patch levels listed were the latest versions available at the time of testing. Patches are cumulative and backwards compatible except where noted in the release notes, so you can use later patch levels except in those cases. Required patches are available on the BMC Customer Support website at http://www.bmc.com/support.

To obtain necessary hotfix files and for more information about hotfixes, contact BMC Customer Support.

Version numbers marked with an asterisk (*) indicate product versions that are different than what is included in the listed suite.

Atrium

Solution or suite	Product name	Version	Service Pack or patch	Function
BMC Dashboards and Analytics Suite 7.6.04	BMC Analytics for Business Service Management	7.6.04		The BMC Analytics for Business Service Management (BMC Analytics for BSM) application provides out-of-the-box interactive reporting and analysis that enables technical and non-technical users to quickly examine data for trends and details associated with how IT is supporting business services and goals.

platform	BMC Atrium Core: - BMC Atrium CMDB - BMC Atrium Integrator - Product Catalog - Service Catalog - Atrium Web Services	7.6.04	SP 2 + hotfix (Normalization Engine)	Provides a configuration management database (BMC Atrium CMDB) coupled with common user, programmatic, and reporting interfaces to accelerate attainment of BSM. - BMC Atrium CMDB stores information about the configuration items (CIs) in your IT environment and the relationships between them. Data consumers such as the BMC Remedy Asset Management product read data from the production dataset. - The BMC Atrium Integration Engine (AIE) product enables you to transfer data between an external datastore and BMC Atrium CMDB or the BMC Remedy Action Request System product. - The Product Catalog provides a normalized reference of software, hardware, and other types of products and their characteristics that enhance the accuracy of BMC Discovery products by uniquely identifying a product regardless of installed name or location.
	BMC Atrium Discovery and Dependency Mapping	8.3		Provides an automated method for discovering, cataloging, and maintaining a company's configuration data.
BMC Dashboards and Analytics Suite	BMC Dashboards for Business Service Management	7.6.03		The BMC Dashboards for Business Service Management (BMC Dashboards for BSM) application provides highly interactive, timely access to key service support metrics to help IT management optimize decisions and accelerate the alignment of IT with business goals.
BMC Remedy IT Service Management	BMC Service Level Management	7.6.04	SP 1 + hotfix	The BMC Service Level Management application enables a service provider, such as an IT organization, a customer support group, or an external service provider, to formally document the needs of its customers or lines of business by using service level agreements, and to provide the correct level of service to meet those needs.
	BMC IT Business Management	7.6.04	SP 1	BMC IT Business Management provides IT leaders visibility into costs, activities, assets, resources, and suppliers to effectively manage the IT business and ensure business alignment.

Cloud

Solution or suite	Product name	Version	Service Pack or Patch	Function
BMC Cloud Lifecycle Management 2.1.00	BMC Cloud Lifecycle Management	2.1.00	SP1 + hotfix	Provides a complete solution for establishing a cloud environment, including a Service Catalog that defines service offerings, a self-service console for procuring resources, and cloud management capabilities.

BMC Cloud Lifecycle Management compatibility with BMC Atrium SSO is pending. BMC Cloud Lifecycle Management is targeting a future release for full compatibility with BMC Atrium SSO. See SW00416103.

Service Operations - Application Program Management

Solution or suite	Product name	Version	Service Pack or Patch	Function
BMC ProactiveNet Performance Management 8.6.20	BMC Transaction Management Application Response Time, either Infrastructure Edition or Service Level Edition	3.9.00		Enables you to manage the performance and reliability of your worldwide applications to measure site health based on end-user experience metrics, such as availability, accuracy, and performance.

Service Operations - Data Center Automation

Solution or suite	Product name	Version	Service Pack or Patch	Function
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Automation Suite	8.1.03		Automate the management, control, and enforcement of configuration changes across servers, networks, databases, and applications in the traditional data center and in the cloud.
BMC BladeLogic Automation Suite 8.1.03	BMC Application Release Automation - Enterprise Edition BMC Application Release Automation - Standard Edition	8.1.03 8.1.02		BMC BladeLogic Application Release Automation automates the long list of discrete tasks needed to deploy Web applications and dramatically simplifies the process, making it easier and less expensive for organizations to leverage Web application server technology.

BMC BladeLogic Automation Suite 8.1.03	BMC Atrium Orchestrator Platform	7.6.01.04 *		Delivers workflow-based process templates, with which customers can rapidly adapt and deploy functional design to ensure consistent and appropriate, policy-based response across the enterprise.
BMC BladeLogic Automation Suite 8.1.03	BMC Atrium Orchestrator Content Installer	7.6.05.01, Cloud AR 2.1.00		Content installer for BMC Atrium Orchestrator.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Client Automation	8.2.00 **		Enables administrators to manage software changes, manage content changes, configure endpoints, and collect inventory information.
NA	BMC BladeLogic Client Automation Discovery Integration for CMDB	8.2.00		Integrates discovered configuration data with the BMC Remedy IT Service Management suite of products. This integration enables you to use BMC Remedy Asset Management, BMC Remedy Change Management, BMC Remedy Incident Management, and BMC Remedy Problem Management to access accurate, real-time information about IT infrastructure components across your enterprise.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Decision Support for Network Automation	8.1.03***		A web-based reporting and analytics tool, used together with the BMC BladeLogic Network Automation solution to provide extensive reporting capabilities based on the network devices you manage.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Decision Support for Server Automation	8.1	SP 3	A web-based reporting application that provides extensive report capabilities related to your data center servers that are managed by BMC BladeLogic. BMC Service Automation Reporting and Analytics uses rich data warehouse schema and dimensional modeling principles to access and report on historical data captured by BMC BladeLogic.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Integration with Atrium	8.1	SP 3	Enables integration between BMC BladeLogic and Atrium components.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Network Automation	8.1.03		Manages change, configuration and compliance of network assets.
BMC BladeLogic Automation Suite 8.1.03	BMC BladeLogic Server Automation	8.1.03		Acts as a platform for the management, control and enforcement of configuration changes in the data center.

** 8.2.00.001 is required if using BMC BladeLogic Client Automation for discovery for software license management use cases.

*** Requires BOXI 4.0 on a separate server.

Service Operations - Proactive Operations

Solution or suite	Product name	Version	Service Pack or Patch	Function
BMC ProactiveNet Performance Management 8.6.20	BMC Capacity Management - Capacity Optimization	4.5	SP1	Automatically analyze, forecast, and optimize performance and capacity across all resources (IT and business) and environments — physical, virtual, and cloud.
BMC ProactiveNet Performance Management 8.6.20	BMC Portal, including the following modules: • BMC Performance Manager Portal 2.9 (with PATROL 3.9.00)	2.9.10*		Provides a common web-based interface for managing and monitoring your IT infrastructure while monitoring business services.
BMC ProactiveNet Performance Management 8.6.20	BMC ProactiveNet Core BMC ProactiveNet Performance Management Reporting	8.6.02 8.6.02 (no SP)	SP 1 (Core)	A real-time analytics solution that detects performance abnormalities in the IT environment, delivers early warning of degrading performance, and reduces time from issue detection to resolution. This early warning is delivered by Intelligent Events that result from analyzing and correlating data across the monitored IT infrastructure, speeding the ability to detect abnormal trends before end users and mission critical applications are impacted. It also provides the users with views, detailed graph displays, reports and other tools for diagnosing performance issues.
BMC ProactiveNet Performance Management 8.6.20	BMC Transaction Management Application Response Time, either Infrastructure Edition or Service Level Edition	3.9.00		Enables you to manage the performance and reliability of your worldwide applications to measure site health based on end-user experience metrics, such as availability, accuracy, and performance.
BMC ProactiveNet Performance Management 8.6.20	Integration for BMC Remedy Service Desk	8.6.02		Provides the integration from certain Service Assurance products to BMC Remedy IT Service Management.
	BMC Service Impact Management (backwards compatibility testing)	7.4		

Service Support

Solution or suite	Product name	Version	Service Pack or Patch	Function
NA	BMC Remedy Action Request System	7.6.04	SP 2	Enables the building of powerful business workflow applications which can automatically track anything that is important to the processes in your enterprise. Companies use AR System to track such diverse items as stock trades, benefits data, inventory assets, spare parts, and order fulfillment. A common use of AR System is to automate the internal help desk.
BMC Remedy IT Service Management Suite 7.6.04	BMC Remedy IT Service Management: • BMC Remedy Asset Management • BMC Remedy Change Management • BMC Remedy Service Desk, including: ◦ BMC Remedy Incident Management ◦ BMC Remedy Problem Management	7.6.04	SP 2	The BMC Remedy Asset Management application lets IT professionals track and manage enterprise CIs - and their changing relationships - throughout the entire CI lifecycle. BMC Remedy Change Management provides IT organizations with the ability to manage changes by enabling them to assess impact, risk, and resource requirements, and then create plans and automate approval functions for implementing changes. BMC Remedy Service Desk allows IT professionals to manage incidents, problem investigations, known errors, and solution database entries.
BMC Remedy IT Service Management Suite 7.6.04	BMC Remedy Knowledge Management	7.6.04	SP 2	Allows users to author and search for solutions in a knowledge base. It includes a comprehensive editor with extensive editing tools and a robust search engine that allows users to search for solutions using natural language or Boolean searches.
BMC Remedy IT Service Management Suite 7.6.04	BMC Service Request Management	7.6.04	SP 2	Allows IT to define offered services, publish those services in a service catalog, and automate the fulfillment of those services for their users.

Mainframe integrations

See the following documentation for information on mainframe integrations:

- BMC Atrium Discovery and Dependency Mapping - Discovering Mainframe Computers
  Information about using the z/OS agent and BMC Atrium Discovery and Dependency Mapping to discover mainframe computers.

Compliance pending

The following table contains products that did not meet reference stack validation in this release.

Product	Windows	Linux	SQL Server	Oracle	Tomcat	Java	Apache
BMC AppSight 7.8.00	Y	N	N	Y	Y	Y	NA
BMC BladeLogic Database Automation 8.1.02	N - agent only	Y	Y - agent postgresql - manager	Y - agent postgresql - manager	NA	NA	NA
Entuity Network Monitoring for BPPM 8.5.01	Y	Y	N - MySQL	N - MySQL	Y	Y	Y
BMC TrueSight End User Monitor 5.1.01	N - vApp	N - vApp	NA	NA	NA	NA	NA
BMC ITBM 7.6.04 SP1	Y	Y	Y	Y	NA* *BMC ITBM requires an Application Server, so JBoss is used for BSM Reference Stack 2.1	Y	NA

BSM Reference Stack

The BSM Reference Stack program helps you install BMC products with compatible versions of third-party infrastructure products together by testing an *infrastructure stack* of specific releases and verifying that they work together to demonstrate key use cases. The BMC Remedy IT Service Management suite, version 8.1, was certified with BSM Reference Stack 2.1.00 and some earlier releases of the infrastructure stack.

This section lists the third-party products tested in BSM Reference Stack 2.1.00. For more information, see the documentation for that release.

Infrastructure stack
The following tables contain information about the components and products in BSM Reference Stack.

Infrastructure stack

The infrastructure stack represents the foundational components for the BSM Reference Stack applications. You can choose to standardize on either the Windows or the Linux stack requirements.

These guidelines do not represent the only possible infrastructure for BSM applications. Specific infrastructure requirements can be found in product documentation.

Infrastructure Stack components

Component	Windows	Linux
OS	Windows 2008 R2 (64-bit)	Red Hat Enterprise Linux 5.5 (64-bit)

Database	MS-SQL 2008 Enterprise Edition SP 1 (64-bit)	Oracle Enterprise Edition 11g R1 (64-bit)
Application server	Tomcat 6.0.26 (64-bit)	Tomcat 6.0.26 (64-bit)
Web server	Apache 2.2 (32-bit)	Apache 2.2 (64-bit)
Reporting engine	BusinessObjects XI 3.1 SP3 *or* 4.0	BusinessObjects XI 3.1 SP 3 *or* 4.0
Java (JDK/JRE)	JDK/JRE 1.6.0_20*	JDK/JRE 1.6.0_20*

*see Oracle critical patch update notice

Oracle critical patch update

Oracle has issued a security advisory and critical patch update for multiple security vulnerabilities. Details can be found on the Oracle site at this URL: http://www.oracle.com/us/technologies/security/javacpujune2011-313339.html.

Application stack

BSM Interoperability 8.5.1 contains a detailed listing of the applications verified in this release, with the exception of the following application, which is not part of the BSM Reference Stack:

- BMC BladeLogic Client Automation Discovery Integration for CMDB

User permissions

This section describes the user permissions used in the Incident Management and the Problem Management modules. It also provides recommendations for assigning user permission groups.

For general information about user permissions in the BMC Remedy ITSM suite applications, see BMC Remedy IT Service Management Suite permissions.

Incident Management permissions

The following permissions are used in the Incident Management application:

Permissions	Description	Application user license type

Incident Master	Users with Incident Master permissions can perform the following functions: • Create incidents • Modify all incidents independently of any functional roles or support group affiliations • View Incident templates **Note:** To create and modify templates, you need the Support Group Admin Functional role. With this role, the modification of templates is restricted to those for which the user is a member of the Authoring Group. • Configure: • Cost Category • Cost Center information • Cost Rate templates • Financial rules • Chargeback periods **Note:** Chargeback is a function of the costing sub-system and is given automatically with the other costing features, for example, access to the Product Catalog console. Use of the Master permissions groups should be limited to key personnel who either own a process or require full control of all Incidents. **Recommendation:** Limit the use of these permissions to individuals playing a Service Desk Analyst role who require full access to all Incidents. Users with these permissions must also belong to a Support Group before they can open the Incident form.	Fixed or Floating

Incident User	Users with Incident User permission can perform the following functions: • Create incidents • Modify incidents based on functional roles and support group affiliations (that is you must be a member or either the Assigned or Owner Group to have modify access to the Incidents with this permission) • View Incident templates **Note:** You must grant the Support Group Admin functional role to create and modify templates. With this role, template modification is restricted to templates for which the user is a member of the authoring group. **Recommendation:** Limit the use of these permissions to individuals playing one of the following Service Desk roles: • Group Coordinator • On-Duty Manager • Operations Manager • Operator and Specialist • Problem Coordinator, • Change and Release Coordinator • Service Level Manager • Service Owner Users with these permissions must also belong to a Support Group to open the Incident form.	Fixed or Floating
Incident Submitter	Users with Incident Submitter permission can create and query all incidents. They cannot modify incidents. **Recommendation:** Grant these permissions to individuals who need to submit and view incidents. Typically, these permissions are given to any who fulfills one of the roles mentioned under the Incident User permissions. User-type permissions are required if the person needs modification access. Users with these permissions must also belong to a Support Group to open the Incident form.	None

Incident Viewer	Users with Incident Viewer permission can: • query all incident requests • add Work Info records • update Work Info records Users with Incident Viewer permissions cannot: • submit incident requests • modify incident requests **Recommendation:** Grant these permissions to individuals who need only read access to incidents. Typically, these permissions are given to most BMC Remedy ITSM applications users (that is, users who do not already have the 'Master', 'User' or 'Submitter' permission) for them to access incident information. Users with these permissions must also belong to a Support Group to open the Incident form.	None
Incident Config	Users with Incident Config permission can perform functions that span the following components: • Incident Management component, *configure*: • Management application settings • Incident Impact values • Incident Urgency values • Incident Priority weight ranges • Incident Prioritization • Incident rules (general field enforcement and assignment rules) • Work Info Inbound and Outbound communications counters • Decision Trees • Scripts • Incident Templates (can create and modify all templates regardless of Authoring group affiliation) • Foundation component, *for KPIs, configure*: • Flashboard parameters • KPI titles (and register, this is an advanced option) • Requestor component: • Create and update Summary Definitions **Recommendation:** Grant these permissions to individuals who configure the component functions in the preceding list. Typically, people who fulfill this role are Application Administrators.	Fixed or Floating

Related topic

Adding a support staff person

Mapping Incident Management permission groups to BMC Service Management Process Model roles

The following table lists the incident management roles that are defined in the BMC Service Management Process Model and the equivalent permissions that each role needs in Incident Management to complete the relevant procedural steps.

> ⚠ **Note**
> This section does not list all of the permission groups and functional roles defined in Incident Management, only those that are mapped to BMC Service Management Process Model roles.

BMC Service Management Process Model role name	Calbro user	Incident Management permission groups
Service Desk Analyst	Francie Stafford	Incident Master Problem Viewer Infrastructure Change Viewer Asset Viewer
Specialist	Ian Plyment	Incident User Problem User Task User Infrastructure Change Viewer Asset Viewer
Group Coordinator	Bob Baxter	Incident User Problem User Infrastructure Change User Asset Viewer
On-Duty Manager	Mary Mann	Incident User Problem Viewer Infrastructure Change Viewer Asset Viewer
Service Owner	Allen Allbrook	Incident User Problem Viewer Infrastructure Change Viewer Asset Viewer
User	Joe Unser	No Incident Management permissions are needed.

Problem Management permissions

The following permissions are used in the Problem Management application:

Permissions	Description	Application user license type

Problem Master	Users with Problem Master permission can perform the following functions: • Create problem investigation, known error and solution database records. • Modify all problem investigation, known error and solution database records independently of any functional roles or support group affiliations. • Configure: • Cost Category information • Cost Center information • Cost Rate templates • Financial rules • Chargeback periods • Access the Product Catalog console Chargeback is a function of the costing sub-system and is given automatically with the other costing features. Use of the Master permissions group should be limited to key personnel who either own a process or require full control of all Problem Management records. **Recommendation:** Limit the use of these permissions to individuals who play the role of Problem Coordinator and who require full access to all Problem Investigation, Known Error and Solution Database records. Users with these permissions must also belong to a Support Group to open the Problem forms.	Fixed or Floating

Problem User	Users with Problem User permission can perform the following functions: • Create: • Problem investigations • Known error records • Solution database records • Modify (based on functional roles and support group affiliations): • Problem investigations • Known error records A user with these permissions and no Problem Management Functional Roles can modify only Problem Investigations and Known Errors where they belong to the Assigned Group. A user with these permissions and Problem Coordinator Functional Role can modify only Problem Investigations and Known Errors where they belong to the Problem Coordinator Group) • Modify (based on support group affiliations): • Solution database records • Access: • Product Catalog console **Recommendation:** Grant these permissions to individuals performing the role of a Problem Coordinator within the Problem Management process. You should also grant these permissions to users that play any of the following roles: • Group Coordinator or a Specialist within the Incident and Problem Management processes • Change Coordinator • Release Coordinator • Availability Manager • Capacity Manager These permissions give those users the ability to create and modify Problems and Known Errors. Users with these permissions must also belong to a Support Group to open the Problem forms.	Fixed or Floating

Problem Submitter	Users with Problem Submitter permissions can create and query all: • Problem investigations • Known errors • Solution database records They cannot modify problem investigations, known errors, and solution database records. **Recommendation:** Grant these permissions to individuals who must submit and view Problem Investigations, Known Errors and Solution Database records. Typically, you give these permissions to any of the roles mentioned in the preceding list of Problem User permissions (User-type permissions are required when the user needs modification access). Users with these permissions must also belong to a Support Group to open the Problem forms.	None
Problem Viewer	Users with Problem Viewer permissions can: • query Problem investigations • query Known errors • query Solution database records • add Work Info records • update Work Info records Users with Problem Viewer permissions cannot: • submit problem investigations • modify problem investigations • submit known error records • modify known error records • submit solution database records • modify solution database records **Recommendation:** Grant these permissions to individuals who need only read access to view Problem Investigations, Known Error and Solution Database records. Typically, these permissions are given to most BMC Remedy ITSM applications users (that is, users who do not already have the 'Master', 'User,' or 'Submitter' permission) so they can access information in the Problem Management records. • Users with these permissions must also belong to a support group to open the Problem forms.	None

Problem Config	Users with Problem Config permissions can perform functions that span the following components: • Problem Management, *configure*: • Problem Impact values • Problem Urgency values • Problem Priority weight ranges • Problem Prioritization • Problem rules (general field enforcement and assignment rules) • Foundation, *for KPIs, configure*: • Flashboard parameters • KPI titles (can also register KPI titles, this is an advanced option) • Incident Management: • Configure decision trees (This configuration option is available to a Problem applications administrator, because you can create decision trees to relate Incidents directly to Known Error and Solution Database records.) **Recommendation:** Grant these permissions to individuals who configure the component functions in the preceding list. You typically give these permissions to someone fulfilling the role of an Application Administrator.	Fixed or Floating

Related topic

Adding a support staff person

Mapping Problem Management permission groups to BMC Service Management Process Model roles

The following table lists the problem management roles that are defined in the BMC Service Management Process Model and the equivalent permissions that each role needs in Problem Management to complete the relevant procedural steps.

This section does not list all of the permission groups and functional roles defined in Problem Management, only those that are mapped to BMC Service Management Process Model roles.

Problem Management role mapping

BMC Service Management Process Model role name	Calbro user	Problem Management permission groups
Specialist	Ian Plyment	Incident User Problem User Task User Infrastructure Change Viewer Asset Viewer

Problem Coordinator	Bob Baxter	Problem User Incident Viewer Infrastructure Change Viewer Asset Viewer Functional Role: Problem Coordinator

Sample data - Incident templates

To help speed up implementation and align organizations with the Best Practice approach, the Incident Management module ships with out-of-the-box sample data in the form of templates that can be used to jump-start the process of creating incident requests.

The following table lists the sample data templates:

Template name	Template Category Tier 1
Windows password reset	Personal Computing
PC's hard disk is full	Personal Computing
Can't start PC	Personal Computing
PC is slow	Personal Computing
PC has virus	Personal Computing
Sound not working	Personal Computing
Exchange password reset	Email
Change entry in global address book	Email
Can't open Outlook	Email
PST folder corrupted	Email
Can't connect to Email	Email
Can't connect to network	Network
Can't connect to wireless	Network
Can't connect VPN	Network
Internet access is slow	Network
Web page cannot be displayed	Personal Productivity
Browser very slow	Personal Productivity
Can't navigate to a page	Personal Productivity
Can't navigate to a secure site	Personal Productivity
Cannot access webmail	Personal Productivity
Addons are disabled	Personal Productivity
Browser stops or crashes	Personal Productivity
Can't install browser update	Personal Productivity
Browser reports a runtime error	Personal Productivity

Can't open WORD document	Personal Productivity
WORD won't start	Personal Productivity
Error when WORD starts	Personal Productivity
Can't print WORD document	Personal Productivity
WORD document is locked	Personal Productivity
Can't open WORD 2007 document	Personal Productivity
Can't open PowerPoint presentation	Personal Productivity
PowerPoint won't start	Personal Productivity
Error when PowerPoint starts	Personal Productivity
Can't print PowerPoint presentation	Personal Productivity
PowerPoint presentation is locked	Personal Productivity
Can't open PowerPoint 2007 presentation	Personal Productivity

Related topic

For information about other out-of-the-box functionality that you can use to jump-start productivity, see System SRDs shipped with the product.

Installing

For information about installing BMC Service Desk as part of the BMC Remedy ITSM Suite (including information about how to install all of the supporting applications, including BMC Remedy AR System and BMC Atrium CMDB, see Installing in the BMC Remedy ITSM Suite online technical documentation.

For instructions for obtaining the files that you need to install the BMC Remedy IT Service Management and supporting applications, see Downloading the installation files.

Downloading the installation files

This topic explains how to obtain the files and the documentation that you need to install the entire BMC Remedy IT Service Management suite.

> **Important**
> You can only download installation files from the solution that you purchased (for example, BMC Remedy IT Service Management or BMC Cloud Lifecycle Management). Find the solution that you purchased on the EPD site; from there, you can locate the correct product, version, and installation ZIP files.

This topic provides information about:

- Downloading the files
- Enabling search in the offline documentation

Downloading the files

⚠ **Note**
When viewing a product suite's latest version in EPD, you see only the components (including licensed add-ons) that are covered under the licenses associated with your Support ID or EPD profile.

The installation program includes the latest service packs and patches. If you just installed the product for the first time, you do not need to apply service packs or patches before you begin using the product. When new service packs and patches are released, you will perform an upgrade of the product to apply the latest changes. You can find information about service packs and patches under What's new.

1. Create a directory in which to place the downloaded files.

   ⚠ **Note**
   On Microsoft Windows computers, ensure that the directory is only one level into the directory structure. The EPD package creates a directory in the temporary directory when you extract the files, and the directory that contains the installation image should not be in a directory deeper than two levels into the directory structure.

2. Go to http://www.bmc.com/available/epd.html.
3. At the logon prompt, enter your user ID and password, and click **Submit**.
4. On the Export Compliance and Access Terms page, provide the required information, agree to the terms of the agreements, and click **Continue**.
5. If you are accessing this site for the first time, create an EPD profile to specify the languages and platforms that you want to see, per the EPD site help; otherwise, skip to step 6.
6. Verify that the correct profile is displayed for your download purpose, and perform one of the following actions:
   - If you are downloading files for a product installation, select the **Licensed Products** tab.
   - If you are downloading files for a service pack or patch, select the **Product Patches** tab.
7. Locate the BMC Remedy IT Service Management Suite.
8. Locate the version you are installing, such as *BMC Remedy IT Service Management Suite 8.1,* and expand its entries.
9. Select the check boxes next to the installation files, documentation, and (if available) associated prerequisites and technical bulletins, that you need to download. For example: **BMC Remedy AR System Server** to show the available versions.
10. Click **Download (FTP)** or **Download Manager**:
    - **Download (FTP)** places the selected items in an FTP directory, and the credentials and FTP instructions are sent to you in an email message.
    - **Download Manager** enables you to download multiple files consecutively and to resume an interrupted download if the connection drops.
      This method requires a one-time installation of the Akamai NetSession client program on the target computer and is usually the faster and more reliable way to transfer files. A checksum operation is used to verify file integrity automatically.

Enabling search in the offline documentation

The **Offline Documentation -** ***productName version*** zip file contains an archived version of the online documentation. For the latest and most comprehensive content, see the BMC Online Technical Documentation Portal.

To enable search in the offline documentation

Deploy the offline documentation on a web server by using one of the following methods:

- If this is the *first* BMC offline documentation archive that you are installing on the web server, extract the zip file to the web application deployment folder of your web container (servlet container).
  For example, with an Apache Tomcat web server, extract the zip file to **<TomcatInstallationDirectory>\webapps**.
- If at least one BMC offline documentation archive *is already installed* on the web server, perform the following steps:
  1. Extract the zip file to your hard drive.
  2. Open the extracted **localhelp** folder.
  3. Copy only the ***productName version*** folder and the ***productName version*.map.txt** file to the **localhelp** folder of your web container (servlet container).
     For example, if you are deploying BMC Asset Management 8.1 documentation to an Apache Tomcat web server, copy the **asset81** folder and the **BMC Asset Management 8.1.map.txt** file to **<TomcatInstallationDirectory>\webapps\localhelp**. Do not include the other folders and file.

To view the offline documentation in a browser

Type the following URL:
http://<servletName>:<portNumber>/localhelp/<extractedDocumentationFolder>/Home.html

For example: **http://SanJoseTomcat:8080/localhelp/ars81/Home.html**

Where to go from here

Carefully review the System requirements for your platform and other tasks, for example, Downloading service packs. You must perform these tasks before you launch the installation program.

For installation instructions, review the following procedures to determine which is the most appropriate for your environment:

- Installing the BMC Remedy ITSM Suite
- Installing the BMC Remedy ITSM Suite Preconfigured Stack
- Installing silently

Configuring after installation

This section describes configuration tasks to perform after you install BMC Service Desk. It provides information about:

- Configuring BMC Service Desk to use Login ID fields to query old incidents
- Configuring the Overview console to display tasks
- Viewing your profile
- Selecting the application preferences
- Configuring Problem Management
- Configuring Incident Management
- Configuring the Email Rule Engine

- Enabling Social Collaboration options

Configuring BMC Service Desk to use Login ID fields to query old incidents

Starting with version 8.0.00 of BMC Service Desk, the **Customer Login ID** and the **Contact Login ID** fields were added to the HPD:Help Desk (Incident) form in Incident Management. After upgrading to version 8.0.00 or later, you will not be able to use these fields to query incidents that were created using previous versions of BMC Service Desk.

Database Administrators can create and run an SQL script in the BMC Remedy AR System Database to copy the **Customer Login ID** and **Contact Login ID** data from the CTM:People (People) form to the HPD:Help Desk form, based on the **Customer** and **Contact People ID** data that is stored in the HPD:Help Desk (Incident) form.

Sample SQL scripts

- To update existing incident records with **Customer Login ID**:

```
Update HPD_Help_Desk SET Customer_Login_ID=(select Remedy_Login_ID from
CTM_People where CTM_People.Person_ID = HPD_Help_Desk.Person_ID);
```

- To update existing incident records with **Contact Login ID**:

```
Update HPD_Help_Desk SET Direct_Contact_Login_ID=(select Remedy_Login_ID from
CTM_People where CTM_People.Person_ID = HPD_Help_Desk.Direct_Contact_Person_ID);
```

For more information about the **Customer Login ID** and the **Contact Login ID** fields, see Using the Customer and Contact fields in Best Practice view.

Configuring the Overview console to display tasks

This topic describes how to configure the Overview console to display the tasks that are assigned to you.

The default behavior of the Overview console is to not display your tasks. If you want the Overview console to display them, then you must change the Show Task configuration option to Yes. You do this from the Task Management tab of the Application Preferences dialog box. You only need to perform this procedure once; the Overview console remembers this setting between sessions.

To configure the Overview console to display tasks

1. From the Applications area of the IT Home Page, select **Foundation Elements > Overview console**.
2. From the Navigation pane of the Overview console, select **Functions> Application Preferences**
3. In the Application Preferences dialog box, click the Task Management tab.
4. From the Show Task menu, select **Yes** and then click **Save**.
   Later, if you want to prevent the Overview console from displaying your tasks, then repeat the preceding procedure selecting **No** from the Show Task menu.

Viewing your profile

You can view and modify your personal profile. When you click My Profile, the People (Search) form appears. In this form, you can:

- Update company information such as organization, business, and home address, and so on
- View permissions

See Configuring people information for information about the People form.

To modify your profile

1. From the Incident Management or Problem Management console Navigation pane, choose **Functions > My Profile**.
2. On the People form, update the information at the top of the form, or click the tab corresponding to the area in which you want to change the profile information.
3. Make your changes by selecting from the various lists that are available.
4. When you finish making the changes, click **Save.**

Selecting the application preferences

The application preferences let you control some of the ways that you interact with BMC Service Desk. For example, you can choose to have the Incident Management console open automatically every time that you log in to the application.

You can also use the application preferences to:

- Set console defaults
- Determine the action that occurs after you save an Incident Request or a Problem Investigation
- Automatically use decision trees, if available, whenever you record a new incident (Incident Management only)

To set your preferences

1. From the Navigation pane of the Incident Management and the Problem Management consoles, choose **Functions > Application Preferences**.

   > ⚠ **Note**
   > To set the application preferences for a component, you must open the Application Preferences form from that component's console. For example, to set the Problem Management application preferences, open the application preferences form from the Problem Management console.

2. Update the Application Preferences form as appropriate.
   The following table describes the settings available on the form.
   Application preference settings

Setting	Description

Preferences for	This is a read-only field that identifies the user.
Default Home Page	Select the console that you want to appear as your home page when you log into the BMC Remedy Action Request System (BMC Remedy AR System) server. For example, if you want the Incident Management console to appear, select Incident Management Console.
Company	Select the company that you want to appear by default in the **Company** field, which is found under the **More Filters** feature on the application's console.
Show	The default console view, with the search criteria, controls which incident requests appear in the Assigned Work area. You can temporarily change this setting from the Navigation pane of the console. The following list shows you the available selections: • **All** — Displays all incident requests or problem investigations • **Submitted by me** — Displays all incident requests and problem investigations that you submitted • **Assigned to Me** — Displays incident requests or problem investigations assigned to you • **Assigned to my Selected Groups** — Prompts you to first select a support group to which you belong, then displays incident requests or problem investigations assigned to that group • **Assigned to All My Groups** — Displays incident requests or problem investigations assigned to all your support groups. You can choose to display all work, or work that are not yet assigned to an individual.
Confirm on Submit	Choose whether to display a confirmation message when you submit a new problem investigation record.
Console Page	
Data Set Name	When multiple data sets exist, such as production and training data sets, select the appropriate data set.
Role	Filter the application table by assignment role using one of the following selections (this filter works in conjunction with the other filters available for the table): **Note:** The selections are different for Incident Management and Problem Management. • Incident Management: • **Assignee** — Show only incident requests for which you or your group is the assignee. • **Owner** — Show only incident requests for which you or your group is the owner. • **All** — Show records for which you or your group is the Assignee, the Owner, or both. • Problem Management: • **Problem Coordinator** — Show only records for which you or your group is the Problem Coordinator. • **Assignee** — Show only records for which you or your group is the assignee. • **All** — Show records for which you or your group is the Assignee or the Problem Coordinator or both.

Overview Console	
Incident Management	• **Show Incidents** — Show incident requests in the Overview console. • **Incident Status** — Choose which incident requests appear on the console according to their status. • **SLM Status** — Choose which incident requests appear on the console according to their service target status. This is available only if BMC Service Level Management is installed (works in conjunction with the Incident Status selection). • **Role** — Choose which incident requests appear on the console according to the incident management assignment roles of Assignee or Owner. **Note:** The Role field is not visible on the Overview console. You can select an incident management assignment role for the Overview console only from Application Preferences.
Problem Management	• **Show Problem** — Show problem investigations in the Overview console. • **Show Known Error** — Choose to show known errors in the Overview console. • **Show Solution** — Choose to show solution in the Overview console. • **Problem Status** — Choose which problem investigations appear on the console according to their status. • **Known Error Status** — Choose which known errors appear on the console according to their status. • **Solution Status** — Choose which solutions appear on the console according to their status. • **Role** — Choose which problem investigations appear on the console according to the problem management assignment roles of Assignee or Problem Coordinator. **Note:** The Role field is not visible on the Overview console. You can select a problem management assignment role for the Overview console only from Application Preferences.
Form	
After New Save	This setting controls the action after you click **Save**. The following list shows the available selections: • **New request after submit** — Closes the newly created record, then opens a blank form in New mode, ready for you to create a new record • **Modify request after submit** — Saves the new record, but leaves it open so that you can continue to work with it and add or change information
Enable Auto-Decision Tree (Incident Management only)	If you select **Yes** from this list and a decision tree is set up, you are prompted by the decision tree when you record a new incident. For more information about decision trees, see Using the Incident Management decision tree.
Tab Views	You can choose whether to show the following tabs if you are using the Classic view: **Financials**, **Date**, **System**, and **Vendor**

3. Click **Save**.

Configuring Problem Management

This section provides configuration information that is specific to Problem Management. It includes information about:

- Problem Management rules
- Problem priority and weight ranges
- Hiding or displaying the Task and the Categorization tabs in Problem Management

Related topic

Custom configuration

Problem Management rules

You can configure Problem Management with rules that best suit your organization's business needs. Problem Management rules determine how problem investigations, solution database entries, and known errors are assigned through the Assignment Engine.

The rules also determine how many days before problem investigations with a status of **Completed** and known errors with a status of **Corrected** automatically move to the **Closed** status.

To configure or update Problem Management rules

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Problem Management > Advanced Options > Rules**, and then click **Open**.
   The Configure Problem Rules form appears.
3. To modify an existing rule, search for the rule, and then open it.
4. Select the company to which this rule applies.
   If it applies to all companies, select **Global**.
5. In the **Description** field, enter a brief description of the rule.
6. To use the assignment engine to automatically assign problem investigations, known errors, and solution database entries to individuals, perform the following steps:
   a. Set Assignment Engine Integration to Yes.
   b. For the role being assigned, select how assignments are routed.
      You can select the assignment process problem managers or assignees for problems, solution database entries, and known errors. For example, the **Problem Manager Assignment Process (Problem)** list value determines the process for automatically assigning a problem manager to an investigation. The following table describes the available assignment processes.

Assignment process	Description

Capacity	The capacity for each person is specified in the **Capacity Rating** field on the People form. The capacity assignment process is a ratio-based method. For example, if person A has a capacity of 100 and person B has a capacity of 200, person B can handle twice as many tickets as person A; the assignment engine assigns two tickets to B, then assigns one ticket to A.
Number	The People form tracks the number of tickets assigned to the person. The number assignment process selects the person with the least number of tickets already assigned.
Round Robin	The People form keeps track of the last time the person received an assignment. The round robin assignment process selects the person who was least recently assigned a service request.

For information about configuring the Assignment Engine, see Working with auto-assignment.

7. Select whether the program requires that CI records are related to the problem investigation record or a known error record, according to the following rules:

Rule	Action
Require Service CI Related On Submit (Problem)	Click **Yes** to ensure a business service CI is related to the problem investigation record when the problem investigation record is submitted.
Require CI Related On Completed (Problem)	Click **Yes** to ensure a CI is related to the problem investigation record when the user moves the problem investigation record to the closed state.
Require Service CI Related On Submit (Known Error)	Click **Yes** to ensure a business service CI is related to the known error record when the known error record is submitted.
Require CI Related On Corrected (Known Error)	Click **Yes** to ensure a CI is related to the known error record when the user moves the known error record to the closed state.

8. To configure the number of days after which a problem investigation or known error automatically move to the **Closed** status, type the number of days in the **Problem Auto Close Completion (in Days)** and the **Known Error Auto Close Corrected (in Days)** fields.

   Note
   The number of days is calculated from the **Last Completed Date** of the problem investigation record and the **Last Corrected Date** of the known error record. The escalation runs daily at 2:00 A.M.

9. Click **Save**.

Problem priority and weight ranges

When a user selects the impact and urgency of a problem investigation or a known error, Problem Management adds the numerical weights together to calculate the priority weight and assign a descriptive priority, such as **Critical**.

Note
You can make changes to individual global values. To make a change for a specific company, however, you *must* create a complete set of values, weight ranges, and prioritization formulas for the company.

For a description of the issues related to priority and weight ranges and the procedures you perform to configure them, see the following topics:

- Problem Management impact
- Problem urgency
- Problem priority weight ranges
- Problem prioritization

Problem Management impact

When a user selects the impact and urgency of a problem investigation or a known error, Problem Management adds these numerical weights together to calculate the priority weight.

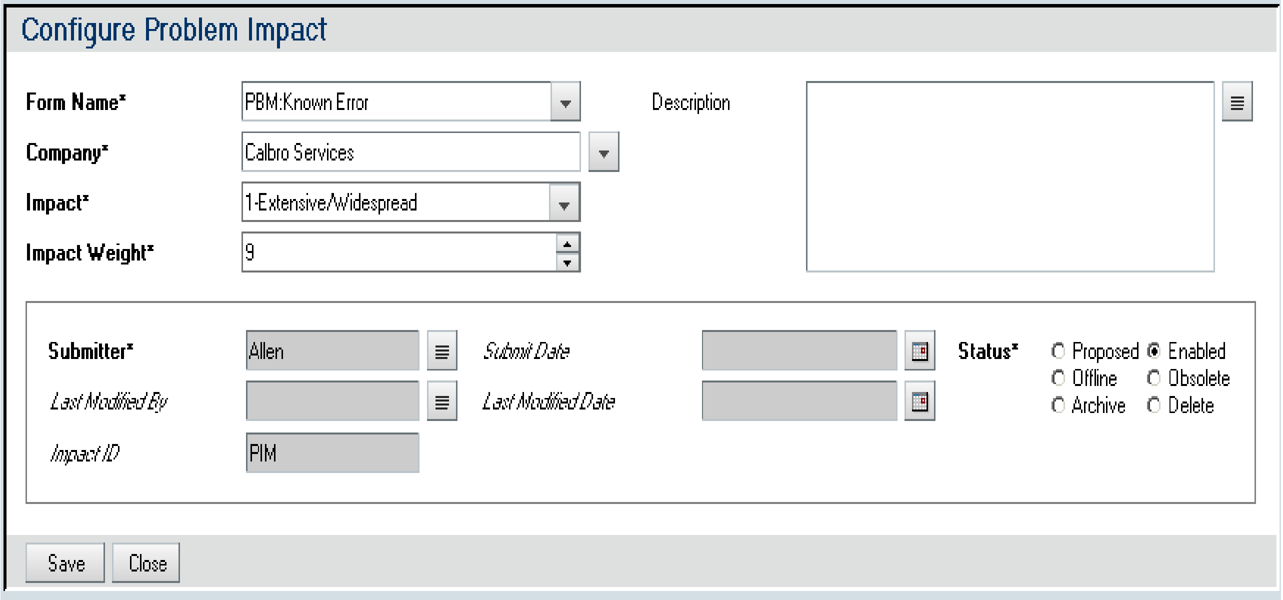
The impact values, which you configure here, map the 4 levels of impact to numerical impact weights. You can set the impact weight for each of the four levels of impact for both problem investigations and known errors. A complete set of global values are installed with Problem Management.

> ⚠ **Note**
> After you change the weight for an impact level, you must reselect the impact in each of the applicable prioritization formulas. For details, see Problem prioritization.

To configure problem impact

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Problem Management > Advanced Options > Priority and Weight Ranges - Impact Values**, and then click **Open**.
   The Configure Problem Impact form appears.
3. To modify a global value, search for the impact value, and then open it.

Configure Problem Impact form



Configure Problem Impact

Form Name*: PBM:Known Error

Company*: Calbro Services

Impact*: 1-Extensive/Widespread

Impact Weight*: 9

Description:

Submitter*: Allen

Submit Date:

Last Modified By:

Last Modified Date:

Impact ID: PIM

Status*: ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

Note
If you are creating new values for a specific company, you must first read this entire section, starting with Problem priority and weight ranges.

4. To create a new value for a specific company perform the following tasks:
    a. From the **Form Name** list, select whether this impact value applies to problem investigations or known errors.

        Note
        If an impact value applies to both problem investigations and known errors, you must create two impact values — one for the Problem Investigation form and the other for the Known Error form.

    b. Select the company to which this impact value applies.
    c. Select the appropriate impact.
5. Enter or select the appropriate impact weight.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.

Problem urgency

When the user selects the impact and urgency of a problem investigation or a known error, Problem Management adds the numerical weights together to calculate the priority weight.

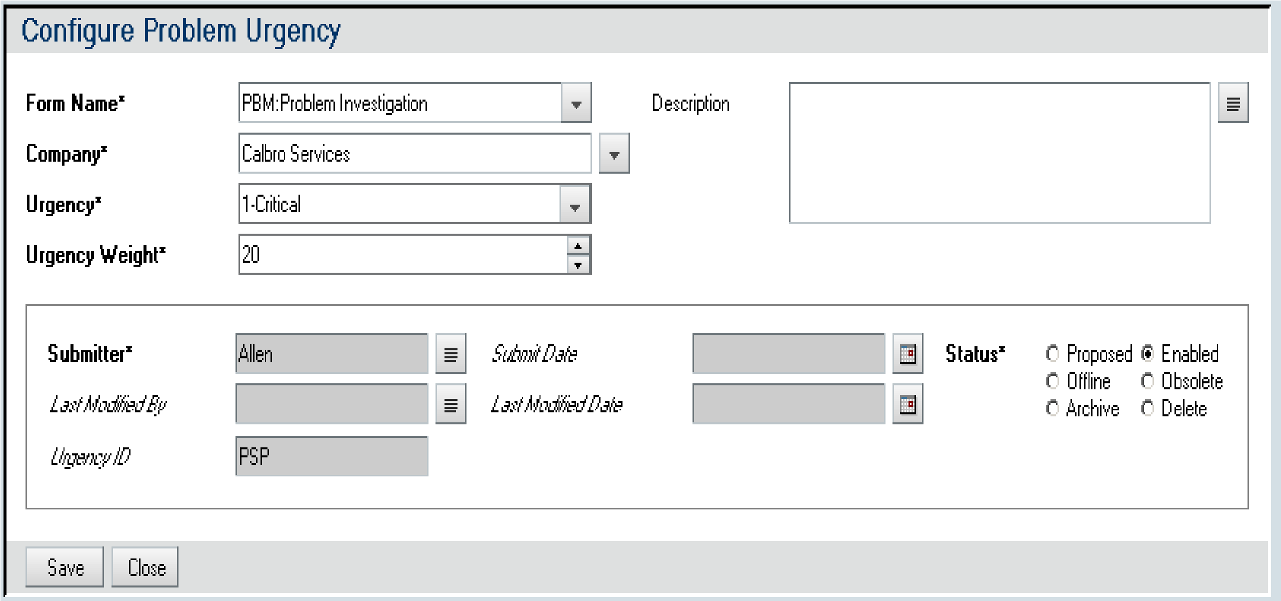
The urgency values, which you configure here, map the four levels of urgency to numerical urgency weights. You can set the urgency weight for each of the four levels of impact for both problem investigations and known errors. A complete set of global values are installed with Problem Management.

Note
After you change the weight for an urgency level, you must reselect the urgency in each of the applicable prioritization formulas. For details, see Problem prioritization.

To configure problem urgency values

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Problem Management > Advanced Options > Priority and Weight Ranges - Urgency Values**, and then click **Open**.
   The Configure Problem Urgency form appears.
3. To modify a global urgency, search for the appropriate urgency, then open it.

   Example of problem urgency value



Configure Problem Urgency

Form Name*	PBM:Problem Investigation	Description	
Company*	Calbro Services		
Urgency*	1-Critical		
Urgency Weight*	20		

Submitter*	Allen	Submit Date		Status*	○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete
Last Modified By		Last Modified Date			
Urgency ID	PSP				

> **Note**
> If you are creating new values for a specific company, you must first read this entire section, starting with Problem priority and weight ranges.

4. To create a new value for a specific company perform the following tasks.
    a. From the **Form Name** list, select whether this urgency value applies to problem investigations or known errors.
    b. Select the company to which this urgency value applies.
    c. Select the appropriate urgency.
5. Type or select the appropriate urgency weight.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.

Problem priority weight ranges

When the user selects the impact and urgency of a problem investigation or a known error, Problem Management adds the numerical weights together to calculate the priority weight.

The priority weight ranges that you configure here determine the descriptive priority (such as **Critical**) displayed on the problem investigation or known error. A complete set of global priority weight ranges is installed with Problem Management.

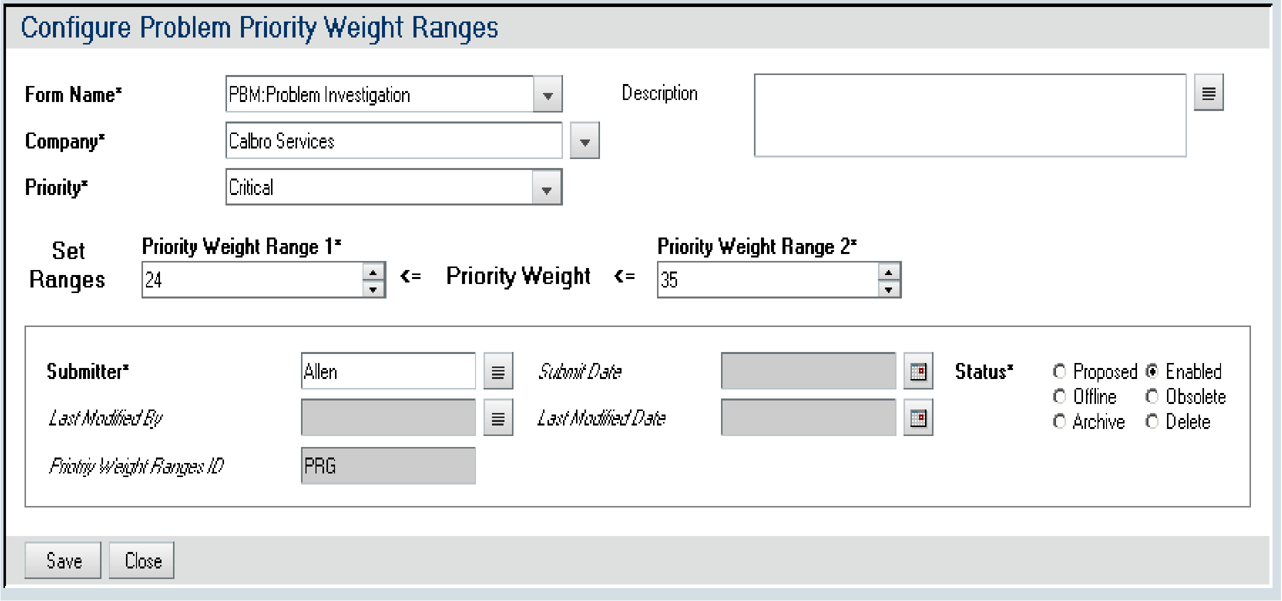
> **Note**
> After you change a priority weight range, you must reselect the impact and urgency in each of the applicable prioritization formulas. For details, see Problem prioritization.

To configure problem priority weight ranges

1. From the Application Administration Console, click the **Custom Configuration** tab.

2. From the **Application Settings** list, choose **Problem Management> Advanced Options> Priority and Weight Ranges - Priority Weight Ranges**, and then click **Open**.
   The Configure Problem Priority Weight Ranges form appears.
3. To modify a global priority weight range, search for the appropriate weight range, and then open it.

   Example of priority weight ranges for problem investigations



Configure Problem Priority Weight Ranges

Form Name* PBM:Problem Investigation

Company* Calbro Services

Priority* Critical

Description

Set Ranges: Priority Weight Range 1* 24 <= Priority Weight <= Priority Weight Range 2* 35

Submitter* Allen

Submit Date

Last Modified By

Last Modified Date

Priority Weight Ranges ID PRG

Status* ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

> **Note**
> If you are creating new weight ranges for a specific company, you must first read this entire section, starting with Problem priority and weight ranges.

4. To create a new value for a specific company perform the following tasks.
   a. From the **Form Name** list, select whether this weight range applies to problem investigations or known errors.
   b. Select the company to which this weight range applies.
   c. Select the priority for which you are defining the weight range: **Critical**, **High**, **Medium**, or **Low**.
5. In the Set Ranges area, type or select the lower (**Priority Weight Range 1**) and upper (**Priority Weight Range 2**) ends of the weight range.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.
8. Repeat this procedure to define the weight range for each of the four priorities for both problem investigations and known errors.

Problem prioritization

When a user selects the impact and urgency of a problem investigation or a known error, Problem Management adds the numerical weights together to calculate the priority weight and assign a descriptive priority, such as **Critical** .

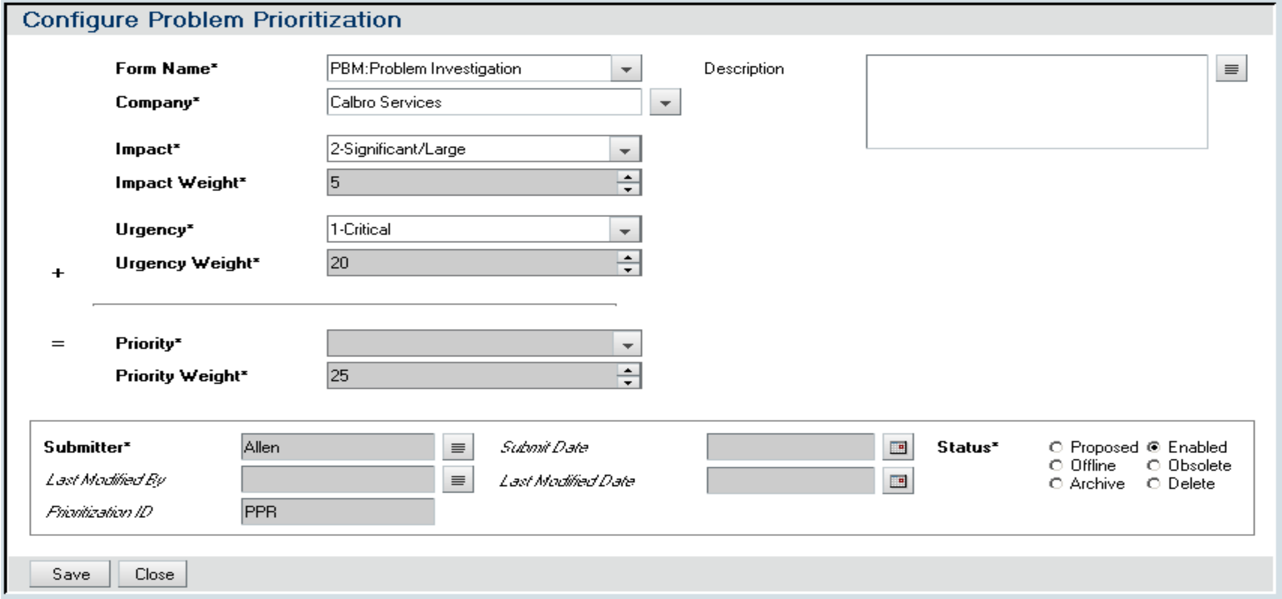
The Configure Problem Prioritization form displays the prioritization formulas. A complete set of global prioritization formulas is installed with Problem Management.

> ⚠ **Note**
> If you change the weight for an impact or urgency level, or change a priority weight range, you must reselect the impact or urgency in the applicable prioritization formulas.

To configure problem prioritization

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Problem Management> Advanced Options> Priority and Weight Ranges> Prioritization**.
   The Configure Problem Prioritization form appears.
3. To modify a global prioritization formula, search for the appropriate prioritization, and then open it.

   Example of problem prioritization



Configure Problem Prioritization

Form Name*: PBM:Problem Investigation

Company*: Calbro Services

Description:

Impact*: 2-Significant/Large

Impact Weight*: 5

Urgency*: 1-Critical

+ Urgency Weight*: 20

= Priority*:

Priority Weight*: 25

Submitter*: Allen

Submit Date:

Last Modified By:

Last Modified Date:

Prioritization ID: PPR

Status*: ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

> ⚠ **Note**
> If you are creating new prioritization formulas for a specific company, you must first read this entire section, starting with Problem priority and weight ranges.

4. To create a new prioritization formula for a specific company perform the following tasks.
   a. From the **Form Name** list, select whether this prioritization formula applies to problem investigations or known errors.
   b. Select the company to which this prioritization applies.
5. As appropriate, select or reselect the impact level from the Impact list.
   The value of the impact weight is updated to the current value from the Configure Problem Impact form.
6. As appropriate, select or reselect the urgency level from the **Urgency** list.
   The value of the urgency weight is updated to the current value from the Configure Problem Urgency form.
7. In the **Description** field, you can enter a descriptive note.
8. Click **Save**.

9. Repeat steps 3 through 8 for each prioritization formula that contains a changed impact weight or changed urgency weight.

Hiding or displaying the Task and the Categorization tabs in Problem Management

You can control whether the Tasks and the Categorization tabs appear in the best practice view of the Problem Investigation form. Both of the tabs appear by default.

If your organization does not use the Task Management System feature, or does not use operational or product categorizations (which appear on the Categorization tab) when managing problem investigations, then you can hide these tabs. You do this from the Application Administration console, using the procedure that follows.

You might perform this procedure, for example, if you want to simplify the view by hiding tabs that are not used.

To hide the Tasks and the Categorization tabs

1. Log in to the BMC Remedy ITSM suite using an account that has Problem Config permissions.
2. From the IT Home page, open the Application Administration console.
3. From the **Custom Configuration** tab, select **Problem Management > Advanced Options > Problem Management Settings**.
4. On the Problem Management Settings dialog box, click **Show Settings**.
5. From the **Show Problem Task Tab** menu, select **No**.
6. From the **Show Problem Categorization Tab** menu, select **No**.
7. Click **Add/Modify Settings**, and then click **Close**.

✓ **Tip**
If these tabs are hidden and you need to display them, reverse this procedure by selecting **Yes** in steps 5 and 6.

Configuring Incident Management

This section provides configuration information that is specific to Incident Management. It includes information about:

- Configuring ROI flashboards
- Configuring decision trees
- Working with scripts
- Incident Management advanced options

Related topic

Custom configuration

Configuring ROI flashboards

This topic describes the ROI parameters, which are configured from the Application Administration console. You need ROI Admin permissions to configure the ROI flashboard.

The following table lists and describes the configured parameters for the Cost of Incident Handling:

Cost of Incident Handling parameter descriptions

Parameter	Description
Cost	The estimated per-hour cost of incident handling used by your organization for creating projections.
Effort Input	For **Effort Input**, the ROI Administrator can select from the following values: • **Specify Effort Estimate** — Your organization selects this value if it wants to specify an estimate that is different from the one specified in the **Baseline Effort** field. This parameter represents he estimated number of hours to complete an incident request. • **Use Baseline Effort** — Your organization selects this value if it wants the flashboard to use the same value as that specified in the **Baseline Effort** field to determine effort input. • **Calculate Cumulative Effort** — Your organization selects this value if it wants the flashboard to calculate the Effort Input value by totaling the effort of all people who recorded work against any given incident request that was closed during the reporting period selected by the user. **Calculate Cumulative Effort** is used only if your organization is tracking effort in the Incident Management application.
Effort Estimate (in hours)	The actual value of the Specify Effort Estimate parameter, if that parameter is configured.
Baseline Effort	The estimated average number of hours required to handle an incident request, expressed in hours, used by your organization for creating projections.

The following table lists and describes the configured parameters for the Cost of Outages flashboards:

Cost of Outages parameter descriptions

Parameter	Description
Company	The customer company to which the rest of the parameters described in this section apply. If they apply to all companies, select **Global**.
Cost (per minute)	The estimated cost of outages used by your organization for creating projections. For example, if your organization estimates that CI outages costs **95** dollars per minute, enter **95**. If your organization estimates that CI outages costs 50 euros per minute, enter 50, and so on. The default setting for this parameter is **10**.
Monthly Outages (in minutes)	The estimated amount of time lost to CI outages per month, expressed in minutes, used by your organization for creating projections. The default setting for this parameter is **10**.

Outage Input	For Outage Input, the ROI Administrator can select from the following values: • **Calculate Cumulative Outage** — Your organization selects this value if it wants the system to use the total amount of time lost to CI outages (in minutes) for the specified date range. This is determined from examining the closed incident request records that also have related CI Unavailability records. For each CI Unavailability record, the system calculates the duration of the unavailability and then adds that amount of unavailability to the running unavailability total for the specified date range. This is the default selection for Outages Input. • **Specify Estimated Outage** — Your organization selects this value if it wants the system to use the number specified in the **Estimated Outage (in minutes)** field to calculate the actual outage cost. When you select Specify Estimated Outage (in minutes), the **Estimated Outage (in minutes)** field appears below the **Outage Input** field. For more information about the **Estimated Outage (in minutes)** field, see the explanation of that field, which follows. The default value is 100.
Estimated Outage (in minutes)	The estimated amount of time, in minutes, lost to outages on a monthly basis, used by your organization for creating projections.

Configuring decision trees

A decision tree takes the user step-by-step through a questionnaire. Based on the user's answers, the decision tree completes part of the form for a new incident request record by copying blocks of text into the record. Each element in the decision tree displays a list of items. The user's final selection completes part of the incident.

A *decision tree* is comprised of *main branches* and *branches*. It might also include *branch items*. A main branch groups together branches and branch items. Branches can group together branch items. The main branches are the initial prompts or questions that the user sees. When a user selects a main branch, the appropriate branches are displayed. For example, a user might select "Is this a hardware issue?" Based on this reply, the decision tree displays a list of: workstation, monitor, or printer issues. When the user selects from a branch, further branch items might be displayed. For example, if the user selects printer issues, the incident might be categorized, and the user can select further from: paper jam, low toner, or other printing issues.

The following is an example branching structure for a decision tree:

- Is this a hardware issue? (Main branch)
- Is this a workstation issue? (Branch 100)
    - Is the workstation unable to boot? (Branch item 101)
    - No power? (Branch item 102)
- Is this a monitor issue (Branch 200)
    - Does the display flicker excessively? (Branch item 201)
    - No power? (Branch item 202)
    - Picture appears incorrectly? (Branch item 203)

To configure a decision tree

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Decision tree configurations >**

Decision Tree, and then click **Open**.
The Decision Tree form appears. The form opens in New mode to create a new decision tree. To modify an existing decision tree, select the appropriate decision tree.

3. If the decision tree applies to all companies, leave the default value of Global in the Company field. Otherwise, select the appropriate company.
4. Enter a brief description in the **Description** field.
If a system has more than one decision tree, users select the appropriate decision tree by this description.
5. If appropriate, select a locale.
6. If the decision tree is not ready to be used, select a status of either **Proposed** or **Offline**. When the decision tree is ready for use, change the status to **Enabled**.
7. Click **Save**.

> ⚠ **Note**
> You can create branches of the decision tree only after you save it.

8. Create main branches of the decision tree by performing the following steps for each main branch.
   a. Click **New Main Branch**.
   The Branch Update dialog box appears.
   b. Type the question in the **Branch Text** field.
   c. If there are multiple main branches, type or select the appropriate sort order.
   This controls the order in which the questions appear.
   d. Click **Save** to save the main branch.
9. Create branch details by performing the following steps for each branch detail.

> ⚠ **Note**
> Branch details specify the actions you take to complete the incident form. They are grouped under main branches. Branch details can include both branches and branch items. A branch is attached directly to a main branch. A branch item is attached to either a branch or another branch item. A branch and a branch item both include a text prompt and an action.

   a. Select the appropriate main branch, branch, or branch item.
   b. Click **New Branch** or **New Branch Item**.
   The Branch Update dialog box appears.
   c. Enter the question or prompt in the **Branch Text** field.
   d. Enter or select the appropriate sort order.

> ✓ **Tip**
> If you leave gaps in the sort order, it is easier to insert branches later. For example, if you give three branches sort orders of 100, 200, and 300, you can later insert another branch at 150 without renumbering.

   e. Select the appropriate incident action type. You are prompted to specify details for the action, as described in the following table:

Incident action type	Details to specify	Effect when branch or branch detail is selected by user
None	No details.	No action is performed.
Template	Select the incident template.	The incident form is populated by the incident template. For information about templates, see Configuring Incident Management templates.
Categorization	Select the appropriate incident type, operational categorization, and product categorization.	The incident form is populated with the values that you specify here.
Summary / Notes	Specify a summary description and perform one of the following actions: • Enter a detailed description. • Select **Yes** for prompt for input and enter questions to prompt the user in the **Detailed Description** field.	The description is copied to the **Summary** field of the incident form. Depending on the selection: • The detailed description are copied to the **Notes** field. • The user is prompted with questions, and the answers are copied to the **Notes** field.
Script	Select the appropriate script.	The script prompts the user with questions to ask the customer. For information about scripts, see Creating scripts.
Solution	Select the appropriate solution entry and whether it resolves or relates to the incident.	Sets the relationship between the incident and the solution entry.
Known Error	Select the appropriate known error and whether it resolves or relates to the incident.	Sets the relationship between the incident and the known error.

f. Click **Save** to save the branch or branch item.

10. Continue to add main branches, branches, and branch items as required.
11. Click **Save** to save the decision tree.

Working with scripts

This section provides information about working with Initiator and Assignment scripts.

- Creating scripts
- Mapping scripts
- Using Manage Mappings

Creating scripts

Use this procedure to create two types of scripts: *Initiator scripts* and *Assignment scripts*.

- Initiator scripts are created and used by the support group that creates incidents. They can be used to provide service desk analysts with questions to ask customers about an incident.
- Assignment scripts are created by non-service desk support groups that are generally assigned incidents for

resolution. These scripts provide service desk analysts with questions to ask customers about their incidents so they can collect information that is relevant to the support group assigned the incident.

To create a script

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Incident Management > Script Configuration > Script Database**, and then click **Open**.
   The Script Setup form appears.
3. Click **Add**.
   The Script Update form appears.
4. In the **Script Type** field, select **Assignment** or **Initiator**.
5. Enter a description and select the status.
6. In **Copy Field**, select where the script is copied when it is selected.
7. Click **Select Group**.
8. In the Select My Group dialog box, select the support group for this script, then click **OK**.
9. In the **Script** field, enter the text of the script, such as a list of questions to ask a customer about an issue.
10. Click **Save**.
    After you create a script, you must relate it to a mapping entry to make it available for selection in BMC Remedy ITSM forms, such as the Incident form in Incident Management.

Mapping scripts

Mappings are used to search for scripts within an BMC Remedy ITSM form, such as the Incident form in Incident Management. Script mappings consist of the following data structures:

- Organization
- Location
- Organizational Categorization
- Product Categorization

To relate a script to a mapping entry

1. From the Application Administration Console, click the **Custom Configuration** tab.
   The Script Setup form appears.
2. To search for the script, enter search criteria, then click **Search**.
3. From the **Application Settings** list, choose **Incident Management > Script Configuration > Script Database**, and then click **Open**.
4. In the Script table, select the script to associate with a mapping.

   > ⚠ **Note**
   > The scripts in the Script table drive the mapping entries in the Script Association Mapping table (that is, the scripts in the Script table are directly related to the mappings in the Script Association Mapping table).

5. In the Script Association Mappings area, click **Search**.
   The Script Mapping Selection form appears.
6. You can search for existing mappings or create a new mapping:
   - To search for existing mappings, enter the search criteria in the Script Mapping Search Criteria section, and then click **Search**.
   - To create a new mapping, click the **New** button.
     The New Script Mapping form appears. The New Script Mapping form contains the mapping fields that you can use for your script.
7. Enter the new script mapping information.
8. Click **Save**.

To relate the script to this mapping entry

1. On the Script Setup form, use the Search Criteria section to search for and retrieve the correct script.
   When the search finishes, it places all of the matches in the table.
2. In the table, select the script and then click **Search** in the Script Association Mappings section.
3. Use the Script Mapping Search Criteria area of the Script Mapping Selection dialog box to locate the mapping to which you want to relate the script.

   > ⚠ **Note**
   > If a mapping does not exist, you can create one by clicking **New**.

4. Select the mapping you want from the table on the Script Mapping Selection dialog box and click **Select**.

Using Manage Mappings

You can use the Manage Mappings form as a central area to add, modify, and delete mapping records.

To use manage mappings

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Script Configuration > Script Database**, and then click **Open**.
   The Script Setup form appears.
3. Click **Manage Mappings**.
   The Manage Mappings form appears.
4. Use this form to add, modify, and delete mapping records.

   > ⚠ **Note**
   > Deleting a mapping might make script entries invisible if scripts are associated with the deleted mapping.

Incident Management advanced options

This section contains information about how to configure advanced options.

- Incident Management settings
- Incident rules
- Incident priority and weight ranges
- Configuring Work Info Inbound and Outbound Communications

Incident Management settings

From the Incident Management Settings dialog box, you can control the following application settings:

- How the application searches for customer or contact information
- Whether the application displays the People form after you select a customer or contact
- How the customer's or the contact's name is shown on the incident request form

> ⚠ **Note**
> These settings are global, that is, they apply to all companies.

To perform the following procedures, you must have Incident Config permissions:

- Configuring the Customer and Contact search type
- Configuring the People form to appear when selecting customer or contact
- Configuring Customer and Contact name format
- Hiding or displaying the Task and Categorization tabs in Incident Management

Configuring the Customer and Contact search type

You can configure which of the People form fields the application uses to search against when the user types information into either the **Customer** or the **Contact** field.

Configuring the customer and contact search type lets the user type some information in the field and then press **Enter** to return a list of partial matches from which an exact match can be chosen.You can configure the **Customer** and the **Contact** fields to search against one of the following People form fields:

- Corporate ID
- First Name
- Internet Email (default)
- Last Name
- Login ID
- Phone Number

For example, using the default configuration, the application searches against the internet email address that appears on the People form. Therefore, if the user types **AAl** in either the **Customer** or the **Contact** field and then presses **Enter**, the application returns a list of all people whose email address starts with AAl (Arthur Albertson, Allen Allworth, Anita Alman, and so on).

To configure the Customer and Contact search type

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Incident Management > Advanced Options > Incident Management Settings**, and then click **Open**.
3. Click **Show Settings** to populate the **Customer and Contact Search Type** field with the current setting.
4. From the **Customer and Contact Search Type** list, select the type of search you want.
5. Click **Add/Modify Settings** to save the setting.

Configuring the People form to appear when selecting customer or contact

You can chose to have the People form appear after the service desk analyst selects a customer or a contact name when registering a new incident request. Having the People form appear gives the service desk analyst the ability to see and, if necessary, edit any of the People information on the People form.

The default setting is **No**, which means the People form does not appear.

To configure the People form to appear when selecting a customer or contact

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Advanced Options > Incident Management Settings**, and then click **Open**.
3. Click **Show Settings** to populate the **Customer** and **Contact Search Type** field with the current setting.
4. From the **Display Customer Info Dialog** list, select **Yes** to have the People form appear.
5. Click **Add/Modify Settings** to save the setting.

Configuring Customer and Contact name format

The customer and contact name format controls how the customer's or the contact's name appears on the Incident Request form. The name format choices are:

- first name, middle name, last name
- last name, first name, middle name (default)
- last name, first name

To configure the Customer and Contact name format

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Advanced Options > Incident Management Settings**, and then click **Open**.
3. Click **Show Settings** to populate the **Customer and Contact Search Type** field with the current setting.
4. From the **Customer and Contact Name Format** list, select the format.
5. Click **Add/Modify Settings** to save the setting.

Hiding or displaying the Task and Categorization tabs in Incident Management

You can control whether the Tasks and the Categorization tabs appear in the best practice view of the Incident form.

Both of the tabs appear by default.

If your organization does not use the Task Management System feature, or does not use operational or product categorizations (which appear on the Categorization tab) when assigning incident requests, then you can hide these tabs. You do this from the Application Administration console, using the procedure that follows.

You might perform this procedure, for example, if you want to simplify the view by hiding tabs that are not used.

To hide the Tasks and the Categorization tabs

1. Log in to the BMC Remedy ITSM suite using an account that has Incident Config permissions.
2. From the IT Home page, open the Application Administration console.
3. From the **Custom Configuration** tab, select **Incident Management > Advanced Options > Incident Management Settings**.
4. On the Incident Management Settings dialog box, click **Show Settings**.
5. From the **Show Incident Task Tab** menu, select **No**.
6. From the **Show Incident Categorization Tab** menu, select **No**.
7. Click **Add/Modify Settings**, and then click **Close**.

✓ **Tip**
If these tabs are hidden and you need to display them, reverse this procedure by selecting **Yes** in steps 5 and 6.

Incident rules

Unlike the Incident Management Settings, which apply globally, incident rules apply to specific companies. For example, you can create incident rules that determine how incident requests are assigned through the Assignment Engine on a company-by-company basis.

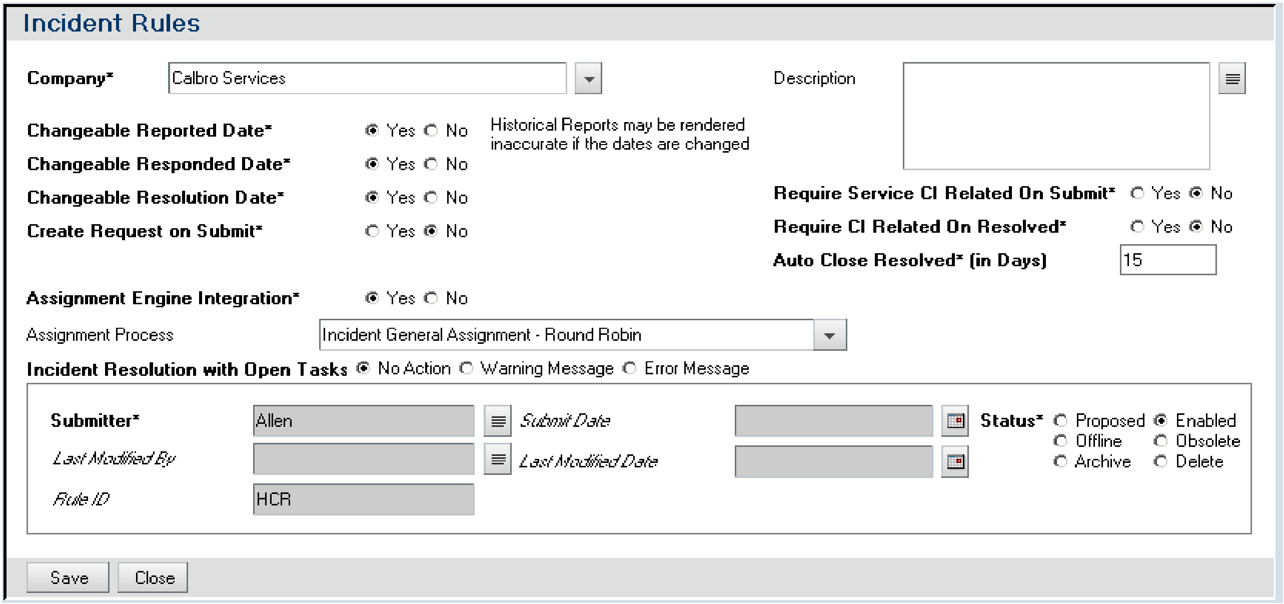
The rules also determine:

- How many days before incident requests with a status of **Resolved** automatically move to the Closed* status
- Whether you can close an incident request with open tasks
- Whether to require that you relate a Service CI to the incident request record when it is created
- Whether to require that you relate a CI to the incident request record when it is resolved

To configure incident rules

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Incident Management > Advanced Options > Rules**, and then click **Open**.
   The Incident Rules form appears.
3. To modify an existing rule, search for the appropriate rule, and open it.

   Example of an incident rule



Incident Rules

Company* Calbro Services

Description

Changeable Reported Date* ● Yes ○ No

Historical Reports may be rendered inaccurate if the dates are changed

Changeable Responded Date* ● Yes ○ No

Changeable Resolution Date* ● Yes ○ No

Create Request on Submit* ○ Yes ● No

Require Service CI Related On Submit* ○ Yes ● No

Require CI Related On Resolved* ○ Yes ● No

Auto Close Resolved* (in Days) 15

Assignment Engine Integration* ● Yes ○ No

Assignment Process Incident General Assignment - Round Robin

Incident Resolution with Open Tasks ● No Action ○ Warning Message ○ Error Message

Submitter* Allen

Submit Date

Status* ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

Last Modified By

Last Modified Date

Rule ID HCR

4. Select the company to which this rule applies.
   If it applies to all companies, select **Global**.
5. Select whether certain dates can be changed on the Incident form.
   The **Changeable Reported Date**, **Changeable Responded Date**, and **Changeable Resolution Date** fields indicate whether these dates on the Incident form can be modified after the incident has been resolved or closed. These dates can be modified only by a user with the functional role of support group manager or support group lead of the incident owner group, or who the Incident Master permission.
6. In the **Create Request On Submit** field, select whether to create a request on submission of an incident.

   If the **Create Request On Submit** option is set to **Yes**, when a user submits an Incident form, a corresponding request is created. The customer can view this request, which indicates the incident status, through the Requester Console.
7. In the **Description** field, you can enter a descriptive note about the rule.
8. Select whether the **Service CI** field is a required field.
   You can configure the **Service CI** field to be a required field when an incident request record is created (this is the default setting). You can also configure the field to never be a required field.
   This configuration is controlled by the **Require Service CI Related On Submit** flag. The flag has two settings, **Yes** and **No**. Out-of-the-box, the flag is configured with the **Yes** setting, which means that the Service CI field is required when someone creates an incident request record. If your organization's business rules do not require a Service CI to be associated with an incident request, then select the **No** value.
9. Select whether the **CI** field is a required field.
   You can configure the **CI** field to be a required field when someone changes an incident request record's status to **Resolved**. You can also configure the field to never be a required field.
   This configuration is controlled by the **Require CI Related On Resolved** flag. The flag has two settings, **Yes** and **No**. Out-of-the-box, the flag is configured with the **No** setting, which means that the **CI** field is never a required field. If your organization's business rules require a CI to be associated with an incident request when it is resolved (or before it is closed), then select the **Yes** value.
10. To configure the number of days after which an incident request automatically moves to the **Closed** status, type the number of days in the **Auto Close Resolved (in Days)** field.

    Note
    The number of days is calculated from the **Last Resolved Date** of the incident request record. The escalation runs daily at 2:00 A.M.

11. To use the Assignment Engine to automatically assign incidents to individuals, perform the following steps:
    1. Set **Assignment Engine Integration** to **Yes**.
    2. Select the appropriate **Assignment Process.**
       The following table describes the available assignment processes:
       || Assignment Process || Description ||

Capacity	The capacity for each person is specified in the **Capacity Rating** field on the People form. The capacity assignment process is a ratio-based method. For example, if person A has a capacity of 100 and person B has a capacity of 200, person B can handle twice as many tickets as person A. The assignment engine assigns two tickets to B, and then assigns one ticket to A.
Number	The People form tracks the number of tickets assigned to the person. The number assignment process selects the person with the least number of tickets already assigned.
Round Robin	The People form keeps track of the last time the person received an assignment. The round robin assignment process selects the person who was least recently assigned an incident.

For information about configuring the assignment engine, see Working with auto-assignment.

12. To configure how Incident Management reacts when an incident request is closed that still has open tasks, select one of the following messages:

Message	Description
Error Message	An error message indicates that the user must close all open tasks before closing the incident. The user cannot close the incident until all tasks are closed, because the error stops all workflow processing. *This is the default option*.
No Action	No error message appears and the user can close the incident even if an open task is associated with it. The task, however, remains open.
Warning Message	A warning message tells the user that the incident still has an open task associated with it. The user can still close the incident. The task, however, remains open. **Note:** If a user *cancels* an incident, all of the associated tasks are also canceled.

13. Click **Save**.

Incident priority and weight ranges

When users select the impact and urgency of an incident, Incident Management adds the numerical weights together to calculate the priority weight and assign a descriptive priority, such as **Critical**.

> ⚠ **Note**
> You can make changes to individual global values. To make a change for a specific company, however, you *must* create a complete set of values, weight ranges, and prioritization formulas for the company.

For a description of the issues related to priority and weight ranges and the procedures you perform to configure them, see the following topics:

- Impact values
- Urgency values

- Incident weight ranges
- Incident prioritization

Impact values

When a user selects the impact and urgency of an incident, Incident Management adds these numerical weights together to calculate the priority weight.

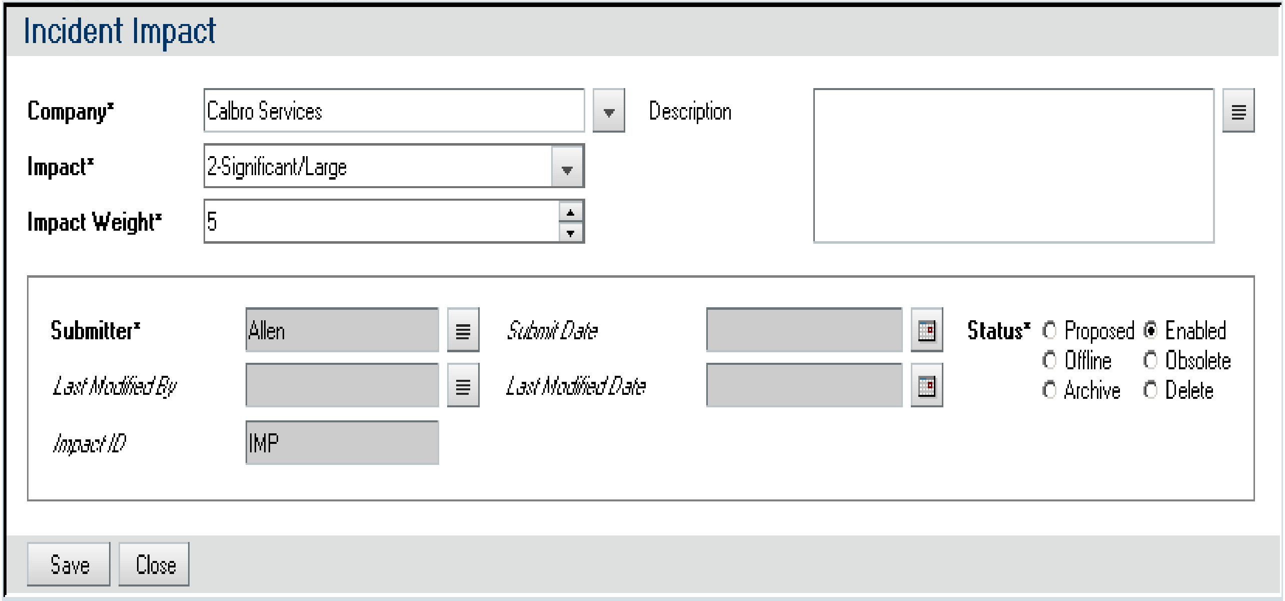
The impact values, which you configure here, map the four levels of impact to numerical impact weights. You can set the impact weight for each of the four levels of impact. A complete set of global values are installed with Incident Management.

> **Warning**
> After you change the weight for an impact level, you must reselect the impact in each of the applicable prioritization formulas. For details, see Incident prioritization.

To configure impact values

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Advanced Options > Priority and Weight Ranges - Impact Values**, and then click **Open**.
   The Incident Impact form appears.
3. To modify a global impact value, search for the impact value, and then open it.

   Example of an incident impact value



Incident Impact

Company* Calbro Services

Description

Impact* 2-Significant/Large

Impact Weight* 5

Submitter* Allen

Submit Date

Last Modified By

Last Modified Date

Impact ID IMP

Status* ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

> **Note**
> If you are creating new values for a specific company, you must first read this entire section, starting with Incident priority and weight ranges.

4. To create a new value for a specific company perform the following tasks.
   a. Select the company to which this impact value applies.

   b. Select the appropriate impact. For example, if the incident is causing major disruptions to the infrastructure for your entire company you might select **1-Extensive/Widespread**. If the incident is affecting one person and that person is still able to work, you might select **4-Minor/Localized**.

5. Type or select the appropriate impact weight. If the Impact is **1-Extensive/Widespread**, you will give it a higher impact number than if the Impact is **4-Minor/Localized**.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.

Urgency values

When a user selects the impact and urgency of an incident, Incident Management adds the numerical weights together to calculate the priority weight.

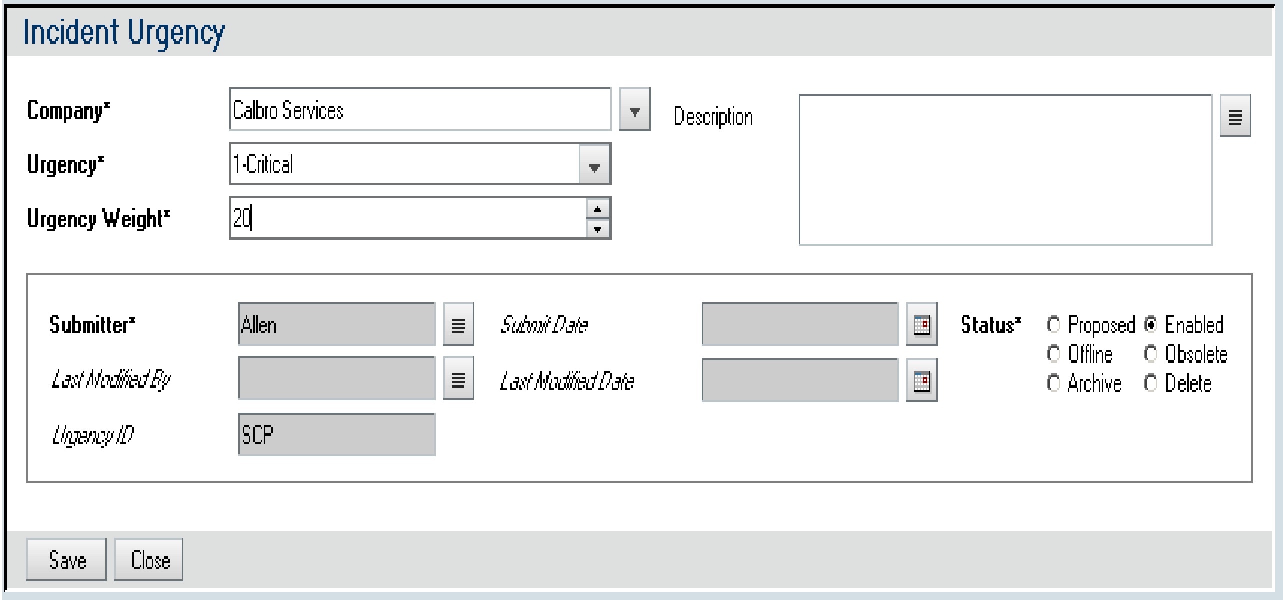
The urgency values, which you configure here, map the four levels of urgency to numerical urgency weights. You can set the urgency weight for each of the four levels of impact. A complete set of urgency values is installed with Incident Management.

> ⚠ **Note**
> After you change the weight for an urgency level, you must reselect the urgency in each of the applicable prioritization formulas. For details, see Incident prioritization.

To configure urgency values

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the Application Settings list, choose **Incident Management > Advanced Options > Priority and Weight Ranges - Urgency Values**, and then click **Open**.
   The Incident Urgency form appears.
3. To modify a global urgency, search for the appropriate urgency, and then open it.

Example of an incident urgency value



Incident Urgency

Company* Calbro Services

Urgency* 1-Critical

Urgency Weight* 20

Description

Submitter* Allen

Last Modified By

Urgency ID SCP

Submit Date

Last Modified Date

Status* ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

⚠ **Note**
If you are creating new values for a specific company, you must first read this entire section, starting with Incident priority and weight ranges

4. To create a new value for a specific company perform the following actions:
   a. Select the company to which this urgency value applies.
   b. Select the appropriate urgency.
5. Type or select the appropriate urgency weight.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.

Incident weight ranges

When a user selects the impact and urgency of an incident, Incident Management adds the numerical weights together to calculate the weight.

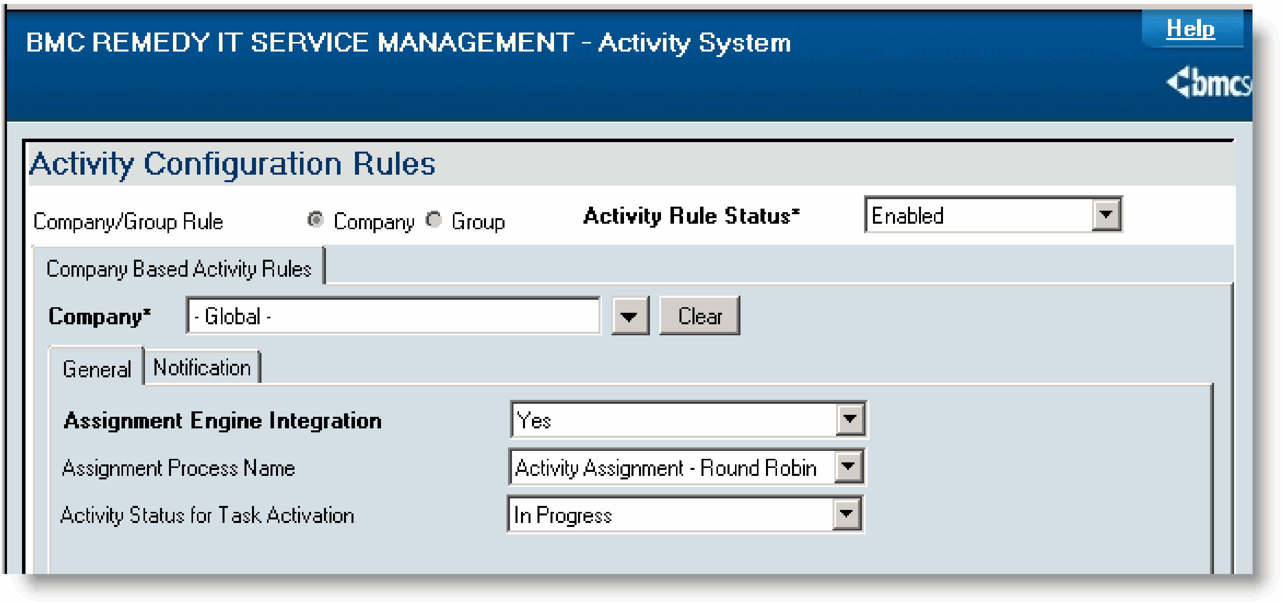
The weight ranges that you configure here determine the descriptive priority (such as **Critical**) displayed on the Incident form. A complete set of priority weight ranges is installed with Incident Management.

⚠ **Note**
After you change a weight range, you must reselect the impact and urgency in each of the applicable prioritization formulas. For details, see Incident prioritization.

To configure weight ranges

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Incident Management > Advanced Options > Priority and Weight Ranges - Weight Ranges**, and then click **Open**.
   The Incident Priority Weight Ranges form appears.
3. To modify a global priority weight range, search for the appropriate weight range, and then open it.

   Example of priority weight ranges



Activity Configuration Rules

Company/Group Rule ● Company ○ Group

Activity Rule Status* Enabled

Company Based Activity Rules

Company* - Global -

Assignment Engine Integration Yes

Assignment Process Name Activity Assignment - Round Robin

Activity Status for Task Activation In Progress

> **Note**
> If you are creating new priority weight ranges for a specific company, you must first read this entire section, starting with Incident priority and weight ranges.

4. To create a new priority weight range for a specific company perform the following actions:
   1. Select the company to which this priority weight ranges applies.
   2. Select the priority for which you are defining the weight range: **Critical**, **High**, **Medium**, or **Low**.
5. In the Priority Weight Range area, enter or select the lower and upper ends of the weight range as **Priority Weight Range 1** and **Priority Weight Range 2**.
6. In the **Description** field, you can enter a descriptive note.
7. Click **Save**.
8. Repeat this procedure to define the weight range for each of the four priorities.

Incident prioritization

When a user selects the impact and urgency of an incident, Incident Management adds the numerical weights together to calculate the priority weight and assign a descriptive priority, such as **Critical**.

The Incident Prioritization form displays the prioritization formulas. A complete set of global prioritization formulas is installed with Incident Management.

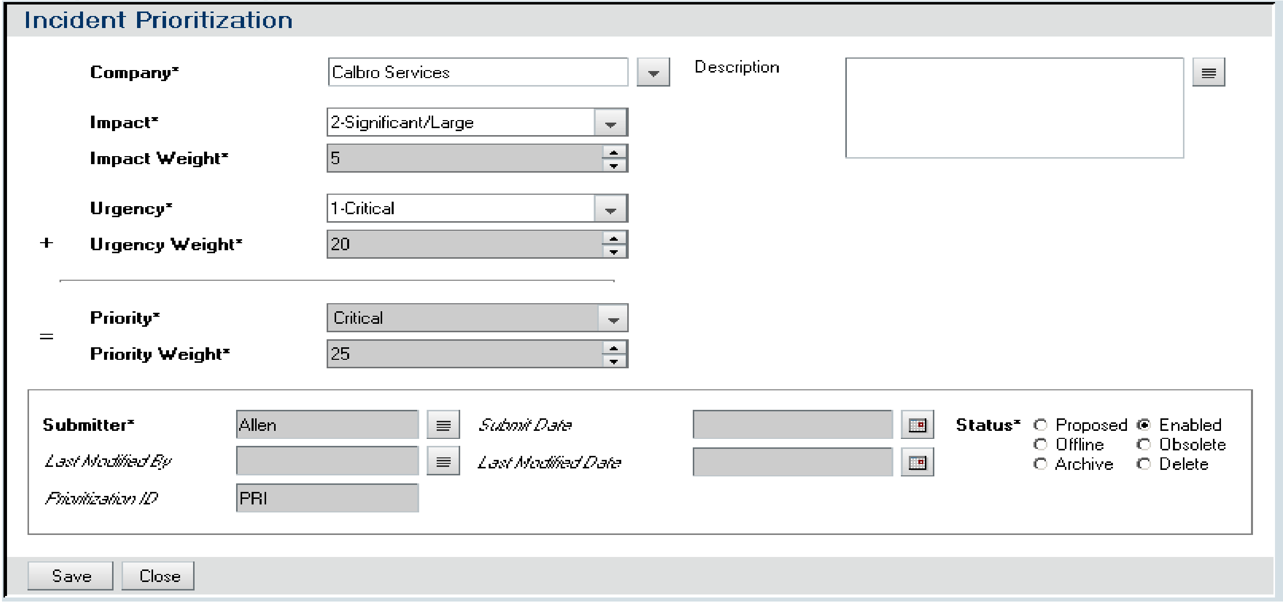
> **Note**
> If you change the weight for an impact or urgency level or if you change any priority weight ranges, you must reselect the impact or urgency in the applicable prioritization formulas.

To configure incident prioritization

1. From the Application Administration Console, click the **Custom Configuration** tab.

2. From the **Application Settings** list, choose **Incident Management > Advanced Options > Priority and Weight Ranges - Prioritization**, and then click **Open**.
   The Incident Prioritization form appears.
3. To modify a global prioritization formula, search for the appropriate prioritization, and then open it.

Example of incident prioritization



Incident Prioritization

Company* Calbro Services

Description

Impact* 2-Significant/Large

Impact Weight* 5

Urgency* 1-Critical

+ Urgency Weight* 20

= Priority* Critical

Priority Weight* 25

Submitter* Allen

Submit Date

Last Modified By

Last Modified Date

Prioritization ID PRI

Status* ○ Proposed ● Enabled ○ Offline ○ Obsolete ○ Archive ○ Delete

> **Note**
> If you are creating new prioritization formulas for a specific company, you must first read this entire section, starting with Incident priority and weight ranges.

4. To create a new prioritization formula for a specific company, select the company to which this prioritization applies.
5. As appropriate, select or reselect the impact level from the Impact list.
   The value of the **Impact Weight** field is updated to the current value from the Configure Incident Impact form.
6. As appropriate, select or reselect the urgency level from the Urgency list.
   The value of the **Urgency Weight** field is updated to the current value from the Configure Incident Urgency form.
7. In the **Description** field, you can enter a descriptive note.
8. Click **Save**.
9. Repeat steps 3 through 8 for each prioritization formula that contains a changed impact weight or changed urgency weight.

Configuring Work Info Inbound and Outbound Communications

Perform this procedure to configure the work info types to add to the totals in the **Inbound** and **Outbound** fields on the Incident Request console in the Classic view.

> **Note**
> The **Inbound** and **Outbound** fields are read-only counters that enable users to quickly view the types of work info entered in the incident.

To configure work info

1. From the Application Administration Console, click the **Custom Configuration** tab.
2. From the **Application Settings** list, choose **Incident Management > Advanced Options > Work Info Inbound and Outbound Communications**, and then click **Open**.
   The Configure Work Info form appears.
3. Select the company, or select **Global** to configure work info for all companies.
4. In the **Work Info Module** field, select **Incident**.
5. In the **Work Info Type** field, select the work info type field to configure.
6. In the **Communication Type** field, select **Inbound** or **Outbound**.
7. Select the status.
8. Click **Save**.

Configuring the Email Rule Engine

This topic provides information about configuring the Email Rule Engine to allow the creation and updating of service requests by email.

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

Process for configuring the Email Rule Engine

The process of configuring the Email Rule Engine consists of the following tasks:

1. Configure the Excluded Subjects list.
2. Configure the Email Rule Engine use cases.
3. Enable the Email Rule Engine.

Related topic

Troubleshooting email record creation and updates

Excluded Subjects list

Excluded subjects are words or phrases that, if they appear in the subject line of an incoming email message, cause the Email Rule Engine to reject the message. For example, because the phrase *Delivery Error* is in the out-of-the-box excluded subject list, the Email Rule Engine rejects any incoming message that contains this phrase.

The following list contains the out-of-the-box excluded subjects:

- Delivery Error
- Failure Notice
- Mail Delivery Failure
- Mail Delivery Subsystem
- Mail System Error
- Mailer-Daemon
- Message Rejected
- Nondeliverable Message

- Out of Office
- Postmaster
- RBE Notification
- Returned Mail
- System Administrator
- Undeliverable
- Undelivered
- Warning: Could not send message

> **Note**
> The out-of-the-box excluded subjects are associated with the Global company setting and apply to all companies in your environment.

The Excluded Subjects list prevents the email inbox that your system uses for creating or updating records from filling with email messages that the Email Rule Engine cannot process.

If your company's email environment generates other subjects that you need to exclude, you can create company specific excluded subjects.

If the email message passes all of the excluded-subject scans, the Email Rule Engine then evaluates the message against the use cases.

Related topics

Creating company specific excluded subjects
Editing the company specific excluded subjects
Record creation and updates by email
Troubleshooting email record creation and updates

Creating company specific excluded subjects

This topic describes how to create excluded subjects for each company in your environment.

Before you begin

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

To create company specific excluded subjects

1. Open the Inbound Email Rule Configuration form.
2. From the **Application** list on the left side of the IT Home page, select **Administrator Console > Application Administration Console > Custom Configuration > Foundation > Email Engine Rules > Configure Rules**.
3. From the **Company** field at the top of the form, select the company for which you are configuring the Excluded Subjects list.
4. Click the **Base Configuration** tab.
5. From the **Category** list, select **Excluded Subject**.
6. Click **Add**.
   An area on the **Base Configuration** tab displays the following fields:
   - **Status**
   - **Category**
   - **Name**
   - **Sort Order**
7. Ensure that the status is **Active**.
   You can later use this field to turn off this excluded subject by changing the status to **Inactive**.
8. Confirm that the entry in the **Category** field is **Excluded Subject**.
9. In **Name**, type the text that you want to exclude.
   For example, if you want to ensure that the Email Rule Engine rejects all email messages with *FW:* in the subject line (that is, all forwarded email messages), type *FW:*.
10. *(Optional)* In **Sort Order**, type a digit that corresponds to the order in which you want the Email Rule Engine to evaluate this excluded subject.
    A subject with **Sort Order** set to **1** is evaluated before a subject with **Sort Order** set to **5**.
11. Click **Submit**.
    The newly created excluded subject appears in the table on the left side of the Inbound Email Rule Configuration form.
12. Repeat the procedure for each subject that you want to exclude.

Where to go from here

When you finish creating the Excluded Subjects list, create the Email Rule Engine use cases.

Related topics

Excluded Subjects list
Editing the company specific excluded subjects

Editing the company specific excluded subjects

This topic describes how to edit the company specific excluded subjects.

You can update the following values for each excluded subject in the Excluded Subjects list:

- **Status** — The value can be **Active** or **Inactive**.
- **Name** — Change the actual text that the Email Rule Engine evaluates.
- **Sort Order** — Change the order in which the Email Rule Engine evaluates the excluded subject.

> ⚠ **Note**
> You cannot edit the out-of-the-box excluded subjects.

Before you begin

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

To edit an excluded subject

1. Open the Inbound Email Rule Configuration form.
2. From the **Application** list on the left side of the IT Home page, select **Administrator Console > Application Administration Console > Custom Configuration > Foundation > Email Engine Rules > Configure Rules**.
3. From the **Company** field at the top of the Inbound Email Rule Configuration form, select the company for which you are editing the excluded subject.
4. Click the **Base Configuration** tab.
5. From the **Category** list, select **Excluded Subject**.
   A table lists the excluded subjects.
6. In the table, double-click the excluded subject that you want to edit.
7. Change the values as required.
8. Click **Modify**.

Related topics

Excluded Subjects list
Creating company specific excluded subjects

Email Rule Engine use cases

The Email Rule Engine determines what action to take according to the rules that you define in the use cases. The basic types of use cases are Create and Update. For example, you can define the following use cases:

- Tell the Email Rule Engine to create an incident request that uses a specified incident request template, based on the content of the email subject line.
- Update an existing incident request with work information notes.

Also, the system uses broadly defined, generic, default use cases when an email message does not match any of those that you define. You cannot modify the default use cases or add to the default set. The out-of-the-box use cases are as follows:

- Add a work information note to a task
- Add a work information note to a Work Order
- Add a work information note to a Known Error
- Add a work information note to a problem investigation
- Add a work information note to an incident request
- Create an incident request

If the Email Rule Engine cannot match an email message to a use case, it rejects the email message.

Defining the use cases requires the following steps:

1. Create the use case record.
   You create the use case record from the **Base Configuration** tab of the Inbound Email Rule Configuration form. For information about creating use cases, see Creating Email Rule Engine use cases.
2. Define the use case rules.
   You define the rules from the **Rule Configuration** tab of the Inbound Email Rule Configuration form. For information about defining the use case rules, see Defining Email Rule Engine use case rules.

You can define multiple use cases.

Related topics

Creating Email Rule Engine use cases
Defining Email Rule Engine use case rules
Record creation and updates by email
Troubleshooting email record creation and updates

Creating Email Rule Engine use cases

This topic describes how to crate Email Rule Engine use cases.

Before you begin

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

To create an Email Rule Engine use case

1. Open the Inbound Email Rule Configuration form.
2. From the **Application** list on the left side of the IT Home page, select **Administrator Console > Application Administration Console > Custom Configuration > Foundation > Email Engine Rules > Configure Rules**.
3. From the **Company** field at the top of the form, select the company for which you are creating the use case.
4. Click the **Base Configuration** tab.
5. From the **Category** list, select **Use Case**.
6. Click **Add**.
7. Ensure that the following fields are completed correctly for the use case that you are creating.
   The fields are mandatory unless labeled as optional.
   - **Status** — **Active** (default) or **Inactive**, controls whether the Email Rule Engine evaluates against this use case at any particular time
   - **Category** — Filled by the system, it should contain **Use Case**; otherwise, go back to **Category** and reselect **Use Case**.
   - **Name** — The name that you want to use for the use case
   - **Applies to Form** *(optional)* — The application to which the use case applies: **Incident**, **Known Error**, **Problem**, **Task**, and so on. The system uses this entry to group the use cases in the table field on the left side of the Base Configuration tab.
   - **Sort Order** *(optional)* — Digit that corresponds to the order in which you want the Email Rule Engine to evaluate this use case relative to other use cases. Use case 1 is evaluated before use case 2, and so on.

     > ⚠ **Note**
     > Do not set the same **Sort Order** value for two use cases. Although the Email Rule Engine evaluates uses cases with the same **Sort Order** value, it might not evaluate them in the same relative order consistently.
8. Click **Submit**.
   The use case appears in the table on the left side of the Inbound Email Rule Configuration form.

Where to go from here

When you finish creating the Email Rule Engine use case, define the use case rules.

Related topics

Defining Email Rule Engine use case rules
Record creation and updates by email
Troubleshooting email record creation and updates

Defining Email Rule Engine use case rules

This topic describes how to define Email Rule Engine use cases. The general procedure for defining each use case is the same. However, the way that you use the fields on the **Rule Configuration** tab depends on the purpose of the use case. The first section describes the panes on the **Rule Configuration** tab and then presents an example that shows you how to use those panes to create use cases.

- Functional panes on the Rule Configuration tab

- Example of creating an email incident request from a template
- To create a use case that generates an incident request from a template
- Where to go from here
- Related topics

⚠ **Note**
You can define and edit custom Email Rule Engine use cases for any company that you create. However, you cannot add or edit use cases for the Global company.

Functional panes on the Rule Configuration tab

You define the Email Rule Engine use case rules on the **Rule Configuration** tab, which has the following panes:

- **Rule Qualification** pane, where you define the rule
- **Actions** pane, where you specify the type of action that occurs when the rule qualifications are met: a Create action or an Update action

When you open the tab, the Rule Qualification pane appears first. To see the **Actions** pane, click inside the **Actions** bar at the bottom of the tab. To go back to the **Rule Qualification** pane, click the **Rule Qualification** bar.

The following tables describe the fields on each of these panes:

Rule Qualification pane

Field name	Description
Field Name	The field on the incoming email message scanned by the Email Rule Engine to determine whether the rule applies: • **From** — Apply the rule when the message comes from a specific sender. • **Plain Text Body** — Apply the rule when the body of the email message contains specific words or phrases. • **Subject** — Apply the rule when the subject line contains specific words or phrases. • **To** — Apply the rule when the message is sent to several valid email accounts, but you want only one of the accounts to do anything with message. The BMC Remedy Email Engine can be configured to host more than one account to handle service request emails.
Operation	The logical operator for the rule qualification with which the Email Rule Engine compares the content of **Field Name** with the value of **Field Value** when evaluating incoming email messages: • **Contains** — Specified field must contain the specified word or phrase • **Equals** — Specified field must match the specified word or phrase • **Starts with** — Specified field must begin with the specified word or phrase
Field Value	The word or phrase that the Email Rule Engine scans for in the field specified in **Field Name** **Note:** You can use % as a wildcard character in this field.
plus button	Click to move **Field Name**, **Operation**, and **Field Value** selections into the **Qualification** field.

And	Add a qualification that is joined to a preceding qualification by an AND condition.
Or	Add a qualification that is joined to a preceding qualification by an OR condition.
Not	Add a qualification that is joined to a preceding qualification by a NOT condition.
Qualification	Contains the rule qualification If you are familiar with the syntax, you can type directly into this field to create a qualification without using the **Field Name**, **Operation**, or **Field Value** fields. You can also use this field to edit existing qualifications.
Action Name	Specifies the basic action that the Email Rule Engine takes when the email message meets the rule qualification: • **Create** — Create a record (available only if the form type selected on the Base Configuration tab is **Incident**). • **Update** — Update a record (default).

Actions pane

Field name	Description
Request Form	Autopopulated from the Base Configuration tab, specifies the application form on which the specified actions will occur. You cannot edit this field.
Find Request in fields (available only if you select **Update** from the **Action** menu)	Specifies where the Email Rule Engine gets the service request ID number, which enables the Email Rule Engine to handle messages about existing service requests You can select one or both of the following qualifications: • **Subject** — The subject line of the forwarded email message • **Body** — The plain text body of the forwarded email message

Data Handling (you can select more than one)	- **Include Email Fields** — Add the entire content of the email (the To, From, subject line, and body text) to the record, instead of just the body text, which is the default behavior. When you are running a Create use case, the content is added to the **Notes** field on the Incident form. When you are running an Update use case, the content is added to the **Notes** field on the Work Info tab. - **Replace Blank Subject** — When the subject line of an incoming email message is blank, add "[No subject provided]". When you are running a Create use case, the phrase is added to the Subject line on the Incident form. When you are running an Update use case, the system uses the phrase only when displaying the details of the selected email message in the Messages tab. For information about the Messages tab, see Troubleshooting email record creation and updates. - **Replace Blank Body** — When the body of an incoming email message is blank, add "[No details provided]". When you are running a Create use case, the phrase is added to the **Notes** field on the Incident form. When you are running an Update use case, the phrase is added to the **Notes** field on the Work Info tab.
Authorization	Not available
Notify Sender	Send a notification to the email sender. Select none or all that apply: - **On Success** — When the action initiated by the sender's email message finished successfully - **On Failure** — When the action initiated by the sender's email message did not finish successfully - **On Rejection** — When the email message does not pass all of the rule's qualifications

Option and **Value** (available only if you select **Create** from the **Action** menu)	*(If needed)* Allows you to specify default information to add to the specified fields when creating or updating a service request. Alternatively, it allows you to specify a template for the use case to use. For example, if you select **Assigned Group** from the **Option** list and type **Front Office** in the **Value** field, when the Email Rule Engine runs the rule, it will update the **Assigned Group** field on the service request record with the value *Front Office*. • **Option** — Provides a list from which you select one of the following options: • A field name. Type the value that you want the field to contain in the **Value** field. • **Template Name**. Type the name of the template that you want the use case to use. • **TemplateID**. Type the ID number of the template that you want the use case to use. • **Value** — Provides an entry field for the value of the option that you selected from the **Option** list. **Note:** You can use % as a wildcard character in this field.
Configured Options	Displays the options that you specify in **Option** and **Value**. If you are familiar with the syntax, you can type directly into this field to specify the options without using the **Option** and **Value** fields. You can also use this field to edit existing configured options.

Before you begin

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

Before you define an Email Rule Engine use case rule, you must create the use case record.

Example of creating an email incident request from a template

This example demonstrates how to create a use case that configures the Email Rule Engine to create an incident request from the Locked User ID template whenever an inbound email message's subject line starts with the phrase "Locked User ID." The Email Rule Engine evaluates email messages by using this rule before any other rule, and it notifies the email sender when the incident request is created successfully.

To create a use case that generates an incident request from a template

1. After completing the steps described in Creating Email Rule Engine use cases, click the **Rule Configuration** tab.
2. In **Form Name**, select **Incident**.

3. In **Use Case**, select the use case that you created in Creating Email Rule Engine use cases.
   The Rule Qualification pane appears.
4. In **Field Name**, select **Subject**.
5. In **Operation**, select **Starts with**.
6. In **Field Value**, type **Locked User ID**.
7. Click the arrow to the right of **Field Value**.
   The following qualification appears in **Qualification**:

   ```
   ('Subject' LIKE "%Locked User ID%")
   ```

8. In **Action Name**, select **Create**.
9. Click the **Actions** bar at the bottom of the form to open the Actions pane.
10. Under **Notify Sender**, click **On Success**.
11. In **Option**, select **Template Name**.
12. In **Value**, type **Locked User ID**.
13. Click the arrow to the right of **Value**.
    The following text appears in the **Configured Option** area:

    ```
    <templateName>Locked User ID</templateName>
    ```

14. Click **Save** in the upper-right corner of the **Rule Configuration** tab.
15. Run a test of the rule by sending an email message that satisfies this rule to the inbox.

Where to go from here

When you finish creating the use cases and defining their rules, enable the email service request feature.

Related topics

Defining Email Rule Engine use case rules
Record creation and updates by email
Troubleshooting email record creation and updates

Enabling the Email Rule Engine

The last step that you perform when configuring the Email Rule Engine is to enable the email service request feature.

Before you begin

To perform any Email Rule Engine configuration procedure, you must have Email Rule Config permissions (these are Foundation related permissions). Also, ensure that the BMC Remedy Email Engine is installed on your system. This includes ensuring that the specific email inbox that your system will use to receive the incoming email is configured. For information about configuring mailboxes, see Configuring BMC Remedy Email Engine.

Also, the person creating the email service request must have their own email address recorded in the **Email Address** field of their People form record.

For an overview of the email service request feature, see Record creation and updates by email.

To set the Email Rule Engine status to True

1. Open the Inbound Email Rule Configuration form.
2. From the **Application** list on the left side of the IT Home page, select **Administrator Console > Application Administration Console > Custom Configuration > Foundation > Email Engine Rules > Configure Rules**.
3. Ensure that the **Process inbound email status** selection is **True**.

Related topics

Record creation and updates by email
Troubleshooting email record creation and updates

Enabling Social Collaboration options

To use the chat, Twitter notification and RSS feed functionality, you must enable it. Out of the box, these options are disabled by default.

To enable chat, Twitter notification, and RSS feed functionality

1. Select **Application Administration Console > Custom Configuration > Foundation > Advanced Options > System Configuration Settings - System Settings**.
2. Click **Open**.
3. Select the Social Collaboration features to enable:
   - Enable Notification via Twitter
   - Enable RSS Feed
   - Enable Chat
4. Click **Save**.
5. For your changes to take effect, log out and log back on.

Upgrading

You can upgrade BMC Service Desk by using the BMC Remedy IT Service Management installer. For information about upgrading BMC Service Desk as part of the BMC Remedy ITSM Suite, see Upgrading in the BMC Remedy ITSM Suite online technical documentation.

For end-to-end instructions on upgrading BMC Remedy AR System, BMC Atrium CMDB, and the BMC Remedy ITSM Suite, see Upgrading in the BMC Remedy AR System online technical documentation.

Integrating

This section provides conceptual information about integrating BMC Service Desk with other products and solutions.

- BMC Atrium CMDB and Incident Management

- Task Management System and Incident Management
- Requester console and Incident Management
- BMC Service Level Management and Incident Management
- BMC Service Request Management and Incident Management
- Costing in Incident Management
- Incident Management interfaces
- Problem Management interfaces

Related topic

For information about developing integrations, see Developing integrations.

BMC Atrium CMDB and Incident Management

From Incident Management, users can search for configuration items (CIs) and relate CIs to an incident. Incident Management integrates with BMC Atrium Configuration Management Data Base (BMC Atrium CMDB) using relationship tables. For information about BMC Atrium CMDB, see BMC Atrium Core.

When BMC Asset Management is installed, this integration is extended by prompting users to create outages against CIs that they are relating to the incident. The outage data is stored in the BMC Asset Management database, with relationships created to the incident.

Task Management System and Incident Management

The Task Management System (TMS) module provides the ability to track specific tasks that are required to resolve an incident.

The integration with TMS provides the ability to use task templates and to define ad hoc tasks. Tasks are defined in TMS task forms.

Requester console and Incident Management

The Requester console provides the front-end user interface into the Incident Management application. The integration:

- Uses the Requester console to define incident requests
- Updates incident request information using the work info record
- Includes an interface back from the incident request to the request that is stored in the Requester console
- Updates the status of the request to the appropriate status of the request, and makes work info entries visible

BMC Service Level Management and Incident Management

Incident Management integrates with the BMC Service Level Management application to provide service level definitions for resolution and response time for incidents.

When BMC Service Level Management is installed, service targets and milestones that are associated with an incident are visible on a tab on the Incident Request form. The location of the tab depends on whether you are looking at the Classic view or the Best Practice view. For more information about these views, see Best Practice and

Classic views.

In addition to the user interface integration, the Incident Management application also uses the definition structure of BMC Service Level Management. BMC Service Level Management has a plug-in architecture for helping users define terms and conditions for a service target, as well as measurements. Incident Management provides a user interface for this BMC Service Level Management plug-in architecture to make it simpler for users to build qualifications using a query-by-example (QBE) model.

BMC Service Request Management and Incident Management

The Incident Management application integrates with BMC Service Request Management. For information about this integration, see Creating requests from fulfillment applications.

When BMC Service Request Management is installed, the Request Entry console replaces the Requester Console. See Incident rules for information about configuring Incident Management to generate a service request, which is viewed from the BMC Service Request Management Request Entry console, every time that an incident request is created.

Costing in Incident Management

Incident Management uses the Cost module to track costs associated with incidents.

The integration uses the common cost creation dialog box that is provided by the Cost module. Fields on the Incident Request form integrate with Cost module forms to show cost data related to an incident.

Incident Management interfaces

Incident Management provides a set of interfaces that other applications can use to integrate with the Incident Management application.

These interfaces include a set of BMC Remedy AR System forms that provide the ability to define, query, and modify incidents. They also include web services interfaces that are built on these forms to provide a mechanism to interact with the Incident Management application using web services. For more information, see Incident Management integrations.

Problem Management interfaces

Problem Management provides a set of interfaces that other applications can use to integrate with the Problem Management application.

These interfaces include a set of BMC Remedy AR System forms that provide the ability to define, query, and modify incidents. They also include web services interfaces that are built on these forms to provide a mechanism to interact with the Problem Management application using web services. For more information, see Problem Management integrations.

Using

This section describes how to use BMC Service Desk to accomplish various goals and tasks. The provided topics include:

- Accessing the interface
- Navigating the interface

- Using Search
- Recording effort spent on an investigation
- Recording CI unavailability in Incident Management
- Relating incident requests and problem investigations
- Printing records
- Modifying records
- Using Incident Management scripts
- Using the Incident Management decision tree
- Tracking costs
- Updating assignment availability
- Assigning or reassigning an incident request to a vendor
- Working with broadcasts
- Creating reminders
- Paging and sending email messages
- Using tasks
- Using BMC Service desk to manage incidents and problems
- Using flashboards
- Using BMC Atrium Service Context
- Working with reports
- Using social collaboration

Accessing the interface

This topic describes how to start the BMC Remedy IT Service Management suite of applications from your browser.

To log in and access the BMC Remedy ITSM Suite applications

1. Type the following URL into your browser:
   http://<webServer>:<port>/arsys/shared/login.jsp
   - <webServer>: Fully qualified name of the BMC Remedy Mid Tier system, specified in the format *server_name.company.com*.
   - <port>: *(Optional)* Port number (required if the web server is not on the default port)
2. In the **User Name** and **Password** fields of the Welcome page, enter your user name and password.
3. Click **Login**. The IT Home Page opens.

   > ⚠ **Note**
   > The IT Home page opens by default, however, system administrators can configure another home page to open, instead.

Navigating the interface

This section provides general information about how to work in the BMC Service Desk user interface. The provided topics include:

- Best Practice and Classic views
- IT Home page
- Using the Overview console
- Using the Requester console
- Navigating consoles, forms, and modules
- User interface standards for field labels
- Icons used in the interface
- Navigating the Incident Management interface
- Navigating the Problem Management interface

Best Practice and Classic views

BMC Remedy ITSM provides both a Best Practice view and a Classic view for key forms.

The Best Practice view is an improved version of the form. In this view, the fields most commonly used are immediately visible. You can access less frequently used functionality from the tabbed sections of the form or from the links in the navigation pane. For example on the Incident request form, the **Templates** field is included in the Best Practice view to encourage the use of templates.

The Classic view is a view of the form similar to the view provided in earlier releases. This view is provided for customers who are upgrading from earlier versions of BMC Remedy ITSM applications and who have not yet adopted the Best Practice view. You can configure many of the BMC IT Service Management (ITSM) suite applications for either the Best Practice view or the original Classic view. You perform the view configuration at the application, group, or individual user level.

This section explains why Best Practice views were developed, outlines the benefits of using them, and provides some recommendations for deploying them.

Best Practice views are available for the following applications and modules in the BMC Remedy ITSM Suite:

- Change request
- Incident request
- Known error
- Problem investigation
- Release request
- Work Order

For information about the benefits of Best Practice view in each application, see Benefits of Best Practice views.

> ⚠ **Note**
> If a procedure description in the documentation differs depending on the view, both methods are described. Instructions for the Best Practice view are provided first.

For detailed information about why Best Practice views were developed, the benefits of using them, and some best practices suggestions about deploying them, see Best Practice and Classic views in the BMC Remedy ITSM Suite documentation portal.

For information about Best Practice views in the Incident Management and Problem Management features, see the following topics:

- Benefits of Best Practice view in BMC Service Desk
- Incident Request form views
- Problem Investigation form views

Benefits of Best Practice view in BMC Service Desk

The topics in this section discuss the benefits of the Best Practice view in the major components of the BMC Service Desk application.

- Benefits of Best Practice view - Incident Management component
- Benefits of Best Practice view - Problem Management component

Benefits of Best Practice view - Incident Management component

The following table describes the benefits of the Best Practice view in BMC Incident Management.

> ⚠ **Note**
> In the table that follows, the Navigation pane links are not mentioned if they are available from the Navigation pane in both views, even if the link is accessed from a different group on the Navigation pane.

Benefits to the Best Practice view of the Incident form

Feature	Classic view	Best Practice view	Benefits
Customer Information	Fields on **Customer** tab: **First Name** **Middle Name** **Last Name** **Phone Number** **Company** **Organization** **Department** **Site**	Fields on Main view: • **Company** ◦ Type ahead ◦ A menu button enables you to select a group by using organizational structure	In the Best Practice view, the fields are displayed in the order in which the information is obtained, which helps you to complete the fields in the correct order. It also reduces the time needed to register an incident, because there is no need to open multiple tabs to complete the registration. The customers start the customer call by introducing themselves. The number of fields is reduced but the information is still accessible from tooltips and from opening the customer record. In BMC Remedy ITSM suite 7.6.00 and later, the letters *VIP* or the word *Sensitive* appears in bold and red if the customer record is flagged as such.

		• **Customer** ◦ Type ahead ◦ Tooltip displays additional customer information including telephone, email, and corporate ID ◦ Links embedded in the field labels provide access to the Customer Information ◦ Quick search by typing the first characters of the primary search field. Primary field, which can be set to email address, first name, last name, telephone number, or corporate ID ◦ Icon to launch Customer Search window ◦ Quick erase icon **Note:** Clicking the chevron in the upper right corner of this section enables you to modify the customer phone and site information for just this incident record.		

Contact information	Fields on **Contact** tab: **First Name** **Middle Name** **Last Name** **Phone Number** **Internet Email** **Company** **Organization** **Department** **Site**	Field on Main view: **Contact** • Type ahead • Tooltip displays additional information • Field label link enables access to the Contact information • A quick search by typing the first characters or digits of the primary search field. Primary search field can be email address, first name, last name, telephone number, or corporate ID. • Quick erase icon **Note:** Clicking the chevron in the upper right corner of this section enables you to modify the contact phone and site information for just this incident record.	The fields appear in the order in which the information is obtained. The number of fields is reduced but the information is still accessible from tooltips and from opening the customer record.
Notes	Field on Main view: **Notes**	Field on Main view: **Notes**	The fields are displayed in the order in which the information is obtained. After identifying themselves, the customers describe their issue in detail.

Template	Available as a link under Quick links	Fields on Main view: **Template** Type ahead	In the Best Practice view, templates are available from a field on the Main view to encourage the use of this feature. Using templates reduces registration time and the average incident handling time. Fields are displayed in the order in which the information is obtained. After the customer describes the issue, the user can determine whether a relevant template is available. **Note:** You can apply templates only when you *create* an incident request, not when you modify one. BMC recommends that you focus on educating the service desk staff to apply the right templates during creation. This focus ensures that you leverage the reduction in registration time, specific assignment settings, and the reduction in resolution times. If the service desk staff do not apply the correct templates during creation of incident requests, offering template application during modification is a workaround that significantly reduces the positive impact that using templates has on an IT organization.
Summary	Field on Main view: **Summary**	Field on Main view: **Summary**	Fields are displayed in the order in which the information is obtained. Now that the issue is understood, it can be summarized, or, in case a template was applied, the summary can be updated if necessary.

Service	Field on Classification tab: **Service**	Field on Main view: **Service** - Type ahead - Field label link opens the Service menu - View Business Service icon allows you to display configuration details of the selected service - Service Context icon widget can be launched to display essential status information about selected service.	This field was moved to the Main view, because the information it contains is considered key information. Out-of-the-box, the Service field is a required field. This ensures that service awareness is used for routing purposes and metrics can be tracked by the selected Service. However, you can configure the field to be not-required. **Note:** The only services that you can select are the ones that the customer is entitled to see. Entitlement is based on a Used By relationship with the Service and the customer, or the organization to which the customer belongs.
Configuration Item (CI)	Field on Classification tab: **CI**	Field on Main view: **CI** Field label link opens the Service menu **Note:** This represents the causal CI.	Because this is considered key information, it was moved to the Main view. Out-of-the-box, the **CI** field is a required field when the incident request is set to the Resolved status. This ensures that the CI is specified. However, you can configure the field to be not-required.
Target Date (renamed from Estimated Resolution Date)	Field on Date/System tab: **Target Date**	Field on Main view: **Target Date**	The **Target Date** is part of the key incident request information.
Work Info	Table on Work Info tab	Fields and table on Work Detail tab (shown initially): **Notes** **First attachment** Additional fields hidden in More Details expand area: **Work Info type** **2nd and 3rd attachments** **Locked** **View Access**	Key incident request information includes Work Info entries.
Escalated	Field on Main view: **Escalated**	This field is not displayed. If BMC Service Level Management is installed, the BMC Service Level Management Status is displayed on the Navigation pane.	Not applicable

Weight	Field on Main view: **Weight**	This field is not displayed, but it is still calculated and completed.	The Weight field is not displayed on the Best Practice view, because it does not contain information needed to resolve the incident request.
Customer's CIs	Table on **Customer** tab	Customers can view the Services that they are entitled to using the **Menu** button of the Service field. Customers can view their related CIs using the **Menu** button of the CI field.	This reduces the number of visible fields to ensure that the most important information is available at-a-glance, while making sure the customer's CI information is still accessible.
Customer's Incidents	Table on **Customer** tab	Available as a link under Quick Actions. The number of open incidents for the customer is displayed on the icon.	This reduces the number of visible fields to ensure that the most important information is available at-a-glance, while making sure the customer's incident information is still accessible.
Operational Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier** 3	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** Type-ahead available for all fields. **Tier 3**	Research suggested that most BMC customers use the operational categorization fields only sporadically. This means that even when the fields are completed, they cannot be used for reporting, because they are not consistently completed. Based on this, access to the fields was moved to a tab, which you configure to appear or be hidden, according to your organization's needs. **Note:** You can specify the operational categorization values for each template.
Product Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer** Type-ahead available for all fields. Auto-complete and pre-fill available for Product Name	The majority of customers do not use the Categorization feature for incident requests. For those who do use it, the functionality was retained through configuration settings; you can chose to turn off the tab, so that it is not visible on the Incident form.

Classification	Fields on **Classification** tab: **Incident Type** **Reported Source** **Reported Date** The other fields have been addressed in separate rows.	Fields on Main view: **Incident Type** **Reported Source** Field on **Date/System** tab: **Reported Date**	Key information includes the fields moved to the Main view.
Tasks	Available on **Tasks** tab	Available on the **Task** tab (The **Task** tab appears by default, but through configuration you can hide it if your organization does not use it.)	Space available on the screen to display tasks is bigger, leading to improved usability.
Incident Assignment	Fields on **Assignment** tab: **Support Company** **Support Organization** **Assigned Group** **Assignee** **Set Assignment using** Tooltip displaying organizational structure	Fields on Main view (**Work Detail** tab): • **Assigned Group** ◦ Type ahead ◦ **Menu** button enables selection of group using organizational structure ◦ Tooltip displaying Support Company, Support Organization, and Assigned Group • **Assignee** ◦ Type ahead ◦ Assign to Me and Auto Assign options are available as links in Quick Actions.	The **Assigned Group** and **Assignee** fields are now on the Main view, because they contain key incident request information.

Incident Owner	Fields on **Assignment** tab: **Owner Support Company** **Owner Support Organization** **Owner Group** • Tooltip displaying organizational structure Owner	Fields on **Date/System** tab: **Owner Group** • Tooltip displaying Support Company, Support Organization, and Assigned Group Owner	The overall number of fields visible on the form has been reduced, while making sure information is still accessible.
Effort Time Tracking	Fields on **Assignment** tab: **Effort Time Spent Minutes** **Total Time Spent Minutes**	Fields on Main view: Time tracking is accessible using the Clock icon next to the Assignee field.	The overall number of fields visible on the form has been reduced, while making sure information is still accessible.
Assignment Transfers	Fields on **Assignment** tab: **Transfers between Groups** **Transfers between Individuals** **Total Transfers**	Not available	The fields are tracked in the background and can still be reported. Past assignment can be found in the Audit Log.
Vendor	Fields on **Vendor** tab: **Vendor Company** **Vendor Organization** **Vendor Group** **Vendor First Name** **Vendor Last Name** **Vendor Phone** **Vendor Email** **Vendor Assignment Status** **Vendor Ticket Number** **Reported to Vendor Date** **Vendor Responded Date** **Vendor Resolved Date**	Fields on Main view: **Vendor Group** **Vendor Ticket Number**	The overall number of fields displayed for Vendor assignment has been reduced, and the key fields were moved to the Main view. This was done because they are part of the key information that should be immediately available when reviewing an incident. Additional information can be registered and reviewed in Work Info.

Resolution Categorization	Fields on **Resolution** tab: **Tier 1** **Tier 2** **Tier 3**	Fields available using the Categorizations tab.	The majority of customers do not use the Categorization feature for incident requests. For those who do use it, the functionality was retained Through configuration settings; you can chose to turn off the tab, so that it is not visible on the Incident form. **Note:** The resolution categorization values can be specified for each template.
Resolution Product Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** Type-ahead is available for all fields. Auto-complete and pre-fill available for Product Name Manufacturer	The majority of customers do not use the Categorization feature for incident requests. For those who do use it, the functionality was retained through configuration settings; you can chose to turn off the tab, so that it is not visible on the Incident form.
Resolution	Fields on **Classification** tab: **Resolution** **Resolution Method** **Cause** **Closure Source** **Satisfaction Rating** **Required Resolution Date** The other fields are shown in other rows in the table.	Fields on Main view: **Resolution**	The Resolution is considered to be key information and was moved to the Main view. The other fields were not consistently used by the majority of BMC customers and were removed.
Date/System	Available on **Date/System** tab	Available on **Date/System** tab with the exception of the Last Acknowledged Date, Last Resolved Date, Re-Opened Date, Required and Solution Created fields	The specified date fields are not made available on the Best Practice view, because these dates do not add value to the resolution of the incident request.
Track Effort	Available as a link under Advanced Functions	No longer available	The tracking functionality within the BMC Remedy ITSM Suite is being redesigned. Because the majority of customers are not using this feature, it was temporarily removed from the application.
Next Stage/Resolve	Not available	**Next Stage** and **Resolve** buttons are new in the Best Practice view.	These buttons were added to improve efficiency.

Read-only behavior	When you do not have modify access, all fields are disabled and read-only.	When you do not have modify access the following message is displayed at the top of the form: `You do not have permission to modify this ticket` The fields are not disabled or read-only, but you cannot save any modifications.	This aids with simplification and enhances performance.

Benefits of Best Practice view - Problem Management component

The following table describes the benefits of the Best Practice view in BMC Problem Management.

> **Note**
> In the table that follows, the Navigation pane links are not mentioned if they are available from the Navigation pane in both views, even if the link is accessed from a different group on the Navigation pane.

Benefits to the Best Practice view of the Problem Investigation form

Feature	Classic view	Best Practice view	Benefits
Coordinator Assignment	Fields on **Assignment** tab: • **Support Company** • **Support Organization** • **Assigned Group** ◦ Tooltip displaying organizational structure • **Assignee** ◦ Tooltip displaying Name, Email, Telephone, and Site • **Set Assignment using** • **Assign to Vendor**	Fields on Main view: • **Coordinator Group** ◦ Type ahead ◦ Menu button enables selection of group using organizational structure ◦ Tooltip displaying organizational structure • **Problem Coordinator** ◦ Type ahead ◦ Tooltip displaying Name, Email, Telephone, and Site	Key problem investigation information includes the group and person responsible for coordinating the problem until closure. Best practice recommends that the problem coordinator be the same person who creates the problem investigation, so these fields are completed automatically with the submitter's information when that person has the functional role of Problem Coordinator. If you leave the fields blank, the Assignment rules determine the field values after the submission.

Problem Location	Fields on **Requester** tab: **Company** **Region** **Site Group** **Site** **Address**	Fields on Main view: **Problem Location** • Type ahead • Tooltip • This field shows the lowest level of location information of the problem coordinator or person who submitted the release request.	Key problem investigation information includes where the problem is coordinated from. This field is also used to determine access rights for multi-tenancy implementations.
Service	Field on **Classification** tab: **Service**	Field on Main view: **Service** • Type ahead • Field label link opens the Service CI menu • View Business Service icon allows you to display configuration details of the selected service • Service context widget can be launched to display essential status information about the selected service	This field was moved to the Main view, because key information for a problem investigation includes the service CI type. In out-of-the-box configurations, the **Service** field is required. This ensures that service awareness is used for routing purposes and that metrics can be tracked by the selected Service. However, you can configure the field to not be required.
CI	Field on **Classification** tab: **CI**	Field on Main view: **CI** Field label link opens the Service CI	Because this is considered key information, it was moved to the Main view. Out-of-the-box, the **CI** field is a required field when you set the problem investigation status to Completed. This ensures the causing **CI** is specified. However, you can configure the field to not be required.
Target Date (introduced in BMC Remedy ITSM suite 7.6.00)	Field on **Classification** tab: **Target Date**	Field on Main view: **Target Date**	The Target date is key problem investigation information. The Target Date field is a required field for any status other than Draft.

Work Info	Table on **Work Info** tab	Fields and table on **Work Detail** tab (shown initially): **Notes** **First attachment** **Additional fields hidden in More Details expand area:** **Work Info type** **2nd and 3rd attachments** **Locked** **View Access**	Key problem investigation information includes Work Info entries.
Weight	Field on Main view: **Weight**	This field is not displayed but it is still calculated and completed.	The Weight field is not displayed on the Best Practice view, because it does not contain information needed to resolve the problem.
Requester	Requester information is available on the **Requester** tab.	Not available.	Because a problem can be created based on multiple incident requests, BMC recommends that you review the related incidents using the **Relationships** tab to review the requesters' information. **Note:** You can capture the Submitter information on the **Date/System** tab.
Operational Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier 3**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** Type-ahead available for all fields. **Tier 3**	Research suggested that most of BMC's customers use the operational categorization fields only sporadically. This means that even when the fields are completed, they cannot be used for reporting, because they are not consistently completed. Based on this, access to the fields was moved to a tab, which you configure to appear or be hidden, according to your organization's needs. **Note:** You can specify the operational categorization values for each template.

Product Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** Type-ahead available for all fields. Auto-complete and pre-fill available for Product Name Manufacturer	These fields were moved to the Navigation pane, because using the CMDB is a better way to perform grouping, trending, and assignment. This, and wanting to reduce the registration time of new incident request records, means that now the product categorization is automatically completed based on the product categorization of the related service.
Classification	Fields on **Classification** tab: **Investigation Driver** **Investigation Justification** **Workaround** **Root Cause** **Reproducible** The other fields are shown in other rows in the table.	Fields on Main view: **Investigation Driver** **Workaround**	Key problem investigation information includes the fields that were moved to the Main view. The **Investigation Justification, Root Cause**, and **Reproducible** fields are not displayed on the Best Practice view. This is because research showed the majority of customers are neither using these fields for reporting nor for problem resolution.
Tasks	Available on **Tasks** tab	Available on **Tasks** tab. The **Tasks** tab appears by default, but if your organization does not use tasks, you can hide the tab.	Space available on the screen to display tasks is bigger, leading to improved usability.

Problem Assignment	Fields on **Assignment** tab: - **Support Company** - **Support Organization** - **Assigned Group** - Tooltip displaying organizational structure - **Assignee** - Tooltip displaying Name, Email, Telephone and Site - **Set Assignment using**	Fields on Main view (**Work Detail** tab): - **Assigned Group** - Type ahead - **Menu** button enables selection of group using organizational structure - Tooltip displaying organizational structure - **Assignee** - Type ahead - Tooltip displaying Name, Email, Telephone, and Site - Assign to Me and Auto Assign options are available as links in Quick Actions.	The Assigned Group and Assignee fields contain key problem investigation information.
Vendor	Fields on **Vendor** tab: **Vendor Name** **Vendor Ticket Number** **Vendor Contact** **Vendor Phone** **Internet Email** **Assigned to Vendor Date** **Vendor Responded On Date**	Fields on Main view (**Work Detail** tab): **Vendor** **Vendor Ticket Number**	The number of fields displayed for Vendor assignment have been reduced to only the essential ones. Key information includes vendor and vendor ticket number details. Additional information can be registered and reviewed in Work Info.
Financials	Available on **Financials** tab	No longer available	The financial functionality within the BMC Remedy ITSM Suite is being redesigned. Because the majority of customers are not using this feature, it was removed in BMC Remedy ITSM suite 7.6.00.
Date/System	Available on **Date/System** tab	Available on **Date/System** tab with the exception of the **Problem Reported On** and **Solution Created** fields	The **Problem Reported On** and **Solution Created** fields are not made available on the Best Practice view, because these dates add value neither for reporting nor resolution.

Paging System	Available as a link under Functions	No longer available	The majority of customers no longer use this feature.
Track Effort	Available as a link under Advanced Functions	No longer available	The tracking functionality within the BMC Remedy ITSM Suite is being redesigned. Because the majority of customers are not using this feature, it was temporarily removed from the application.
Next Stage /Complete	Not available	**Next Stage** and **Complete** buttons are new in the Best Practice view.	These buttons were added to increase efficiency.
Read-only behavior	When you do not have modify access, all fields are disabled and read-only.	When you do not have modify access, the following message is displayed at the top of the form: You do not have permission to modify this ticket. The fields are not disabled or read-only, but the user cannot save any modifications.	This change was made to aid simplification and to enhance performance.

Benefits of Best Practice view in the Known Error module

In the following comparison, the Navigation pane links are not mentioned when they are available from the Navigation pane in both views. This is true even if the link is accessed from a different group on the Navigation pane.

Benefits to the Best Practice view of the Known Error form

Feature	Classic view	Best Practice view	Benefits

Coordinator Assignment	Fields on **Assignment** tab: - **Support Company** - **Support Organization** - **Assigned Group** - Tooltip displaying organizational structure - **Assignee** - Tooltip displaying Name, Email. Telephone and Site - **Set Assignment using**	Fields on Main view: - **Coordinator Group** - Type ahead - **Menu** button enables selection of group using organizational structure - Tooltip displaying organizational structure - **Problem Coordinator** - Type ahead - Tooltip displaying Name, Email, Telephone, and Site	Key information includes knowing which group and which person is responsible for coordinating the known error until it is closed. Best practice recommends that the coordinator of the known error is the same person who creates the known error; the Coordinator fields are automatically completed with the submitter's information when that person has the functional role of Problem Coordinator. If you leave the fields blank, the Assignment rules determine the field values after the submission.
Known Error Location	Field on **Classification** tab: **Company**	Fields on Main view: **Known Error Location** - Type ahead - Tooltip - This field shows the lowest level of location information of the problem coordinator	Key information includes knowing from where the known error is coordinated. The application also uses this field to determine access rights for multi-tenancy implementations.

Service	Field on Main view: **Service**	Field on Main view: **Service** - Type ahead - Field label link opens the Service CI * View Business Service icon allows you to display configuration details of the selected service. - Service context widget can be launched to display essential status information about the selected service.	Moved to the Main view, because this is considered key known error investigation information. Out-of-the-box, the Service field is a required field. This ensures that service awareness is used for routing purposes and metrics can be tracked by the selected Service. However, the field can be configured to be a not-required field.
CI	Field on Main view: **CI**	Field on Main view: **CI** Field label link opens the Service CI	Because this is considered key information, it was moved to the Main view. Out-of-the-box, the CI field is a required field when the known error is set to the Corrected status. This ensures that the causing CI is specified. However, the field can be configured to be a not-required field.
Target Date (Introduced in BMC Remedy ITSM suite 7.6.00)	Field on **Classification** tab: **Target Date**	Field on Main view: **Target Date**	The Target date is considered key information. The **Target Date** field is a required field.
Work Info	Table on **Work Info** tab	Fields and table on **Work Detail** tab (shown initially): **Notes** **First attachment** Additional fields hidden in More Details expand area: **Work Info type** 2nd and 3rd attachments **Locked** **View Access**	Key information includes Work Info entries.
Weight	Field on Main view: **Weight**	This field is not displayed but it is still calculated and completed.	The Weight field is not displayed on the Best Practice view, because it does not contain information needed to resolve the known error.

Operational Categorization	Fields on **Categorization** tab: **Tier 1** **Tier 2** **Tier 3**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** **Tier 3** Type-ahead available for all fields.	Research suggested that most BMC customers use the operational categorization fields only sporadically. This means that even when the fields are completed, they cannot be used for reporting, because they are not consistently completed. Based on this, access to the fields was moved to a tab, which you configure to appear or be hidden, according to your organization's needs. **Note:** You can specify the operational categorization values for each template.
Product Categorization	Fields on **Classification** tab: **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer**	Fields on **Categorization** tab (if configured to be displayed): **Tier 1** **Tier 2** **Tier 3** **Product Name** **Model/Version** **Manufacturer** • Type-ahead available for all fields. Auto-complete and pre-fill available for Product Name	These fields were moved to the Navigation pane, because using the CMDB is a better way to perform grouping, trending, and assignment. This, and wanting to reduce the registration time of new incident request records, means that now the product categorization is automatically completed based on the product categorization of the related service.
Category	Field on **Classification** tab: **Category**	Not available	The Category field does not appear on the Best Practice view. Requests for enhancements should flow directly from the incident management process to the change process and possibly the release management process.

Known Error Assignment	Fields on **Assignment** tab: • **Support Company** • **Support Organization** • **Assigned Group** ◦ Tooltip displaying organizational structure • **Assignee** ◦ Tooltip displaying Name, Email, Telephone, and Site • **Set Assignment using**	Fields on Main view (Work Detail tab): • **Assigned Group** ◦ Type ahead ◦ Menu button enables selection of group using organizational structure ◦ Tooltip displaying organizational structure • **Assignee** ◦ Type ahead ◦ Tooltip displaying Name, Email, Telephone, and Site ◦ Assign to Me and Auto Assign options are available as links in Quick Actions	The **Assigned Group** and **Assignee** fields contain key information.
Vendor	Fields on **Vendor** tab: **Vendor Name** **Vendor Ticket Number** **Vendor Contact** **Vendor Phone** **Internet Email** **Reported to Vendor Date** **Vendor Responded on Date**	Fields on Main view (**Work Detail** tab): **Vendor** **Vendor Ticket Number**	The number of fields displayed for Vendor assignment have been reduced to only the essential ones. Key information includes vendor and vendor ticket number details. Additional information can be registered and reviewed in Work Info.
Tasks	Available on **Tasks** tab	Available on **Tasks** tab	Space available on the screen to display tasks is bigger, leading to improved usability.

Resolution information	Fields on **Resolution** tab: **Workaround** **Root Cause** **Resolution** **Corrective Model/Version** **Patch Last Build ID** **Pre-Release Date** **General Availability Date**	Fields on Main view (**Work Detail** tab): **Workaround** **Resolution**	The number of fields displayed for Resolution on the Main view have been reduced to only the essential ones. Key information includes workaround and resolution details. Additional information can be registered and reviewed in the Work Info field as well as in the related change that corrects the root cause for the known error.
Financials	Available on **Financials** tab	No longer available	The financial functionality within the BMC Remedy ITSM suite is being redesigned. Because the majority of customers are not yet using this feature, it was removed for release 7.6.00 of the BMC Remedy ITSM suite.
Date/System	Available on **Date/System** tab	Available on **Date/System** tab with the exception of the **Problem Reported On** field	The **Problem Reported On** and **Solution Created** fields are not made available on the Best Practice view, because these dates add value neither for reporting nor resolution.
Paging System	Available as a link under Functions	No longer available	The majority of customers no longer use this feature.
Read-only behavior	When you do not have modify access, all fields are disabled and read-only	When you do not have modify access, the following message is displayed at the top of the form: You do not have permission to modify this ticket The fields are not disabled or read-only, but you cannot save any modifications.	This aids with simplification and enhances performance.

Incident Request form views

Service Desk provides different ways to view the Incident Request form:

- Best Practice view (the default view)
- Classic view

Your view is configured for you by your system administrator. For information about configuring views, see Configuring custom views.

⚠ **Note**
If a procedure differs depending on the view, both methods are described. Instructions for the Best Practice view are provided first.

Incident Management Classic view

The Classic view is the Incident Request form as it appeared in previous releases of Incident Management. This view is provided for customers who are upgrading from earlier versions of Incident Management and who are not yet ready to adopt the Best Practice view. The following fields have been added to the **Classification** tab:

- **Service** — Relates business service configuration items (CIs) to the incident request at the time it is created. Service entitlement for business service CIs are related either to the customer directly or to the customer's company, organization, or department. Only the CIs that you are entitled to see appear in the selection list for this field.
- **CI** — Provides a place for you to indicate to which piece of infrastructure the incident request pertains. This field is a *required* field when you resolve the incident, however, you can indicate the CI at any time in the incident request lifecycle.

Incident Management Best Practice view

In this view, the fields most commonly used for creating, resolving, and updating incident requests are immediately visible. You can access additional, less frequently used functionality from the tabbed sections of the form or from the links in the Navigation pane.

The order in which the fields appear on the form reflect the order in which you gather the information when you create the incident request record. This reduces the amount of time needed to create the record and improves the overall efficiency of the operation.

Also, by making the Work Detail tab visible beside the customer information when you open the record, the most important information is immediately visible when you require a quick but comprehensive overview of an existing incident request. The following list outlines the Best Practice view features:

- **Customer** field — The **Customer** field is where you record the name of the customer for whom you will be performing the work related to the incident request. For more information about this field, see Using the Customer and Contact fields in Best Practice view.
- **Contact** field — The **Contact** field is where you record the name of someone who you can contact about the incident request, if the person named in the **Customer** field is unavailable. For example, if the person named in the **Customer** field has an administrative assistant, you would enter this person's name in the **Contact** field. For more information about this field, see Using the Customer and Contact fields in Best Practice view.
- **Template** field — The **Template** field encourages the use of templates.
- **Service** field — The **Service field** relates business service configuration items (CIs) to the incident request at the time it is created. Service entitlement for business service CIs are related either to the customer directly or to the customer's company, organization, or department. Only the CIs that you are entitled to see appear in the selection list for this field.

  > ⚠ **Note**
  > The **Service** field in Incident Management behaves differently from the way that it does with other BMC Remedy ITSM Suite applications. When you open the selection menu associated with this field in other BMC Remedy ITSM Suite applications, you see all of the available services. However, when you open the selection menu associated with this field on the Incident form, you see only those services that are related in some way to the customer named in the **Customer** field. That relationship can exist either with the customer individually, or with the customer's company, organization, or department. Limiting the number of services displayed in the menu to only those that are relevant to the customer helps the service desk analyst more quickly create the incident request.

- **CI** field — The **CI** field provides a place for you to indicate to which piece of infrastructure the incident request pertains. This field is a required field when you resolve the incident, however, you can indicate the CI at any time in the incident request lifecycle.
- **Product categorization** fields — The product categorization fields are automatically filled based on the business service CI that you select in the **Service** field. This automation reduces registration time and makes

sure that the correct information is used to determine the assignment of the incident request. You can also quickly select or change operational and product categorizations from the Quick Actions area of the Navigation pane by using the Select Operational and Select Product links.

Using the Customer and Contact fields in Best Practice view

Depending on how the **Customer** and **Contact** fields are configured, you can search for a customer based on **Corporate ID**, **First Name**, **Internet Email**, **Last Name**, **Login ID**, or **Phone Number**.

If the customer record uses the **VIP** or the **Sensitive** flag, this information appears in red after the **Customer** field label.

Clicking the magnifying glass icon to the right of the **Customer** and the **Contact** fields opens the People form. From there, you can create a customer profile record if one does not exist. For more information about creating a customer profile, see Adding or modifying a customer profile.

The eraser icon to the right of the **Customer** and the **Contact** fields only clears the field's contents. It does not delete the customer profile.

For more information about creating and modifying People records from the Incident Request form, see Adding or modifying a customer profile.

Problem Investigation form views

Problem Management provides you with different ways to view the Problem Investigation and Known Error forms:

- Best Practice view (the default view)
- Classic view

Your view is configured for you by your system administrator. For information about configuring views, see Configuring custom views.

> ⚠ **Note**
> If a procedure differs depending on the view, both methods are described. Instructions for the Best Practice view are provided first.

Problem Management Classic view

The Classic view is the Problem Investigation form as it appeared in previous releases of Problem Management. This view is provided for customers who are upgrading from earlier versions of Problem Management and who are not yet ready to adopt the Best Practice view. The following fields have been added to the Classic view:

- **Service field**--(Problem Investigation and Known Error forms) The **Service** field relates business service configuration items (CIs) to the problem investigation or known error at the time it is created. All available business service CIs appear in the Service field menu and are only limited by the access levels of the person creating the problem investigation or the known error.
- **CI field**--(Problem Investigation and Known Error forms) The **CI** field specifies to which piece of infrastructure the problem investigation pertains. This field can be configured to be a *required* field when you resolve an incident; however, you can specify the CI at any time in the problem investigation lifecycle.

Problem Management Best Practice view

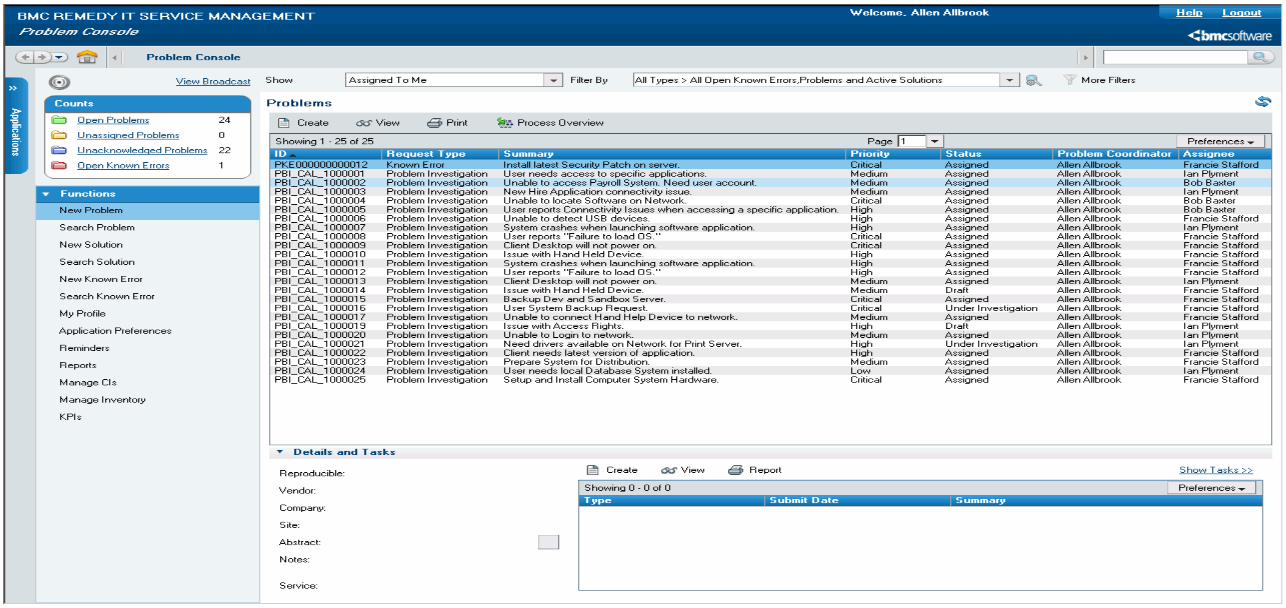
In the Best Practice view, the fields most commonly used for updating, resolving, and closing problem investigations and for working with known errors are immediately visible. You can access additional, less frequently used functionality from the tabbed sections of the form or from the links in the Navigation pane.

The following list outlines the Best Practice view features:

- **Coordinator Group** — *(Problem Investigation and Known Error forms)* Use the **Coordinator Group** field to select a support group. The support groups that appear in the menu each have at least one member with the functional role of a Problem Coordinator. From the **Coordinator Group** menu, you select the company, the organization, and then the support group. Only the selected support group name appears in the **Coordinator Group** field.
- **Problem Coordinator** — *(Problem Investigation and Known Error forms)* Use the **Problem Coordinator** field to select a Problem Coordinator for the problem investigation. The names that appear on this menu belong to the support group selected in the **Coordinator Group** field and have the functional role of Problem Coordinator.
- **Problem Location** — The **Problem Location** field specifies the location of the CI that is the focus of the problem investigation. The **Location** record includes the name of the client company, the region, the site group, and the specific site.
- **Known Error Location** — The **Known Error location** field specifies the location of the CI that is the focus of the knows error. The **Location** record is always the name of the problem coordinator company.
- **Service field** — *(Problem Investigation and Known Error forms)* The Service field relates business service configuration items (CIs) to the problem investigation or known error at the time it is created. All available business service CIs appear in the Service field menu and are only limited by the access levels of the person creating the problem investigation or the known error.
- **CI field** — *(Problem Investigation and Known Error forms)* The **CI** field specifies to which piece of infrastructure the problem investigation pertains. This field is can be configured to be a *required* field when you resolve an incident; however, you can specify the CI at any time in the problem investigation lifecycle.
- **Investigation Driver** — *(Problem Investigation form)* The **Investigation Driver** field specifies the reason for the investigation: **High Impact Incident**, **Reoccurring Incidents**, **Non-Routine Incident**, or **Other**.
- **Product and Operational Categorization** — *(Problem Investigation and Known Error forms)* If the problem investigation record is created from an incident request, the operational categorization and the product categorization fields are automatically filled, out based on the categorizations specified in the originating incident request. Likewise, when you create a known error from a problem investigation, the product categorization fields are automatically filled, based on the categorizations of the originating **Problem Management** record. If you are creating a new problem investigation or known error from within the Problem Management feature, or if the originating record did not specify a product categorization, the product categorization is filled automatically, based on the business service CI that you select in the **Service** field. You can also quickly select or change operational and product categorizations from the Classification tab. This makes sure the correct categorization information is used to manage the problem investigation.

  > ⚠ **Note**
  > If your organization does not track incident requests using categorizations, the Classification tab might not be visible on your version of the user interface.

The Best Practice view is recommended for all Problem Management users, regardless of their role.



BMC REMEDY IT SERVICE MANAGEMENT
Problem Console

Welcome, Allen Allbrook

Help Logout

Problem Console

View Broadcast

Show: Assigned To Me

Filter By: All Types > All Open Known Errors,Problems and Active Solutions

More Filters

Counts	
Open Problems	24
Unassigned Problems	0
Unacknowledged Problems	22
Open Known Errors	1

Functions
- New Problem
- Search Problem
- New Solution
- Search Solution
- New Known Error
- Search Known Error
- My Profile
- Application Preferences
- Reminders
- Reports
- Manage CIs
- Manage Inventory
- KPIs

Problems

Create View Print Process Overview

Showing 1 - 25 of 25 Page 1 Preferences

ID	Request Type	Summary	Priority	Status	Problem Coordinator	Assignee
PKE000000000012	Known Error	Install latest Security Patch on server.	Critical	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000001	Problem Investigation	User needs access to specific applications.	Medium	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000002	Problem Investigation	Unable to access Payroll System. Need user account.	Medium	Assigned	Allen Allbrook	Bob Baxter
PBI_CAL_1000003	Problem Investigation	New Hire Application connectivity issue.	Medium	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000004	Problem Investigation	Unable to locate Software on Network.	Critical	Assigned	Allen Allbrook	Bob Baxter
PBI_CAL_1000005	Problem Investigation	User reports Connectivity Issues when accessing a specific application.	High	Assigned	Allen Allbrook	Bob Baxter
PBI_CAL_1000006	Problem Investigation	Unable to detect USB devices.	High	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000007	Problem Investigation	System crashes when launching software application.	High	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000008	Problem Investigation	User reports "Failure to load OS."	Critical	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000009	Problem Investigation	Client Desktop will not power on.	Critical	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000010	Problem Investigation	Issue with Hand Held Device.	High	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000011	Problem Investigation	System crashes when launching software application.	High	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000012	Problem Investigation	User reports "Failure to load OS."	High	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000013	Problem Investigation	Client Desktop will not power on.	Medium	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000014	Problem Investigation	Issue with Hand Held Device.	Medium	Draft	Allen Allbrook	Francie Stafford
PBI_CAL_1000015	Problem Investigation	Backup Dev and Sandbox Server.	Critical	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000016	Problem Investigation	User System Backup Request.	Critical	Under Investigation	Allen Allbrook	Francie Stafford
PBI_CAL_1000017	Problem Investigation	Unable to connect Hand Help Device to network.	Medium	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000019	Problem Investigation	Issue with Access Rights.	High	Draft	Allen Allbrook	Ian Plyment
PBI_CAL_1000020	Problem Investigation	Unable to Login to network.	Medium	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000021	Problem Investigation	Need drivers available on Network for Print Server.	High	Under Investigation	Allen Allbrook	Ian Plyment
PBI_CAL_1000022	Problem Investigation	Client needs latest version of application.	High	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000023	Problem Investigation	Prepare System for Distribution.	Medium	Assigned	Allen Allbrook	Francie Stafford
PBI_CAL_1000024	Problem Investigation	User needs local Database System installed.	Low	Assigned	Allen Allbrook	Ian Plyment
PBI_CAL_1000025	Problem Investigation	Setup and Install Computer System Hardware.	Critical	Assigned	Allen Allbrook	Francie Stafford

Details and Tasks

Reproducible:
Vendor:
Company:
Site:
Abstract:
Notes:
Service:

Create View Report Show Tasks >>

Showing 0 - 0 of 0 Preferences

Type	Submit Date	Summary

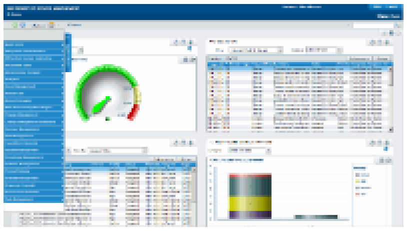
IT Home page

When you start the BMC Remedy IT Service Management Suite, the IT Home page displays the Overview console by default. However, you can set up what you want to see on the IT Home page. If you are a system administrator, you can configure the page for all users. Otherwise, you can configure your own user ID to see your views.

This topic provides the following information:

- IT Home page and its functional areas
- Configuring the IT Home page
  - To add or delete panels
  - To configure panels
  - To expand and collapse panels
  - To restore a default IT Home page view
  - To hide or show the navigation pane
- Customizing and using the IT Home page video

The following figure illustrates the functional areas of the IT Home page. Click the image to expand it.



IT Home page and its functional areas

The following table describes each of the functional areas of the IT Home page.

Functional area	Purpose
Home page header	
Logout	Click **Logout** to exit the application.
Breadcrumb bar	The breadcrumb bar helps you keep track of the records you are viewing and helps with navigation. For more information about breadcrumbs, refer to Navigating consoles, forms, and modules.
Global search	Type in a word or a phrase in the search area, and the application will search across multiple forms for records that match your input. For more information about global search, refer to Using Global search.
Navigation pane	

Applications	Depending on your permissions and other installed applications, the following links are displayed. Use them to open applications. - **Quick Links** - **AR System Administration** - **AR System Sample Application** - **Administrator Console** - **Analytics** - **Asset Management** - **Atrium Core** - **Atrium Integrator** - **Change Management** - **Change Management Dashboard** - **Contract Management** - **Data Management** - **Foundation Elements** - **Incident Management** - **Knowledge Management** - **Problem Management** - **Process Designer** - **Product Catalog** - **Release Management** - **Requester Console** - **Return On Investment** - **Service Level Management** - **Service Request Management** **Note:** When you run your mouse over the applications, you see a second menu. You can select one of those options to go directly to a form. For example, roll over **Change Management** and select **Change/Release Calendar**. The Calendar screen appears.
Configuration Buttons	Use these buttons to configure your panel display.
Overview console	
Company and **View By**	These fields combine to provide a way to indicate the company name and the assigned-to categories filtering the records in the Console List table.
Refresh	This button refreshes the data in the table.
Preferences	This button allows you to set preferences for the console list table. You can remove columns, set refresh intervals, reset and save your preferences.

Console List table	This table lists the different types of requests.

Configuring the IT Home page

You can configure the IT Home page to display information of your choice. For example, Bob Baxter is the Manager for payroll at Calbro Services. He likes to keep track of all potential problems, changes, and incidents pertaining to his department. He also tracks software license contracts so that he knows which ones are about to expire. Bob configures his panels to display all the information he is looking for, as follows:

- **Asset Management > Contracts About to Expire in 90 Days**
- **Change Management > All Open Changes with Extensive Impact**
- **Incident Management > All Open Incidents with Extensive Impact**
- **Problem Management > All Open Problems by Status and Priority**

To add or delete panels

You can specify how many panels to display on your IT Home page up to a maximum of four panels.

1. In the IT Home page, click the ⊕ button.
   Four panels appear.
2. To delete a panel, click the ⊗ button on the panel.

To configure panels

You can select what to display on your IT Home page.

> ⚠ **Note**
> You can configure your panels only with options for which you have permissions.

1. In the panel, click the **Show** list and run your cursor over the list of options.
2. From the list of work areas for each option, select the one to display (for example, **Asset Management > Software Certificates**).
   The panel displays your selection.
3. Repeat steps 1 and 2 for your other panels.
   To change display on a panel, click the ✎ button to display the **Show** list, and make another selection.
4. Click the 💾 button to save your IT Home page.
   A dialog box confirms that your customized layout has been saved.
5. Click **OK**.
   When you next log on, you will see your saved IT Home page.

To expand and collapse panels

1. In the panel, click the ▼ button.

The panel collapses.

2. In the panel, click the ▶ button.
   The panel expands to its original size.

To restore a default IT Home page view

1. In the IT Home page, click the ↺ button.
   A dialog box informs you that the default layout for this page will be brought back.
2. Click **OK** to proceed or **Cancel** to retain your current layout.
   If you click **OK**, the panels on the IT Home page disappear and the Overview Console is displayed.

To hide or show the navigation pane

In the IT Home page, click the **Applications** button to hide or show the navigation pane.

Customizing and using the IT Home page video

> **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

Using the Overview console

The information in this section is for people who fulfill one or more of the following support roles:

- Problem coordinators
- Service desk analysts
- Specialists
- Group coordinators
- On-duty managers

This section provides the following information:

- Console list table
- Overview console functional areas
- Selecting status values

Use the Overview console if you must respond to, manage, or track individual or group work assignments from a variety of sources. For example, if your company runs the full BMC Remedy ITSM suite, either you or the group you manage might receive work assignments from BMC Asset Management, BMC Incident Management, BMC Problem Management, and BMC Change Management. From the Overview console, you can quickly get information about all your work assignments and perform the procedures that you use most often.

The Overview console provides a view of work assigned across multiple applications. The implementation of the Overview console uses a BMC Remedy AR System ARDBC plug-in to provide a consolidated view of all assigned work from data sources in multiple applications without using replication of data or complex SQL views that bypass APIs.The plug-in architecture is data driven. Configuration forms define how the plug-in is set, including which forms to query, which fields to map to the table field, and an ARDBC form that performs the query.

As you work with the forms and dialog boxes associated with this console, you might see a plus sign ⊕ included in a field label. You can type part of the information next to these fields and press ENTER. If an exact match is located, the program automatically completes the field. If a selection list appears, double-click the item you want to put in the field. Using auto-fill fields and lists is faster, more consistent, and more accurate than typing the information.

Console list table

The Console List table lists different types of requests. The types of requests that you can choose from depend on the applications that are installed.

The table lists the following fields:

Field name	Description
Request ID	ID of the request. The prefix identifies each type of request. See the prefix descriptions in the following table.
Parent Request ID	ID of the parent request from which the current request was created, if applicable.
Request Type	Type of the request. Request types include: • Incident • Problem Investigation • Known Error • Change • Release • Work Order
Summary	Short description of the request
Service	Service CI related to the request
Status	Current status of the request
Priority	Priority of the request
Assignee Group	Support group to which the request assignee belongs to
Assignee	User name of the user to who the request is assigned. • BMC Change Management - Change Manager • Release Management - Release Coordinator • BMC Service Request Management - Request Manager • BMC Service Desk - Assignee

A specific prefix identifies each type of request:

Prefix	Description

CRQ	Identifies change requests. To view and define change requests, BMC Change Management must be installed.
RLM	Identifies release requests. To view and define release requests, BMC Change Management must be installed.
TAS	Identifies tasks.
SDB	Identifies solution database entries. To view and define solution entries, BMC Service Desk must be installed.
INC	Identifies incidents. To view and define incidents, BMC Service Desk must be installed.
PBI	Identifies problems. To view and define problems, BMC Service Desk must be installed.
PKE	Identifies known errors. To view and define known errors, BMC Service Desk must be installed.
PR	Identifies purchase requisitions. To view and define purchase requisitions, BMC Asset Management must be installed.

You can also change the table's contents by using the Show and Company filters at the top of the console:

- **Show** — Shows records that either are assigned to you or to your support groups.
  - **Submitted By Me** — All change requests created by you.
  - **All** — All change requests, regardless of who created them.
  - **Assigned To Me** — All change requests assigned to you.
  - **Assigned To My Selected Group** — All change requests assigned to a specific support group of which you are a member. If you select this, you are prompted to select the support group.
  - **Assigned To All My Groups** — All change requests assigned to all of the support groups of which you are a member.
- **Company** — Shows records that are created for the selected company.

If there are more entries than the system can show in the table, use the arrow keys at the right top corner of the table to scroll through the table.

Overview console functional areas

This section illustrates the functional areas of the Overview console and describes what you can do in each of the functional areas.

Overview console functional areas

Functional area	Purpose
Overview Console header	
Search	The Global search feature lets you search across multiple forms for records that match a key term.

Show/Company	This area contains the following fields: Show and Company. These fields combine to provide a way that you can filter the records in the console table. The Show field provides a filter by which you can manage the contents of the Console List table. The choices are: - **Submitted By Me** — Shows all records submitted by you. - **Assigned To Me** — Shows all records assigned to you. - **Assigned To My Selected Groups** — Asks you to select one of the groups to which you belong, and then displays the records assigned to that group. - **Assigned To All My Groups** — Displays the records assigned to or requested for all of the support groups to which you belong. The **Company** field restricts the criteria that you choose in the **Show** field for the selected company. This helps you manage the number of records returned by the **Show** field.
Refresh	Refreshes the data in the tables. **Note:** Refresh does not appear in the Overview console when it is used in the IT Home page.
Navigation pane	
View Broadcast, or **New Broadcast**	Opens the broadcast dialog box, from where you can view, create, modify, and delete broadcasts When there are unread broadcast messages, this area displays a message: `New Broadcasts`, followed by the number of new messages. When there are new broadcast messages, the area also turns red. **Note:** If you open the Overview console with no new broadcast messages, but the View Broadcast link is red, open the Application Preferences dialog box and make sure that a Console View preference has been selected.
Functions	Use the links in this area to do the following actions: - **Select Status Values** — See only those records in a certain state, which you specify from the Select Status Values dialog box. See Selecting status values. - **My Profile** — Set your profile. - **Application Preferences** — Set your program preferences and options. This function is also available from the application console.
IT Home Page	Use this link to open the IT Home Page.
ROI Console	Use this link to open the Return on Investment (ROI) console.
CMDB	Use this link to open the BMC Atrium CMDB.
Console List panel	
View	Displays a form containing detailed information about the selected record in the Console List table. In a Hub and Spoke environment, when you click **View**, you open a record directly from the spoke server.

Create	Creates a new record.
Create for Company	On a hub server in a Hub and Spoke environment, creates a record after asking you to select a company from a list of operating companies. The record is created and submitted on the spoke server where the company is defined.
Print	Displays a report of the record contents that can be printed.
Service Context	Opens the Service Context Summary view for the record selected in the console table. For more information about Service Context, see Using BMC Atrium Service Context. **Note:** The Service Context icon is only available on the Overview console when you open the Overview console from the Applications list.
Search for Ticket	Opens a dialog box from which you can select the type of ticket you are searching for. After you select the type of record from the menu, click the Select button to open a search form specific to the type of ticket you are searching for. **Note:** To see activity records and CI unavailability records, you must search for those tickets, because these records are not displayed in the Console List table.
Preferences	Using Preferences, you can control the appearance of the Console List table. For example, you can add or remove a column.
Console List table	Lists the different types of requests. See Console List table.

Selecting status values

You can use the Select Status Values dialog box to filter the requests that appear in the Overview console based on their status.

To select status values

1. From the Navigation pane, choose **Functions > Select Status Values**.
2. In the Select Status Values dialog box, select the status values for each category from the lists, then click **OK** to close the dialog box.
3. If the Assigned Work table does not refresh with the filtered records, click **Refresh** to reload the table's contents.

Using the Requester console

For organizations that do not install BMC Service Request Management, the Requester console is an interface for users to create and view their requests.From the Requester console, users can create a request that is submitted to BMC Change Management or BMC Incident Management. Depending on how the application is configured, the console might display incident requests and change requests entered on the user's behalf by support staff, in addition to the requests that the user created. Users can also view requests and respond to a survey after the request has been resolved.

Requester console users are typically employees who need assistance from the IT support staff to implement a change or resolve an incident. However, the user might not be an employee. Non-employees can also be users because non-registered users can also submit service requests.

Traditionally, after a user made a telephone call to a central help desk, a support staff member logged the request. BMC Incident Management and BMC Change Management provide user self-provisioning. Using the Requester console, users can submit, track, and (in some cases) resolve their own requests. BMC Change Management and BMC Incident Management are preconfigured to work with the Requester console. However, an organization can decide to make the Requester console unavailable.

> **Note**
> BMC Service Request Management, when it is installed, replaces the Requester console. For more information, see Service Request Management.

Requester Console users

Users of the Requester Console are usually employees who need assistance from the IT support staff. The user or requester is typically an employee in the organization who must have a change implemented or an incident resolved. But any member of your organization can be a requester.

However, the user *might* not be an employee. Non-employees can also be requesters, since non-registered users can also submit service requests. Traditionally, after a requester made a telephone call to a central help desk, a support staff member logged the request.

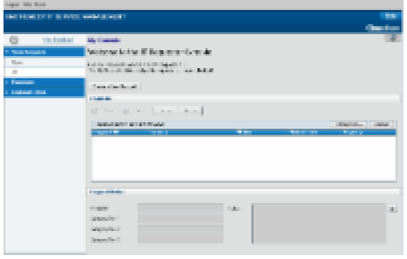
BMC Service Desk: Incident Management and BMC Change Management provide user self-provisioning. Using the Requester Console, requesters can submit, track, and (in some cases) resolve their own requests, and, as a result, improve the overall efficiency.

BMC Change Management and BMC Service Desk: Incident Management are preconfigured to work with the Requester Console. However, an organization can set an option to make the Requester Console unavailable.The Requester Console is the primary interface for requesters to define and view their requests. From the Requester Console, you can define a request that is submitted to BMC Change Management or BMC Service Desk: Incident Management. You can also view requests and respond to a survey after the request has been resolved.

The following figure illustrates the key areas on the Requester Console.

Requester Console key areas

Click the following figure to expand it.



Navigating consoles, forms, and modules

This topic describes how to navigate around BMC Remedy ITSM consoles, forms, and modules:

- What happens to data as I move back and forth on the breadcrumb trail?
- How does the breadcrumb trail behave with forms in Search mode?
- Can I force a second window to open?
- Which consoles, forms, and modules open in a new window?

In most cases, when you open consoles, forms, and modules from the IT Home page, they open inside the IT Home page view. Similarly, if you open a form from a console, the form replaces the console in the view.

Note
If you are working in a hub and spoke environment and open a spoke server record from the hub server, the spoke server record opens in its own window. Each subsequent spoke server record that you open from a hub server also opens in its own window. You can open as many spoke server windows as necessary.

Be aware that opening a spoke server record on a hub server can take a little longer than it does to open records in environments that are not configured for the Hub and Spoke capability. This is because the hub server must first determine which spoke server to connect to and then open the record in separate browser window.

If you open a related record from a form, the related record opens in the view that was occupied by the form. For example, if you are working with a problem investigation (the "parent" record) and from the parent record you open a related incident request, the incident request replaces the parent record in the view. If you then open a change request from the incident request, the change request replaces the incident request in the view, and so on. To help you keep track of the records you are viewing and to help with navigation, there is a breadcrumb bar across the top of the view field.

Note
Not all of the consoles, forms, and modules open in the view area. For example, the BMC Remedy AR System Approval Central module opens in a new window. When a console, module, or form opens in a window, it is not added to the breadcrumb bar.

The breadcrumb bar contains links to the records that you opened from the parent record. When you open a record, the breadcrumb trail expands along the breadcrumb bar to the right, with the new link. If there are more than six links in the breadcrumb trail, arrows appear at one or both ends of the bar that let you scroll back and forward on the bar to see links not currently in the view.

The first link in the breadcrumb trail indicates the place from which you started. It can be a console or a form. For example, if you open a change request record directly from the IT Home page, the first link in the breadcrumb trail takes you to the change request.

The last link corresponds to the record currently in the view. If you open a link to the left of the record currently in view, the system truncates the breadcrumb trail to that link. The history is retained, however, so you can use the back and forward arrows in the navigation controls to move through the bar one record at a time. There is also a history of your most recently viewed records, which you can use to move directly to a record. Click the down arrow to open the history list.

Note
The **Forward** button is only visible after you move back down the breadcrumb bar by opening a link to a record that you previously viewed.

The breadcrumb navigation buttons and bar
(Click the following image to expand it.)

If you are viewing a record from the middle of the breadcrumb trail and then branch off to another parent-type record, the system removes the forward breadcrumb trail from the point where you branched off and starts a new history from there, using the new parent-type record as the starting point. For example: You open a problem investigation, then open a related incident request, and from the incident request you open a related change request. If you go back to the incident request record and then open a second problem investigation, the breadcrumb bar no longer contains a link to the change request. The breadcrumb trail now shows the original problem investigation, the incident request, and the second problem investigation. It then shows any related records that you subsequently open from the second problem investigation.

When you close the parent record, the system removes the breadcrumb history.

What happens to data as I move back and forth on the breadcrumb trail?

If you are entering information into a record and open another record from the breadcrumb trail, the system prompts you to save the work, if you have not done so. If you do not save the information, the system does not preserve it on the record and you must re-enter it later.

If someone updates a record on your breadcrumb trail that is not currently in the view, those changes are visible to you when you open the record again.

How does the breadcrumb trail behave with forms in Search mode?

If you run a search from a form that is in Search mode, the last entry in the breadcrumb trail is the name of the form.

When you open a record from the search results table, that record does not appear in the breadcrumb trail. However, if you drill down through that record to open other related records, those related records *will* appear in the breadcrumb trail.

To return to the originating record, use the history list.

> ⚠ **Note**
> All of the records that you open from a form in Search mode are added to the history list.

To return to the results table, click the name of the form in the breadcrumb trail.

Can I force a second window to open?

If you press the **Shift** key and then double-click a record entry in any table, the record opens in a second window. Also, if you hold the **Shift** key and click a link, button, and so on, the form or dialog box associated with the link or button opens in another window.

> ⚠ **Note**
> If there is a record in the history list that you want to open in a second window, press the **Shift** key and then *double-click* the entry.

If you are working in a new record that has not yet been saved and open a new child type record (task, activity, CI, and so on), the system will open a new window automatically to accommodate the new child record. This prevents the information in the new, unsaved parent record from being lost.

Which consoles, forms, and modules open in a new window?

Not all of the consoles, forms, and modules open in the IT Home page's view. The consoles, forms, and modules in the following list open in a new window. If you open one of these from the IT Home page, any unsaved changes to the IT Home page are lost.

> ✓ **Tip**
> Before you open any of the following consoles, forms, or modules, save the changes to the IT Home page that you want to keep.

- BMC Action Request System Administrator
- Application Administration
- BMC Service Level Management
- Analytics
- Service Management Process Model

User interface standards for field labels

On BMC Remedy ITSM forms, field labels provide data entry hints.

The following table lists the significance of field-label formats and special characters.

Significance of field labels for data entry

Field-label format or special characters	Significance for data entry
Bold label followed by an asterisk (*)	Field is required to submit and update the form. **Note:** If you leave the field blank when you attempt to submit the form, the field is highlighted with a red border.
Field label not bolded	Field is optional.
Italicized label	System-generated value for this field. Typically this field is read-only for the user.
Label followed by a plus sign ⊕	Additional functionality is associated with this field. Typically, you access this functionality by pressing **Enter**. For example, you might press **Enter** in a field to access a search dialog box or to perform a search based on the value typed into the field. If a field label followed by a plus sign is also bolded, the field is required. Otherwise, the field is optional.

Icons used in the interface

This table describes the icons used on the consoles and in the Best Practice view of the application interface.

Icon descriptions

Icon	Description
📄	**Detail** — Displays detailed information about the field's content. For example, if you click the Detail icon associated with the Customer field, the People form appears with information about the customer whose name appears in the field.
🔍	**Search** — Searches for field contents. This icon is associated with fields that have the ability to open a search dialog box or form.
🖧	**Explore CI** — Opens the BMC Atrium Explorer for the CIs selected in the **Service** and **CI** fields.

	Clear field contents — Clears the contents of the field and allows you to make another selection. It does not delete the record.

Navigating the Incident Management interface

The following topics contain information about how to work with the Incident Management interface:

- Incident Management consoles overview
- Functional areas of the Incident Management console
- Working with the Watch List

Incident Management consoles overview

The following consoles provide access to all or a part of Incident Management:

- Requester console
- Overview console
- Incident Management console

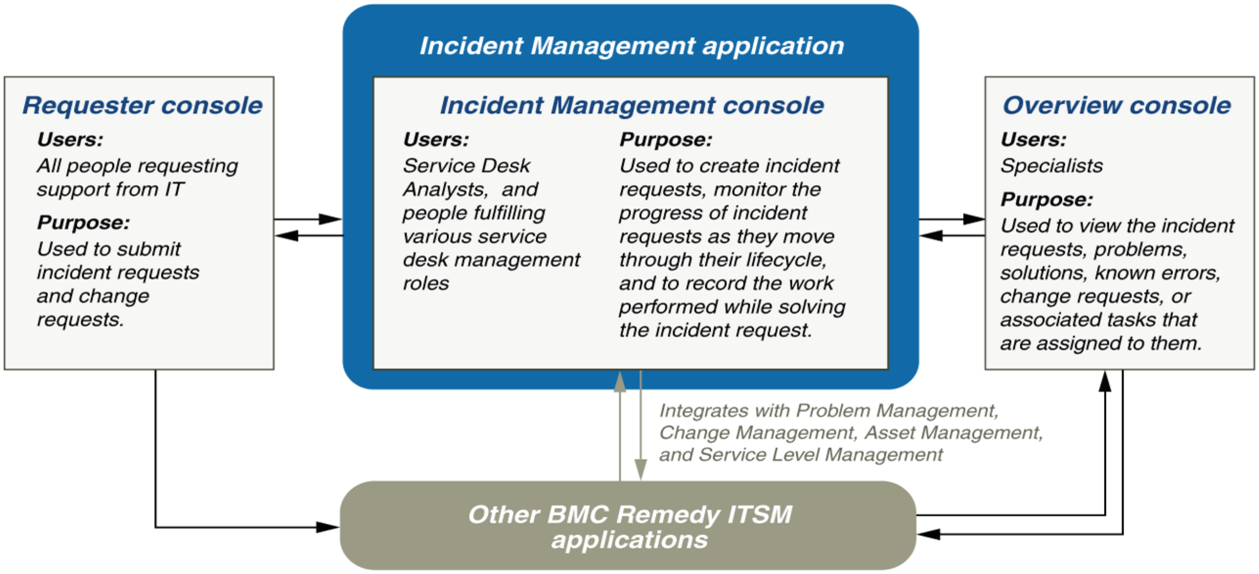
The illustration, below, shows how these consoles integrate with Incident Management and other BMC Remedy ITSM applications.

From the Requester console, IT users can submit incident requests directly to Incident Management.

Using the Overview console, service desk workers who fulfill many different roles can view incident requests that are assigned to them through Incident Management, and additional work assignments that come to them through other BMC Remedy ITSM applications with which Incident Management integrates:

- BMC Service Desk: Problem Management
- BMC Asset Management
- BMC Change Management

The Incident Management console is the main console for the application. It provides service desk workers with a single point from which they can generate incident requests, monitor the progress of incident requests as they move through their lifecycle, and record work that was performed while solving the incident request.


Incident Management application
Incident Management console
Users:
Service Desk Analysts, and people fulfilling various service desk management roles
Purpose:
Used to create incident requests, monitor the progress of incident requests as they move through their lifecycle, and to record the work performed while solving the incident request.
Requester console
Users:
All people requesting support from IT
Purpose:
Used to submit incident requests and change requests.
Overview console
Users:
Specialists
Purpose:
Used to view the incident requests, problems, solutions, known errors, change requests, or associated tasks that are assigned to them.
Integrates with Problem Management, Change Management, Asset Management, and Service Level Management
Other BMC Remedy ITSM applications

Functional areas of the Incident Management console

This table describes the areas of the Incident Management console and the features and functions that you can access from them.

Functional area	Purpose
Incident Management console header	
Plus sign	Adds a new record.
Magnifying glass	Opens the Search feature.
Breadcrumb bar	A navigation aid that contains links to related records that you opened from the current incident request. For more information about the Breadcrumb bar, see Navigating consoles, forms, and modules.
Breadcrumb navigation controls	• **Back** button takes you back one link in the breadcrumb trail. • **Forward** button takes you forward one link in the breadcrumb trail. The **Forward** button is only visible if you have returned to a record on the breadcrumb trail that you previously viewed. • Drop down menu contains links to all the records that you have viewed from the current incident request, including records that might not be currently visible in breadcrumb trail. • **Home** icon takes you to the IT Home page.
Refresh	Refreshes the data in the tables.
Search	If you have BMC Knowledge Management installed, this search feature lets you search across multiple forms for records that match a key term. For more information about using this search, see Using Global search.

Show **Filter By** Magnifying glass icon **By Role** **More Filters**	The **Show**, **Filter By,** and **By Role,** fields combine to control which incident request records appear in the Incidents table. - **Show** — This field has a menu from which you select the basic criteria by which you want to filter the contents of the Incident table, the menu choices include: - **Submitted by me** — All incident requests submitted by you - **All** — All incident requests, regardless of who submitted them - **Assigned to me** — All incident requests assigned to you - **Assigned to my group** — All incident requests assigned to a specific support group of which you are a member. If you select this, you are prompted to select the support group. - **Assigned to all my groups** — All incident requests assigned to all of the support groups of which you are a member - **Watch List** — All incident requests on the Watch List **Note:** If you select **Watch List**, **Filter By** is not available. - **Filter By** — This field places further conditions on the criteria that you chose in the **Show** and **Role** fields. This helps you to manage the number of records returned by the search. For example, if you select **Assigned To All My Groups** from the **Show** field and **Owner** from the **Role** field and **All Open > Critical Priority** from the **Filter By** field, then the Incidents table contains all records assigned to your groups for which you are the owner with the priority of Critical. - Magnifying glass icon — Click this icon to open the **Manage My Searches** dialog box from which you can edit, save, and delete custom searches. Saved custom searches appear in the My Searches list under the **Filter By** field. For more information about **Manage My Searches**, see Managing custom searches. - **By Role** — From this field, select an Incident Management assignment role: Assignee, Owner, or All (meaning Assignee or Owner, or both). The **By Role** selection combines with the **Show** selection to limit the records presented in the Incident table. For example, if you select **Assigned To All My Groups** from the **Show** field and **Owner** from the **Role** field, then all records assigned to the groups that you belong to, for which the group is the assigned owner, appear in the Incident table. You can configure a default **Role** field selection using Application Preferences. **Note:** The **By Role** field is unavailable if you select All or Submitted By Me from the **Show** menu. - **More Filters** — If you still have a large number of records after using the **Show, Role,** and **Filter By** fields, click **More Filters** to open a dialog box that contains fields in which you can indicate even more precise information, such as product or operational categories. For example, using **More Filters** you can add the product category Hardware to the filter. The funnel icon beside the More Filters link is active when a filter from this area is used.
Navigation pane	

View Broadcast, or New Broadcast	Opens the broadcast dialog box, from where you can view, create, modify, and delete broadcasts. When there are unread broadcast messages, this area displays a message: `New Broadcast`, along with the number of new messages. When there are new broadcast messages, the area also turns red. From more information, see Broadcasting messages in this table. If you open the console with no new broadcast messages, but the **View Broadcast** link is red, open the Application Preferences dialog box and make sure that a Console View preference has been selected. For information about how to view and select the Console View preference, see **Setting application preferences** in this table.
Counts	This area contains incident request metrics. The numbers relate to the selection in the **Show** field. For example, if the **Show** field contains **Submitted by me**, then the metrics that appear in this area show the open, unassigned, unacknowledged, and breached incidents that were submitted by you.
Functions	Use the links in this area to do the following actions: • **New Incident** — Create a new incident request record. See Registering incident requests. • **Search Incident** — Search the database for current incident request records. See Using Search. • **My Profile** — Set your profile. See Viewing your profile. • **Application Preferences** — Set your application preferences and application options. See Selecting the application preferences. • **Reminders** — View and create reminders. See Creating reminders. • **Reports** — Create and run custom reports. See Working with reports. • **Manage CIs** — Search for information about specific CI types and gives you access to the CI records. See Managing configuration items. • **Manage Inventory** — Access the Manage Inventory form of BMC Asset Management. See Inventory management. • **KPIs** — Click the KPIs link to select and to view the incident management flashboards. The flashboards that appear represent, in graphical format: • Process KPI — See About the KPI flashboards for information about how to use these flashboards. • Total Open Incidents — Click either **All Open** or **By Status and Priority**.
Applications	This area contains links to other BMC applications, consoles, and modules. The contents of this area depend on what other applications and so on are installed. Click the double greater-than sign to open or close this panel.
Incidents table	A list of the incident request records according to the company selected in the **Show** field and the **Filter By** field.
Create	Creates a new incident request record.
Create for Company (for Hub and Spoke installations	Creates a new incident request record after asking you to identify the company you are creating the record for.
View	Shows the incident request record that is selected in the Incidents table.

Print	Prints the selected record in the Watch List and the Incidents table.
Process Overview	Opens the detailed Incident Management process in the BMC Service Management Process Model, if the full BMC Service Management Process Model application is installed and configured. Otherwise, it opens a high-level diagram of the incident management process.
Service Context	Opens the Service Context Summary view for the record selected in the console table. The Service Context button is only available when a business service CI is associated with the incident record. If a business service CI is associated with the incident record, the CI name appears in the Service column of the Incident table. For more information about Service Context, see Using BMC Atrium Service Context.
Quick Actions	Select the action from the menu. You can perform the following quick actions: • **Assign to group member** — Reassigns the incident request to another member of your group • **Assign to me** — Reassigns the incident request to yourself • **Incident Closure** — Moves incident requests with a status of **Resolved** to the **Closed** status.
Preferences	Click Preferences to open a menu from which you can add or remove columns from the table, set the rate at which the application refreshes the table contents, or restore the default table preferences.
Detail and Tasks	**Details** — When selected, contains detailed information about the record selected in the Incidents table. To see Incident Details when the Tasks table is showing, click **Show Details**. The **Create**, **View**, and **Report** icons relate to the work information notes that appear in the table. For information about working with work information notes, see Creating work information entries from the console. **Note:** You can sort the table by clicking any of the column headings, except Notes. The table does not sort on the Notes column. **Tasks** — When selected, lets you view tasks associated with the incident request record selected in the Incidents table. To see Tasks when Details is showing, click **Show Tasks**.

Working with the Watch List

The Watch List provides a separate area where you can place records that you particularly want to monitor.

> ⚠ **Note**
> You can use the Watch List to track an incident request record throughout its lifecycle, even if it is reassigned to a group that you do not belong to. After you add an incident request record to the Watch List, it stays there until you remove it.

The following table describes how to add and remove records from the Watch List.

Working with the Watch List

Action	Note
Viewing the Watch List	From the **Defined Searches** list in the Navigation pane, click **Watchlist**.

Returning to the Incidents table	From the **Defined Searches** list in the Navigation pane , run one of the searches.
Adding records	1. From the Incidents table, select the record to add. 2. Click **Add to Watch List**. 3. When you add a record to the Watch List, it is still enabled in the Incidents table.
Removing records	1. From the Watch List table, select the record to remove. 2. Click **Remove From Watch List**. 3. This does not delete the record from the database; it only removes it from the Watch List.

Note
When you are viewing the Watch List , the **Company** and **View By** fields at the top of the Incident Management console are disabled.

Navigating the Problem Management interface

The following topics contain information about how to work with the Problem Management interface:

- Problem Management consoles overview
- Functional areas of the Problem Management console

Problem Management consoles overview

The following consoles provide access to all or a part of Problem Management:

- Problem Management console
- Overview console

The Problem Management console is the main console for the application. It provides problem coordinators and specialists with a single point from which they can create problem investigations, known error entries, and solution database entries. It also provides a place from which they can monitor the progress of problem investigations as the investigation moves through its lifecycle, and record work that was performed during the investigation.

Using the Overview console, specialists can view problem investigations that were assigned to them through the Problem Management application. The specialist role is fulfilled by all IT employees and long term contractors, other than Service Desk Analysts and IT Operators. Specialists can also view work that was assigned to them through the other BMC Remedy IT Service Management applications with which Problem Management integrates:

- BMC Service Desk: Incident Management
- BMC Asset Management
- BMC Change Management

Functional areas of the Problem Management console

This table describes the functional areas of the Problem Management console.

Problem Management console functional areas

Functional area	Purpose
Problem Management console header	
Plus sign	Adds a new record.
Magnifying glass	Opens the Search feature.
Breadcrumb bar	A navigation aid that contains links to related records that you opened from the current problem investigation. For more information about the Breadcrumb bar, see Navigating consoles, forms, and modules.
Breadcrumb navigation controls	• **Back** button takes you back one link in the breadcrumb trail. • **Forward** button takes you forward one link in the breadcrumb trail. The **Forward** button is only visible if you have returned to a record on the breadcrumb trail that you previously viewed. • Drop down menu contains links to all the records that you viewed from the current problem investigation, including records that are not currently visible in breadcrumb trail. • **Home** icon takes you to the IT Home page.
Refresh	Refreshes the data in the tables.
Search	If you have BMC Knowledge Management installed, the Global search feature lets you search across multiple forms for records that match a key term. For more information about this feature, see Using Global search.

<table>
<tr>
<td><b>Show</b>
<b>Filter By</b>
Magnifying glass icon
<b>By Role</b>
<b>More filters</b></td>
<td>
<p>The <b>Show</b>, <b>By Role</b>, and <b>Filter By</b> fields combine to control which problem investigation records appear in the Problem table.</p>
<ul>
<li><b>Show</b> — Select the basic criteria by which you want to filter the contents of the Problem table, the menu choices include:
<ul>
<li><b>Submitted by me</b> — All problem investigations created by you</li>
<li><b>All</b> — All problem investigations, regardless of who created them</li>
<li><b>Assigned to me</b> — All problem investigations assigned to you</li>
<li><b>Assigned to my group</b> — All problem investigations assigned to a specific support group of which you are a member. If you select this, you are prompted to select the support group.</li>
<li><b>Assigned to all my groups</b> — All problem investigations assigned to all of the support groups of which you are a member</li>
</ul>
</li>
<li><b>Filter By</b> — Places further conditions on the basic criteria that you chose in the <b>Show</b> and <b>Role</b> fields. This helps you manage the number of records returned by the search. If you select <b>Assigned To All My Groups</b> in the <b>Show</b> field, Problem Coordinator in the <b>Role</b> field and <b>All Open > Critical Priorities</b> from the <b>Filter By</b> field, the Problems table contains open problem investigations assigned to your groups for which you are the problem coordinator that have a critical priority.
<p>The magnifying glass icon opens the Manage My Searches dialog box from which you can edit, save, and delete custom searches. Saved custom searches appear in the My Searches list under the Filter By field. For more information about Manage My Searches, see Managing custom searches.</p>
</li>
<li><b>By Role</b> — From this field, select a Problem Management assignment role: Assignee, Problem Coordinator, or All (meaning Assignee, or Problem Coordinator, or both). The <b>Role</b> selection combines with the <b>Show</b> selection to limit the records presented in the Problem table. For example, if you select <b>Assigned To All My Groups</b> from the <b>Show</b> field and <b>Problem Coordinator</b> from the <b>Role</b> field, then all records assigned to the groups that you belong to, for which the group is the assigned problem coordinator, appear in the Problem table. You can configure a default <b>Role</b> field selection using Application Preferences.
<p><b>Note:</b> The <b>By Role</b> field is unavailable when you select one or more of the following conditions:</p>
<ul>
<li><b>All</b> or <b>Submitted By Me</b> from the <b>Show</b> menu</li>
<li><b>Solution Database</b> or <b>All Types</b> from the <b>Filter By</b> menu</li>
</ul>
</li>
<li><b>More Filters</b> — If you still have a large number of records after using the <b>Show, Role,</b> and <b>Filter By</b> fields, click <b>More Filters</b> to open a dialog box that contains fields in which you can indicate even more precise information, such as product or operational categories. For example, using <b>More Filters</b> you can add the product category Hardware to the filter. The funnel icon beside the More Filters link is active when a filter from this area is used.</li>
</ul>
</td>
</tr>
<tr>
<td><b>Navigation pane</b></td>
<td></td>
</tr>
</table>

View Broadcast, or New Broadcast	Click this link to open the broadcast dialog box, from where you can view, create, modify, and delete broadcasts. When there are unread broadcast messages, this area displays a message: `New Broadcast`, along with the number of new messages. When there are new broadcast messages, the area also turns red. For more information about broadcasting messages, see Working with broadcasts. **Note:** If you open the Problem Management console with no new broadcast messages, but the **View Broadcast** link is red, open the Application Preferences dialog box and make sure that a Console View preference has been selected. For information about how to view and select Console View preferences, see Selecting the application preferences.
Counts	This area shows the number of open, unassigned, and unacknowledged problem investigations and the number of open known errors according to the selection in the **Show** field.
Functions	Use the links in this area to do the following actions: • **New Problem** — Create a new problem investigation record. See Creating a problem investigation. • **Search Problem** — Search the database for problem investigation records. See Using Search. • **New Solution** — Create new solution database entries. See Creating a solution entry. • **Search Solution** — Search the database for solution database entries. See Using Search. • **New Known Error** — Create new known errors. See Creating a known error. • **Search Known Error** — Search the database for known errors. See Using Search. • **My Profile** — Set your profile. Viewing your profile. • **Application Preferences** — Set your application preferences and application options. See Selecting the application preferences. • **Reminders** — View and create reminders. See Creating reminders. • **Reports** — Create and run custom reports. See Working with reports. • **Manage CIs** — Search for information about specific CI types and gives you access to the CI records. Managing configuration items. • **Manage Inventory** — Access the Manage Inventory form of BMC Asset Management. See Managing inventory. • **KPIs**-Click the **KPIs** link to select and to view the problem management KPI flashboards. The flashboards that appear represent, in graphical format: ◦ Process KPI — See Using the KPI flashboards. ◦ Total Open Problems — Click either **All Open** or **By Status and Priority**.
Applications	This area contains links to other BMC applications, consoles, and modules. The contents of this area depend on what other applications and so on are installed. Click the double greater-than sign to open or close this panel.
Problems table	Displays high-level details about the records that match the criteria specified in the **Company** and **Assigned To** fields, or that were found by the most recently completed search.
Create	Opens a dialog box from which you can select to create either a **Known Error**, **Problem Investigation**, or **Solution Database** record.

Create for Company (Hub and Spoke environments only)	Opens a selection list from which you select the company you are creating the record for. You then select to create either a **Known Error**, **Problem Investigation**, or **Solution Database** record.
View	Opens the **Known Error**, **Problem Investigation**, or **Solution Database** record selected in the Problems table.
Print	Prints the details of the **Known Error**, **Problem Investigation**, or **Solution Database** record selected in the Problems table.
Process overview	If the full BMC Service Management Process Model application is installed, opens the detailed BMC Service Management Process Model Problem Management process. Otherwise, it opens a high-level diagram of the problem management process.
Service Context	Opens the Service Context Summary view for the record selected in the console table. The Service Context button is only available when a business service CI is associated with the problem investigation. If a business service CI is associated with the problem investigation, the CI name appears in the Service column of the Problems table. For more information about Service Context, see Using BMC Atrium Service Context.
Preferences	Click Preferences to open a menu from which you can add or remove columns from the table, set the rate at which the application refreshes the table contents, or restore the default table preferences.
Details and Tasks	**Details** — When selected, contains detailed information about the record selected in the Problems table. To see Details when the Tasks table is showing, click **Show Details**. The Create, View, and Report icons relate to work information notes. For information about working with work information notes, see Creating Work Information entries. **Note:** You can sort the table by clicking any of the column headings, except Notes. The table does not sort on the Notes column. **Tasks** — When selected, lets you view tasks associated with the record that is selected in the Problems table. To see **Tasks** when **Details** is showing, click **Show Tasks**.

Using Search

You can search for records from the application consoles. To do this, you can run a series of predefined searches, search all of the records using the Search form, or create and save your own custom searches using advanced qualifications.

This section describes the following tasks:

- Managing custom searches
- Searching all records
- Using Global search
- Searching all records from a hub server

Methods of searching records

Method	Description	Reference to instructions

Predefined search	Quickly find records for which you frequently search. You can create custom searches.	Managing custom searches
Searching all records	Use this type of search when you are looking for record that is not associated with your ID or your group's ID, or any time you search all of the records.	Searching all records
Advanced search (for BMC Asset Management only)	Search for computer systems with specific components. For example, you can search for all computer systems running a specific patch or operating system.	Performing an advanced CI search
BMC Atrium CMDB advanced CI search (for BMC Asset Management only)	Use the BMC Atrium CMDB query dialog box to build complex searches.	Using the BMC Atrium CMDB query dialog box to search for CIs

Managing custom searches

You can define and save custom searches. Custom searches using advanced qualifications allow you to create searches with very specific search criteria, which you can save for reuse. After you save the custom search, it appears in the My Searches list of the Manage My Searches dialog. It is also listed in My Searches list under the **Filter By** field.

> ⚠ **Note**
> The My Searches options is listed only after a custom search is defined.

In BMC Asset Management, you can also create custom searches on the Contract Management console and on the Software Asset Management console.

This topic contains the following information:

- To define a custom search
- To edit or delete a custom search filter

To define a custom search

1. At the top of the console, click the 🔍 icon beside the **Filter by** field.
2. On the Manage My Searches dialog, in the **Search Name** field type a name for the search.
3. Click **Build Search Qualification** to open the Advanced Qualification Search Builder dialog box, and then define the search qualification.
4. From the **Keywords** or **Fields** selection boxes, select the keywords or record fields on which you want to search.
5. To insert operators (+, =, >,<, and so on), click the appropriate operator button. Place literal values between double quotation marks:

```
'Urgency' = $NULL$
'Priority' = "High"
```

Example
If Allen Allbrook is performing an incident request review and he needs to search for incident requests that meet the following criteria:

- Impact => 2-Significant/Large or 1-Extensive/Widespread
- Service = Payroll Service

```
('Impact' = 2-Significant/Large" OR
'Impact' = "1-Extensive/Widespread")
AND 'Service' = Payroll Service" AND
'Last Resolved Date' >= 07/19/2008"
```

To search for articles where Business Service = Payroll Service:

```
'Business Service' ="Payroll Service" AND
'Last Resolved Date' >= "07/19/2010"
```

6. Click **Select** to close the Advanced Qualification Builder, and then click **Save**.
7. Close the Manage My Searches dialog box.
   The search appears in the My Searches list of the **Filter by** field.

To edit or delete a custom search filter

1. At the top of the console, click the icon beside the **Filter by** field to open the Manage My Searches dialog box.
2. Under My Searches, select the search filter that you want to modify or delete.
3. To modify the search filter, edit it as necessary and then click **Save**.
4. To delete the search filter, click **Delete**.
5. Click **Close**.

Searching all records

The following procedure describes how to search all records. Use this type of search when you are looking for record that is not associated with your ID or your group's ID, or any time you search all of the records.

To search all records

1. From the application console navigation pane, choose **Functions > Search *application***, where *application* is either Work order, Change, Release, Knowledge, Problem or Incident.
   A form appears that you can use to perform the search. The form is laid out in a similar way as the actual request form. It contains the same tabs and the same fields.
2. Use the tabs and fields to build your search conditions.
   To reduce the number of records found by the search, enter as much information into the form as you can.

> ⚠ **Note**
> If the **Customer** field is configured to search on an attribute other than **First Name** or **Last Name**, you can still search using the customer's name by opening the **Additional Search** tab and using the **First Name** or **Last Name** fields.

3. When you finish entering your search criteria, click **Search**.
   When the search finishes, the search results table lists all the records that match the search criteria.

   > ⚠ **Note**
   > The search criteria are persistent. This means that if you run a search and then close the application, the next time that you open the application and perform this procedure, the search criteria that you entered in this step are still present in the search form. They remain until you change or delete them.

4. Scroll through the table to find the specific record you want.
5. When you find the record, select it to display in **Modify** mode.

   > ⚠ **Note**
   > When you open a record from the search results table, it is added to the history list, but not to the breadcrumb bar. However, any related records that you open from the record do appear in the breadcrumb bar and get added to the history list.

Using Global search

If you have BMC Knowledge Management installed, you can use the Global search feature in any of the BMC Remedy ITSM application consoles.

Global search searches across multiple forms for records that match a word or phrase that you type in the search area.

> ⚠ **Note**
>
> - Global search results include information only from the forms that you have permission to access. That is, you need permission to access an application to have its records appear in the search results.
> - The Global search does not include BMC Asset Management CI's .

This topic provides the following information:

- To use Global search
- Limitation
- Special characters and boolean expressions in Global search
- Related topics

To use Global search

1. In the text field to the right of the breadcrumb bar, type your search string and then click the Search icon.

   Global search

2. Locate the record you want in the search results table and double-click it.
   The record opens in the viewing area and the system updates the breadcrumb trail with an entry for the record you opened.

   > **Note**
   > As you drill down through the record, each record you open is also added to the breadcrumb trail.
   >
   > If you want to maintain the contents of the search results table to view later, do not change the text in the Search field. If you do, when you click the **Search** icon to return to the search results table, the search feature will execute a new search based on the changed content of the Search field.

3. To return to the search results table, click the **Search** icon again.

Limitation

Global search results might include external files that have been registered as knowledge base items. If the search conditions are fulfilled by XML or HTML files that have been registered in this way, the Global Search Results screen appears distorted due to the tags that are used in XML and HTML files. Additionally, the **Advanced search** link on the search results screen becomes unresponsive.

Asset CIs are not included in the Global Search.

Special characters and boolean expressions in Global search

Global search uses Full Text Search (FTS) to find the search strings in requests and other records. Some characters are used to control the search criteria, as indicated in the following table.

Special characters and their results

Special character	Results	Example search string	Example results
"	Performs a phrase search on the terms enclosed in double-quotation marks (")	"firewall blocked"	• firewall blocked her access • firewall blocking my access

,	Find requests that contain any of the specified words	- firewall, blocking - "firewall, blocking"	- firewall blocks access - firewall will block access - firewall is not working - try blocking his access
%	Wildcard to extend the search **Note:** You do not need to use a wildcard to extend the search for word stems, such as "ed," "s", and "ing," because word stems are automatically included.	%fire%	- backfire - file - firewall

> **Note**
> Searches that start with a wildcard character are not as efficient as searches that use an exact phrase or a trailing wildcard. For example, searching for the term "%block" is less efficient than searching for either "block" or "block%".

You can use use boolean expressions in your search. Boolean operators include parentheses (), AND, OR, and NOT. The boolean operators must be specified in upper case; otherwise, they are treated as search strings.

Boolean operators and their results

Boolean operator	Results	Example search string	Example results
AND	Find requests that contain all of the specified words and phrases	firewall AND blocking	- firewall blocks access - firewall will block access

OR	Find requests that contain any of the specified words and phrases	firewall OR blocking	• firewall blocks access • firewall will block access • firewall is not working • try blocking his access
NOT	Exclude the specified word or phrase	firewall NOT blocking	firewall is not working
()	group expressions	firewall AND (block, allow)	• firewall blocking access • set up firewall to allow access

Global search results reflect both the search terms and the configuration of full text search. Configurable options that affect search results include case sensitivity, the list of ignored words, thesaurus, and stemming. For more information about full text search, see Enabling full text search.

Related topics

Configuring Full Text Search (FTS)

Global search indexed fields

This section provides a list of the fields on each form that are indexed for use by Global search. The information in these fields can be found by Global search.

The following topics are provided:

Activity form indexed fields

The following is a list of the fields on the Activity form (AAS:Activity) that are indexed for use by Global search.

Field	Field ID
Activity ID	1000000182
Assignee	1000003230
Assignee Support Company	1000003228
Assignee Support Group	1000003229
Assignee Support Organization	1000003227
Company	1000000001
Notes	1000000151
Region	200000012
Request ID	10000006
Site	260000001
Site Group	200000007
Summary	1000000000
z2TF Work Log Description	301389926
z2TH WorkLog	301389923

Help Desk form indexed fields

The following is a list of the fields on the Help Desk form (HPD:Help Desk) that are indexed for use by Global search.

Field	Field ID
Assigned Group	1000000217
Assigned Support Company	1000000251
Assigned Support Organization	1000000014
Catagorization Tier 3	1000000065
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Closed Date	1000000564
Company	1000000082
Contact Last Name	1000005782
Customer Last Name	1000000018
Detailed Description	1000000151
Incident Number	1000000161
Manufacturer	240001003
Owner	1000000715
Owner Group	1000000422

Owner Support Company	1000000426
Owner Support Organization	1000000342
Product Categorization Tier 1	200000003
Product Categorization Tier 2	200000004
Product Categorization Tier 3	200000005
Product Model/Version	240001005
Product Name	240001002
Region	200000012
Reported Date	1000000560
Resolution	1000000156
Service	303497300
Service Request ID	301572100
Site	260000001
Site Group	200000007
Summary	1000000000
z2TF Work Log Description	301394446
z2TH HPD Worklog	301389614

Infrastructure Change form indexed fields

The following is a list of the fields on the Infrastructure Change form (CHG:Infrastructure Change) that are indexed for use by Global search.

Field	Field ID
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065
Change Coordinator	1000003230
Change Coordinator Group	1000003229
Change Coordinator Support Company	1000003228
Change Coordinator Support Organization	1000003227
Change Manager	1000000403
Change Manager Group	1000000015
Change Manager Support Company	1000000251
Change Manager Support Organization	1000000014
Company	1000000001
Customer Last Name	1000003298

Detailed Description	1000000151
Infrastructure Change ID	1000000182
Manufacturer	1000002270
Product Categorization Tier 1	1000001270
Product Categorization Tier 2	1000001271
Product Categorization Tier 3	1000001272
Product Model/Version	1000002269
Product Name	1000002268
Region	200000012
Service	303497300
Service Request ID	301572100
Site	260000001
Site Group	200000007
Summary	1000000000
Vendor fields	
z2TF Work Log Description	301389926
z2TH Worklog	301389923

Known Error form indexed fields

The following is a list of the fields on the Known Error form (PBM:Known Error) that are indexed for use by Global search.

Field	Field ID
Assigend Group	1000000217
Assigned Group Pblm Mgr	1000000837
Assigned Support Company	1000000251
Assigned Support Organization	1000000014
Assignee	1000000218
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065
Company	1000000001
Detailed Description	1000000151
Known Error ID	1000000979
Manufacturer	240001003
Product Categorization Tier 1	200000003

Product Categorization Tier 2	200000004
Product Categorization Tier 3	200000005
Product Model/Version	240001005
Product Name	240001002
Service	303497300
Summary	1000000000
Support Company Pblm Mgr	1000000834
Support Organization Pblm Mgr	1000000835
Tempoarary Workaround	1000000855
Vendor Name	1000000396
z2TF Work Log Description	301389897
z2TH PBM Worklog	301389875

Problem Investigation form indexed fields

The following is a list of the fields on the Problem Investigation form (PBM:Problem Investigation) that are indexed for use by Global search.

Field	Field ID
Assigend Group	1000000217
Assigned Group Pblm Mgr	1000000837
Assigned Support Company	1000000251
Assigned Support Organization	1000000014
Assignee	1000000218
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065
Company	1000000001
Detailed Description	1000000151
Manufacturer	240001003
Problem Investigation ID	1000000232
Product Categorization Tier 1	200000003
Product Categorization Tier 2	200000004
Product Categorization Tier 3	200000005
Product Model/Version	240001005
Product Name	240001002
Region	200000012

Service	303497300
Site	260000001
Site Group	200000007
Summary	1000000000
Support Company Pblm Mgr	1000000834
Support Organization Pblm Mgr	1000000835
Temporary Workaround	1000000855
Vendor Name	1000000396
z2TF Work Log Description	301389897
z2TH PBM Worklog	301389875

Release form indexed fields

The following is a list of the fields on the Release form (RMS:Release) that are indexed for use by Global search.

Field	Field ID
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065
Company	1000000001
Detailed Description	1000000151
Manufacturer	1000002270
Product Categorization Tier 1	1000001270
Product Categorization Tier 2	1000001271
Product Categorization Tier 3	1000001272
Product Model/Version	1000002269
Product Name	1000002268
Region	200000012
Release Coordinator Group	1000000015
Release Coordinator	1000000403
Release Coordinator Support Company	1000000251
Release Coordinator Support Organization	1000000014
Release ID	303489800
Service	303497300
Site	260000001
Site Group	200000007
Summary	1000000000

Vendor fields	
z2TF Work Log Description	301389926
z2TH Worklog	301389923

Solution Database form indexed fields

The following is a list of the fields on the Solution Database form (PBM:Solution Database) that are indexed for use by Global search.

Field	Field ID
Abstract	1000000000
Assigend Group	1000000217
Assigned Support Company	1000000251
Assigned Support Organization	1000000014
Assignee	1000000218
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065
Company	1000000001
Department	200000006
Manufacturer	240001003
Organization	1000000010
Product Categorization Tier 1	200000003
Product Categorization Tier 2	200000004
Product Categorization Tier 3	200000005
Product Model/Version	240001005
Product Name	240001002
Region	200000012
Searchable	1000001469
Site	260000001
Site Group	200000007
Solution	1000001203
Solution Database ID	1000001204
Summary	1000001202
z2TF Work Log Description	301389897
z2TH PBM Worklog	301389875

Task form indexed fields

The following is a list of the fields on the Task form (TMS:Task) that are indexed for use by Global search.

Field	Field ID
Assignee	10010413
Assignee Support Company	1000000251
Assignee Support Group	10002506
Assignee Support Organization	1000000014
Catagorization Tier 3	1000000065
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Company	1000000001
Customer Last Name	1000003298
Manufacturer	1000002270
Name	10007000
Notes	10000101
Product Categorization Tier 1	1000001270
Product Categorization Tier 2	1000001271
Product Categorization Tier 3	1000001272
Product Model/Version	1000002269
Product Name	1000002268
Region	200000012
Request ID	10000006
Site	260000001
Site Group	200000007
Summary	8
Task ID	1
z2TF_WorkInfoSummary	10000547
z2TH_Worklog	10000523

Work Order form indexed fields

The following is a list of the fields on the Work Order form (WOI:WorkOrder) that are indexed for use by Global search.

Field	Field ID
Categorization Tier 1	1000000063
Categorization Tier 2	1000000064
Categorization Tier 3	1000000065

Company	1000000001
Customer Last Name	1000003298
Detailed Description	1000000151
Manufacturer	1000002270
Product Categorization Tier 1	1000001270
Product Categorization Tier 2	1000001271
Product Categorization Tier 3	1000001272
Product Model/Version	1000002269
Product Name	1000002268
Region	200000012
Request Assignee	1000003230
Request Assignee Support Organization	1000003227
Request Assignee Support Company	1000003228
Request Assignee Support Group	1000003229
Request Manager	1000000403
Request Manager Group	1000000015
Request Manager Support Company	1000000251
Request Manager Support Organization	1000000014
Service	200000020
Service Request ID	301572100
Site	260000001
Site Group	200000007
Summary	1000000000
Work Order ID	1000000182
z2TF Work Log Description	301389926
z2TH WorkLog	301389923

Searching all records from a hub server

The search form described in this procedure is associated only with hub and spoke environments.

Use this type of search from the hub server when you are looking for a record not associated with your ID or your group's ID, or any time you must search all records.

Note
The hub and spoke search is limited to only the fields that you see on the Hub and Spoke Search form.

To search all records

1. From the Navigation pane of the hub server, choose **Functions > Search *applicationName***.
   The Hub and Spoke Search console appears.
2. Enter the search criteria.
3. When you finish entering your search criteria, click **Search**.
   When the search finishes, the search results list contains all the records that match the search criteria.
4. Scroll through the results list to find the specific records that you want.

   > ⚠ **Note**
   > When you open a record from the search results table, it is added to the history list, but not to the breadcrumb bar. However, any related records that you open from the record do appear in the breadcrumb bar and get added to the history list

Recording effort spent on an investigation

You can record time spent working on the investigation. The **Effort Time Spent** field is an informational field that tracks the time spent on the investigation per session.

> ⚠ **Note**
> You perform this task in the Classic view.

To record effort spent on an investigation

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. In the Navigation pane, choose **Advanced Functions > Track Effort**.
3. Complete the Investigation Effort Log dialog box as appropriate.
   You can change the assignee effort duration for your own effort logs, but not those of another support group or individual.

   > ⚠ **Note**
   > The time values in the **Effort Duration Hours** and **Minutes** fields are not filled in by the system. You must type these values manually. Also, if you are updating the **Effort Duration**, you must make the calculations manually and then type the new values in the **Hours** and **Minutes** fields. For example, if you previously logged 10 minutes on a problem investigation and then spent an additional 90 minutes on the investigation (for a new total of 1 hour and 40 minutes), you type 1 in the **Hours** field and 40 in the **Minutes** field.

4. Click **Add** to save your total effort time in the effort log.
5. Click **Close** to close the dialog box.

Recording CI unavailability in Incident Management

CI unavailability is the actual down-time of a CI. You can record CI unavailability due to an unexpected circumstance from the incident.

⚠ **Note**
You can record CI unavailability only if BMC Asset Management is installed.

To record CI unavailability

1. Open the incident request record.
2. Click the **Relationships** tab.
3. From the **Request Type** list, select **Configuration Item**, and then click **Search**.
4. Click inside the CIs table to refresh the contents and then select the CI record against which you want to record the unavailability.
5. In the **Relationship Type** field of the CI Relationships Search dialog box, select the relationship type.
6. Click **Relate with Unavailability**.

   ⚠ **Note**
   Relate with Unavailability is available only when you are searching for CIs to relate to an incident.

7. In the **Unavailability Type** list, select whether the unavailability is scheduled or unscheduled, and whether it is full or partial unavailability.
8. Select the actual start date of the unavailability.
9. Complete additional fields of the form, as appropriate.
10. Click **Save**.
11. Close the CI Relationship Search dialog box.

Relating incident requests and problem investigations

By defining and maintaining relationships among records, you can create a more sophisticated overview of the connections and interdependencies among the current problem investigation and additional service issues being tracked by your system.

This topic contains information about:

- Relationship types
- Copying relationships
- Defining relationships
- Indicating impacted areas
- Modifying relationship types
- Performing quick actions on a relationship
- Removing relationships

Relationship types

Incident requests and problem investigations make different relationship types, as described in the following sections:

- Incident requests
- Problem investigations

Incident requests

An incident request can be related to any of the following record types:

- Configuration item (CI)
- Another incident
- Solution database entry
- Known error
- Problem investigation

Additionally, if your environment runs BMC Asset Management and BMC Change Management, incident requests can also be related to the following record types:

- CI unavailability
- Release
- Infrastructure change

Problem investigations

A problem investigation can be related to any of the following record types:

- CI
- Incident request
- Solution database
- Known error
- Another problem investigation

Additionally, if your environment runs BMC Asset Management and BMC Change Management, a problem investigation can also be related to the following record types:

- Configuration item (CI) unavailability
- Infrastructure change

A known error can be related to any of the following record types:

- Configuration item
- Incident request
- Solution database
- Another known error
- Problem investigation

If you have BMC Change Management, a known error can also be related to infrastructure change or a release record.

> ⚠ **Note**
> You cannot define a relationship *from* a solution database record *to* another record type. You can only define a relationship *to* a solution database record *from* another record type. For example, from an open incident request, you can create a relationships to a solution database record. You cannot, however, create a relationship from an open solution database record to an incident request.

Copying relationships

When you define a relationship between the current record and another record, the other record might already have one or more records related to it. To more thoroughly document all the record relationships, you can chose to relate the other record's related records to the current record. For example: you are creating a relationship between Incident Request Record A and CI B. Unknown to you, CI B already has a relationship with Incident Request Record C. However, by using the procedure described in this section, you discover the relationship between CI B and Incident Request Record C and subsequently decide to make a relationship between Incident Request Record A and Incident Request Record C. To view the other record's other relationships and relate them to the current incident request record, use the procedure that follows.

> ⚠ **Note**
> You cannot use this procedure to copy related CIs.

To copy relationships

1. Open the incident request or problem investigation record.
2. Click the Relationships tab.
3. From the Relationships table, select the record with the other relationships that you want to copy.
4. From the **Quick Actions** list on the Relationships tab, select **Get Related Relationships**, then click **Execute**
   .
   The Copy Related Relationships dialog box appears. This dialog box contains a table of all other records related to the record you selected in Copying relationships.
5. From the table of related records, select the other record that you want to relate to the current record.

   > ⚠ **Note**
   > To see the details of the other record, select it, then click **View**. A form appears with detailed information about the selected record. Use this feature to help you determine whether you want to relate the other record to the current record.

6. Click inside the **Relationship Type** field.

   > ⚠ **Note**
   > The contents of the **Relationship Type** list depends on the type of record you are trying to create the relationship with.

7. Select the type of relationship you want to create, and then click Select.
8. Click **OK** to dismiss the note that confirms the relationship creation.
9. Close the Copy Related Relationships form.
   The newly created relationship appears in the Relationships table.

Defining relationships

Use the following procedures to define a relationship:

- To define a relationship (Classic view)
- To define a relationship (Best Practice view)

> ⚠ **Note**
> Work info records are tied to the record on which they are created. This means that when you create a relationship among records, you can only view a work info record from the record where it was originally created.

To define a relationship (Classic view)

1. Open the incident request or problem investigation record.
2. Click the **Relationships** tab.
3. From the **Request Type** list, select the type of record you want to relate the current record to.
4. Click **Search**.
5. In the dialog box that appears, complete the search criteria tabs with the relevant information, and then click **Search**.

   > ⚠ **Note**
   > The content of the dialog box depends on the type of record you chose in the **Request Type** list. Try to supply as much information as possible in the search dialog box to reduce the overall number of records returned by the search.

6. From the search results table that appears, select the request type with which you want to create the relationship.
7. From the **Relationship Type** list at the bottom of the search dialog box, select the type of relationship you want to create.
8. Create the relationship by clicking the appropriate relate button at the bottom of the dialog box.

   > ⚠ **Note**
   > The specific text on the relate button depends on the type of relationship you are creating. For example, if you are in Incident Management and you are creating a relationship with another incident request record, the button reads Relate. If you are creating a relationship with a known error, there are two relate buttons: **Relate With Solution** and **Relate Without Solution**, and so on.

9. Click **OK** to dismiss the dialog box.

To define a relationship (Best Practice view)

1. Open the incident request or problem investigation record.
2. In the Quick Actions area, click the arrow beside **Create Relationship to**.
3. From the menu, select the type of record to you want to relate the current record to.

> ⚠ **Note**
> If BMC Knowledge Management is installed in your environment, then continue with this procedure. Otherwise, go to step 5 of To define a relationship (Classic view) and complete that procedure.

4. In the **Search** field of the dialog box that opens, type a search string. For example, if you are creating a relationship to an incident request about a printer that regularly goes off-line, you might type **printer off line**. The search scans multiple fields in each record looking for a match, and returns a list of records that contain the phrase "printer off line" in one of the scanned fields.

> ⚠ **Note**
> The type of search dialog box that appears depends on the type of record you chose from the menu. Try to supply as much information as possible in each type of search to reduce the overall number of records returned by the search. If, after using a more specific search string, the search returns too many records, consider using the advanced search. To do this, click **Use Advanced Search**, which opens a form in search mode that is relevant to the type of relationship you are making. This search behaves the same way as the search described in To define a relationship (Classic view).

5. From the search results table, select the specific record to which you want to create the relationship.
6. From the **Relationship Type** list at the bottom of the search dialog box, select the type of relationship you want to create.
7. Create the relationship by clicking the appropriate relationship type button at the bottom of the dialog box.

> ⚠ **Note**
> The specific text on the relate button depends on the type of relationship you are creating. For example, if you are creating a relationship with another incident request record, the button reads **Relate**. If you are creating a relationship with a known error, there are two relate buttons: **Relate With Solution** and **Relate Without Solution**, and so on.

8. Click **Close** to dismiss the dialog box.

Indicating impacted areas

The Impacted Areas dialog box gives you a place to show the region, site, location, and so on, that are affected by the content of the record. Use the following procedure to indicate the impacted areas.

To indicate an impacted area

1. Open the incident request, problem investigation, or known error record.
2. In the Navigation pane, choose **Advanced Functions > Impacted Areas**.
3. In the Navigation pane, choose **Functions > Impacted Areas**.
4. From the Impacted Areas dialog box, select items from the various lists that help describe the impacted area appropriate for the incident you are working on, for example, **Company**, **Region**, and so on.

> ⚠ **Note**
> Required fields are marked with an asterisk.

5. Click **Add**.

> ⚠ **Note**
> You can add as many impacted areas as necessary. You can also delete areas that you have previously chosen in this dialog box.

6. When you finish indicating the impacted areas, click **Close**.

Modifying relationship types

After you define a relationship, you can change the relationship type and update the relationship description. Use the following procedure to modify the relationship.

To modify a relationship

1. Open the incident request or problem investigation record.
2. Click the **Relationships** tab.
3. From the Relationships table, select the relationship you want to modify.
4. From the Quick Actions list, select **Modify Relationship Type**, and then click **Execute**.
5. Enter the new relationship details according to the onscreen instructions.
6. Click **Save** to save your changes.

Performing quick actions on a relationship

You can perform many other actions on a relationship. For a list of these actions, see the tables in the following procedure.

To perform a quick action

1. Open the incident request or problem investigation record.
2. Click the **Relationships** tab.
3. From the Relationships table, select the relationship entry for which you want to perform the action.
4. From the **Quick Actions** list, select the action you want to perform, such as **Get Impacted Areas**.
The following table lists available quick actions for any related item:
Effects of general relationship actions

Relationship action	Effect
Get Related Relationships	Copies the relationships of the selected record to the current incident's relationships
Modify Relationship Type	Prompts you to modify the relationship type, as described in Modifying relationship types

More quick actions are available when you select a related configuration item, as indicated in the following table:

Relationship action	Effect

BMC Atrium Explorer	Opens a graphical relationship viewer that shows a selected CI's relationship with other records
Create New CI Unavailability	If BMC Asset Management is installed, creates CI unavailability for the selected CI
Get CI Impact/Urgency	Copies the impact and urgency of the selected CI
Get CI Product Categorization	Copies the product categorization from the selected CI to the classification of the current incident
Get CI Resolution Product Cat.	Copies the product categorization from the selected CI to the resolution of the current incident
Get Impacted Areas	If BMC Asset Management is installed, prompts you to select impacted areas, as defined in the selected CI, into the current incident's impacted areas

5. Click **Execute**.

Removing relationships

Use the following procedure to remove a relationship.

To remove a relationship

1. Open the incident request or problem investigation record.
2. Click the Relationships tab.
3. In the Relationships table, select the relationship you want to remove.
4. Click **Remove**.
5. Click **Yes** when prompted to confirm the removal.

Printing records

You can print a copy of a record to keep for filing purposes or to share with someone who does not have access to BMC Service Desk.

To print a record

1. Open the record that you want to print.
2. Click **Print** at the bottom of the form to open the Business Objects Report Preview dialog box.
   The Business Objects Report Preview dialog box appears, enabling you to view the record before you print it.
3. Click the **Print** icon on the menu bar at the top of the dialog box.
4. When the print confirmation dialog box appears, click the **Print** icon to send the record to your local printer.
5. Close the Business Objects dialog box.

Modifying records

After you generate a record, you can modify or update the information it contains. Use the following procedure to modify a record.

To modify a record

1. Open the record that you need to modify.
2. Click the field, tab, or link in the Navigation pane that contains or takes you to the information you want to update.
3. Make the appropriate changes.
4. Click **Save**.

Using Incident Management scripts

Scripts are detailed instructions that have been set up at your company to help you record important information about an incident request. You have access only to scripts that have been set up for your support group. Scripts might include a list of questions to ask the user. These questions can assist you in resolving or assigning the incident.

The following list describes the types of scripts:

- Initiator scripts — Select an initiator script when you record an incident after you indicate the user.
- Assignment scripts — Select an assignment script when you assign or reassign an incident after you indicate the assignee. The assignment scripts correspond to the group to which you are assigning the incident. For example, a networking group might have specific questions for you to ask the user when you assign the incident.

This topic contains information about how to use the following script types:

- To use an Initiator script
- To use an Assignment script

To use an Initiator script

1. On the Incident Management console, click **Create**.
2. Record the user's information in the Customer field.
3. From the Navigation pane, select **Advanced Functions > Initiator Script**.
4. From the Navigation pane, select **Functions > Initiator Script**.

To use an Assignment script

1. On the Incident Management console, open an incident request record or click **Create.**
2. Ensure the user's name is recorded in the **Customer** field.
3. From the Navigation pane, select **Advanced Functions > Assignment Script**.
4. From the Navigation pane, select **Functions > Assignment Script**.

Using the Incident Management decision tree

A decision tree takes you step-by-step through a questionnaire. Based on your answers, the decision tree completes part of the form for a new incident request record. Each element in the decision tree displays a list of items. Your final selection completes part of the incident.

Decision trees are built by a manager or administrator at your company.

You can set up your preferences to use available decision trees whenever you start a new incident. For information about setting up your application preferences, see Selecting the application preferences.

For information about configuring decision trees, see Configuring decision trees.

Disclaimer
Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

[!common:_graphicsLibrary^video_icon.png!|www.youtube.com/watch?v=CZoBd5208eM] [View video on YouTube|www.youtube.coı

Tracking costs

The **Financials** tab on the Classic view of the Problem Investigation form shows the financial effect of the problem on a company or site. Knowing how much an unresolved problem costs helps you determine whether and when to perform a formal problem investigation.

This tab displays Investigation Costs. If BMC Asset Management is installed, this tab also displays Cost of CI Unavailability.

You can record the cost involved in working on a problem investigation. If the problem investigation is related to an incident with CI unavailability, you can update the costs of CI unavailability.

Note
The CI unavailability feature is available when BMC Asset Management is installed and is used to track both scheduled and unscheduled outages against CIs.

Recording the cost of working on an investigation

You can record the costs of working on the investigation by using the **Financials** tab on the Problem Investigation form.

Note
Recording the cost of working on an investigation is performed from the Classic view.

To record the cost of working on an investigation

1. With the relevant Problem Investigation form open, click the **Financials** tab.
2. In the Investigation Cost area, click **Create**.

The **Cost Category** field is set to Problem Investigation. This indicates the form from which you entered the charge. You cannot change this value.

3. On the Cost form, select the appropriate cost center code from the list.
   This is the code name for the business unit or organization within the company to be charged for servicing the problem investigation. When you select the cost center code, the **Company** and **Cost Center Name** fields display the values attached to the cost center code.
4. From the **Cost Classification** list, select either **Actual** or **Budget**.
5. In the **Related Cost** field, type the cost amount, and select the currency from the list.
6. If appropriate, you can also:
   - Select the cost type. Cost types are defined by your organization for reporting purposes.
   - Enter a description.
   - Select the unit type. The unit type indicates whether cost is measured as a flat rate, or in hours or minutes. If you select a unit type of hours or minutes, you must type the number of hours or minutes in the **Related Units** field.
   - Enter the date the charge was incurred. To set it to the current date, you can leave this field blank.
7. Click **Save**.
   The totals for budgeted and actual costs appear at the bottom of the table.
8. Repeat steps 2 through 7 for each cost associated with the investigation.

Recording the cost of CI unavailability

If CI unavailability is recorded for a related incident request or change request, the cost of the CI unavailability appears on the **Financials** tab. You can record additional costs of CI unavailability.

⚠ **Note**
Recording the cost of CI unavailability is performed from the Classic view.

To record the cost of CI unavailability

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Click the **Financials** tab.
3. In the Manually Entered CI Unavailability area, click **Create**.
4. Complete the Cost Update form.
5. Click **Save**.

Updating assignment availability

Your assignment availability status indicates whether you are available to accept work assignments. If your status is **Yes**, you are available. If your status is **No**, you are not available.

You can quickly update your status using the **My Profile** function.

⚠ **Note**
If you have management level permissions, you can also update the status of the people in the support group that you manage.

To update assignment availability

1. From the Navigation pane, choose **Functions > My Profile**.
2. From the **Assignment Availability** menu, choose the status you want.
3. Click **Save**.

Assigning or reassigning an incident request to a vendor

If you need third-party vendor support to resolve an incident, use the vendor-related fields on the Incident form to track the assignment.

This topic contains information about the following types of assignment or reassignment:

- To assign or reassign an incident to an internal vendor (Best Practice view)
- To assign or reassign an incident to an external vendor (Best Practice view)
- To assign or reassign an incident to a vendor (Classic view)

To assign or reassign an incident to an internal vendor (Best Practice view)

1. Open the incident request record.
2. From the **Vendor Group** menu, select the vendor.
3. If the vendor's ticket number is available, type it in the **Vendor Ticket Number** field.

   ⚠ **Note**
   If the Vendor Group has a group email address assigned to it, the notification goes to the group email address. If no group email address is configured for the Vendor Group, then notifications are sent to the individual email addresses of the Vendor Group members.

4. Click **Save**.

To assign or reassign an incident to an external vendor (Best Practice view)

To send an external vendor an email notification, use the Email function from the Functions area in the Navigation pane.

To assign or reassign an incident to a vendor (Classic view)

1. Open the incident request record.
2. Click the Vendor tab.
3. To assign the incident to a vendor support group, select the vendor company, organization, and group.
   If the person indicated in the **Vendor Contact** field is registered in the People form with a valid email address, Incident Management sends an email notification to that person.

Note
If the Vendor Contact field is empty, email notification goes to the Vendor Support Group group email address. If no group email address is configured for the Vendor Group, notifications are sent to the individual email addresses of the Vendor Group members.

4. If you selected the vendor from the menus, you can press **Enter** in either of the vendor name fields to select the vendor contact. If the vendor is not listed, you can type the vendor contact information.
   Enter any other information that you are tracking, such as the vendor ticket number.
5. Click **Save**.

The **Vendor Assignment Status** field is set to **Assigned**. The **Reported to Vendor Date** is set to the current date and time, if you did not specify otherwise.

Working with broadcasts

This feature lets you send messages to your entire organization, selected groups within the organization, and to external customers as well. You can use this feature to send messages about work in progress, system status, planned work, and so on. You can also use this feature to view messages that were broadcast to you from other groups in your organization.

Disclaimer
Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

Creating broadcast messages

For information about creating a broadcast message directly from the Incident or the Problem form, see Creating broadcast messages from the Incident or Problem form.

This section describes how to define a broadcast message. To define a broadcast, you must have the Broadcast Submitter functional role.

To create a broadcast message

1. On the application console, click the **View broadcast** link or the **New broadcast** link.
2. In the View broadcast dialog, click **Create**, which appears below the Broadcast table.
3. Enter information in the required fields.
   Required fields appear in bold on the **Broadcast Details** tab.
   - **Company** — Select the company where this broadcast will be sent. Only users with access to this company see the broadcast. To send the broadcast to everyone, select **Global** from the **Company** list.
     The **Company** field is mandatory. To specify a specific part of the company, fill in the other location fields. For example, you can specify the site, organization, or department.

> ⚠ **Note**
> Out of the box, you can only define broadcast messages for the **Global** company.

- **Subject** — A short description of what the broadcast is about
- **Broadcast Message** — The text of your message
- **Broadcast Type** — Select a broadcast type from the list
- **Broadcast Start Date** and **Broadcast End Date** — To start the broadcast now, click in the **Broadcast Start Date** field, and then press **Enter**. To select a date from the calendar, click the **Browse** button next to the field. Select a date from the calendar on which to start the broadcast and the date to end it. You can also specify times of the day using the **Time** feature at the bottom of the calendar.
- **Broadcast Originated From** — This is automatically filled in. The contents depend on where you are creating the broadcast. If you broadcast from an investigation, the value is set to **Problem Investigation**.
- **Broadcast Originated From ID** — When you define a broadcast from within a record, this field is automatically filled in. If you define a broadcast from the main console, the field is unavailable.
- **View Access** — To make the broadcast visible only to members of your organization, select **Internal**. To make the broadcast visible from the Requester console, select **Public**.
- **Send to Twitter?** — To post the broadcast message using the configured Twitter account, select **Yes** . For additional information on receiving broadcast messages using Twitter, see Receiving BMC Remedy ITSM broadcasts on Twitter.

  > ⚠ **Note**
  > This option is available only when you select Global in the **Company** field and set the **View Access** value to Public.

- **Notify** — Select **Yes** to broadcast notification automatically sent to an individual or group.
  If you select **Yes**, an **Email** button and the Notify Support area appears.
  - Use the **Manual Email** button to manually send an email about the broadcast. On the Email System form, enter the recipient's email address in the **Internet Email** field, and then click **Send Email Now**.
  - Use the Notify Support area to indicate which group to notify of the broadcast. You must complete all three fields--**Support Company**, **Support Organization**, and **Support Group**. The notification is sent at the time and on the date specified in the **Broadcast Start Date** field.
- **Priority** — Select a priority level for the broadcast. The choices are **Low**, **Medium**, and **High**.

4. To add an attachment to the Broadcast, right-click inside the table and select **Add** from the menu.
   In the Add Attachment dialog box, click **Open** to attach the indicated file. Only one attachment is allowed for each broadcast.
5. If you want members of another group to be able to modify the message, follow these steps:
   a. Click the **Authoring Groups** tab, and then click **Manage Authoring Groups**.
   b. On the Authoring Group dialog box, select the group to have authoring rights, and then click **Add**.
6. Click **Save**.

Creating broadcast messages from the Incident or Problem form

To create a broadcast message from one Incident Management or Problem Management form, you must have the functional role of Broadcast Submitter. To have this functional role added to your system ID, contact your system administrator.

To create a broadcast message from a Service Desk form

1. Open the New/Modify Broadcasts form, as follows:
   - *(Best Practice view)* From the Navigation pane, select **Quick Actions > Broadcast Incident** (or **Broadcast Problem**).
   - *(Classic view)* From the Navigation pane, select **Functions > Broadcast Incident** (or **Broadcast Problem**).

   > ⚠ **Note**
   > When you create a broadcast message from a record, it is related to that record. When you create a broadcast message from a console, it is not related to any specific record.

2. Enter information in the following required fields:

Field	Explanation
Company	Select the company to which this broadcast pertains. Only users with access to this company can see the broadcast. If you select **Global** from the **Company** list, the broadcast is sent to everyone. Of the various **Location** fields, only **Company** is mandatory. The other **Location** fields: **Region**, **Site Group**, **Site**, **Organization**, and **Department**, are informational fields that allow you to specify the physical location, and so on, to which the broadcast applies. These fields otherwise do not restrict who can see the broadcast. All people assigned to the specified company will see the broadcast.
Subject	A short description of what the broadcast is about.
Broadcast Message	The text of your message.
Broadcast Type	Select a broadcast type from the list.
Broadcast Start Date and **Broadcast End Date**	To start the broadcast now, click inside the **Broadcast Start Date** field, and press **Enter**. To select a date from the calendar, click the **Browse** button next to the field, then use the calendar that appears to select the date on which the broadcast is to start and the date on which you want it to end. You can also specify times of the day using the Time feature at the bottom of the calendar.
Broadcast Originated From	This field is completed by the system. The contents depend on where you are creating the broadcast. If you broadcast from an incident, this is set to Incident.
Broadcast Originated From ID	This field is filled in by the system, but only when you create a broadcast from within a record. If you create a broadcast from the main console, the field appears dimmed.
View Access	Select **Internal** if you want the broadcast enabled only for members of your organization. If you also want the broadcast enabled from the Requester console, select **Public**.

Notify	If you want a broadcast notification automatically sent to an individual or group, select **Yes**. If you select **Yes**, the **Manual Email** button and the Notify Support area appear. Use the **Manual Email** button to manually send an email about the broadcast to a person or group. When the Email System form appears, enter the recipient's email address in the Internet email field, and then click **Send Email Now**. Use the Notify Support area to indicate the group you want to notify of the broadcast. You must complete all of the fields: **Support Company**, **Support Organization**, and **Support Grou**p. The notification is sent at the time and on the date specified in the **Broadcast Start Date** field.
Priority	Select a priority level for the broadcast. The choices are **Low**, **Medium**, and **High**.

3. To add an attachment to the broadcast message, right-click inside the table and choose **Add** from the menu that appears.
   The Add Attachment dialog box appears. Use this to indicate the file you want to attach. Click **Open** to attach the indicated file. You are limited to one attachment for each broadcast.
4. To allow members of another group to modify the message, perform the following steps:
   a. Click the **Authoring Groups** tab.
   b. Click **Manage Authoring Groups**.
      The Authoring Group dialog box appears.
   c. Indicate the group that you want to have authoring rights by selecting from the menus.

      > ⚠ **Note**
      > The support group that you belong to appears in the table by default.

   d. Click **Add** when you finish.
   e. You can indicate another group, or click **Close** to dismiss the dialog box.
5. Click **Save** to save the broadcast message and close the dialog box.

   > ✓ **Tip**
   > When viewing a broadcast message, you can also create new broadcast messages. For information about how to do this, see Viewing and modifying broadcast messages.

Viewing and modifying broadcast messages

While viewing broadcasts, you can modify the message (if you belong to an authorized authoring group), define a new broadcast message, and under some circumstances (when viewing the message from the current record) relate the broadcast message to the current record.

To view broadcast messages

1. On the application console, click the **New broadcast** link that notifies you when there are new, unread broadcast messages. If there are no new or unread broadcasts, a **View Broadcast** link is displayed instead.
2. In the View broadcast dialog, select the message to view from the Broadcast table, and then click **View**.
3. To view another message, close the View Broadcasts dialog box, select the broadcast message to view, and then click **View**.

Limiting the number of messages

> **Note**
> This section applies only when using the Classic view.

When viewing broadcasts from the current Asset, Change, Problem or Incident record, you can limit the number of broadcasts that appear in the Broadcast table.

> **Note**
> You can perform this task only when using the Classic view.

To limit the number of messages

1. From the **Quick Links** area of the **Navigation** pane, click **View Broadcast**.
2. On the View Broadcast dialog box, click the **Broadcast Search Criteria** tab, and then complete the fields in the tab.
   To return the smallest number of broadcasts, complete as many of the fields as possible.
3. When you finish specifying the search criteria, click **Search**.

Controlling the timing of broadcast pop-up messages

From the BMC Asset Management, BMC Change Management, BMC Service Desk:Incident Management, and BMC Service Desk Problem Management consoles, you can control the timing of broadcast pop-up messages. Broadcast pop-ups alert you to the presence of broadcast messages.

The options are:

- **Never** — Broadcast messages do not automatically pop up on the screen. You will have to click the **Broadcasts** link to view them.
- **On Console Open** — Broadcasts messages display on the screen when you open the console.
- **On Console Refresh** — New broadcast messages display only when you refresh the console.

To set the timing of pop-up messages

1. From the application console, choose **Functions** > **Application Preferences**.
2. In the Request Preferences form, click the **Broadcast** tab.
3. In the **Broadcast Auto Popup** field, specify one of the following default settings:
   - Never
   - On Console Open
   - On New Broadcast
4. Click **Save**.

   > **Note**
   > For the changes to take effect, you must close the application and log on again.

Creating reminders

Use reminders to create notes for yourself and others. You can send the reminders by email and can specify when they are sent. You can create generic reminders, or you can create reminders that are associated with a specific request.

For example, you can send yourself a note about a specific investigation to remind yourself to follow up on it. You can create and view reminders from either the Incident Management or Problem Management console or from within a specific incident request, problem investigation, known error, or Solution Database entry. The location from which you create or view a reminder determines which reminders you see:

- **Incident Management console** — You can view all reminders that you created.
- **Incident Request** form — You can view all reminders associated with that incident. This includes the reminders that were created by other users of BMC Service Desk.
- **Problem Management** console — You can view all reminders that you created.
- **Problem Investigation** form — You can view all reminders associated with that investigation. This includes reminders created by other users of BMC Service Desk.
- **Known Error** form — You can view all reminders associated with that known error. This includes reminders created by other users of BMC Service Desk.
- **Solution Database** form — You can view all reminders associated with that Solution Database entry. This includes reminders created by other users of BMC Service Desk.

To create a reminder

1. From the Navigation pane in either the Problem Management console or the Problem Investigation form, choose **Functions > Reminders**.
2. From the Navigation pane in either the Problem Management console or the Problem Investigation form, choose **More > Reminders**.

   > ⚠ **Note**
   > If you create a reminder from the Incident Management or Problem Management console, the reminder is general in nature. If you open a record and create a reminder, the reminder is specific to the open record.

3. Click the **Create Reminder** tab.

   > ⚠ **Note**
   > If you are creating the reminder from the main console, skip the next step.

4. To remove the link between the reminder you are creating and the open record, select, and then delete the contents of the **Link to Request-ID** field. The **Request-ID** and **Form** fields are filled in automatically by the system. The **Request-ID** field links the reminder to the open record.
5. From the **Notify list**, select either **Individual** or **Group**, depending on whether you are sending the reminder to a single person, or a group of people.
6. In the **Recipient** field, type the name of the person or group to whom you want to send the reminder.
   If you need more space to type the entry, click the **Browse** button next to the field. A larger text entry box appears.
   If you type a person's name and press **Enter**, the system automatically fills in the **AR Login** field. If the system discovers multiple matches with the name you entered, another dialog box appears that enables you to specify which of the matching names you want to receive the reminder.
7. In the **Time** field, enter the date and time you want the system to send the reminder.

You can type the information directly into the field, or you can click the button next to the field and select the date and time from the calendar that appears. By default, the **Time** field contains the current date. The default time is one hour ahead of the current time.

8. In the **Subject** field, enter information about the reminder.
   If you need more space to type the entry, click the **Browse** button next to the field. A larger text entry box appears.
   The information in this field appears in the subject line if the reminder is sent by email.
9. In the **Message** field, type the reminder message text.
   If you need more space to type the entry, click the **Browse** button next to the field. A larger text entry box appears.

   > ⚠ **Note**
   > Do not type text in the **Log** field. This field records the subject line and message of the reminder when it is sent.

10. Click **Save**.
    A confirmation message appears.
11. Click **Close** to close the Reminders dialog box.
    The reminder is sent at the time you specified.

Paging and sending email messages

BMC Service Desk gives you different methods of sending messages to either individuals or organizations:

- Pages
- Email

This section describes how to send both types of messages.

- Paging a person or on-call group
- Sending email
- Record creation and updates by email

> ⚠ **Note**
> BMC Service Desk can send notification messages to individuals, based on incident assignments and other events, as pages or emails. For information about configuring notifications as pager messages or email messages, see Configuring notifications.

Paging a person or on-call group

You can page individuals or the on-call member of a group about the current record using the Paging System feature.

To page a person or an on-call group member

1. Open the incident request or problem investigation record.
2. In the Navigation pane, choose **Functions > Paging System**.
3. In the Navigation pane, choose **More> Paging System.**

4. Select one of the following options:
    - **Page By Person** to page an individual
    - **Page By On-Call Group** to page the on-call member of a specified group
5. Select the recipient:
    a. Complete the fields in the Search Criteria area, and then click **Search**.
    b. Click the recipient's name in the search results table, and then click **Select**.

    > ⚠ **Note**
    > If you are sending a page to a person (instead of an on-call group) and need help determining the correct person, you can see more information about the individual by selecting their name from the list, and then clicking View. This opens the People form, which contains detailed information about the recipient.

6. Complete the fields in the Paging Information area, as follows, and then click **Send Page Now**.
    - **Pager Service Provider** — Select the recipient's pager service provider from the list.
      If you are sending a page to a person, you can find this information by selecting the person's name from the search results list, and then clicking View (as described in step 4). When the People form appears, click the Notifications tab and look for the following field: Pager Service Provider.

      > ⚠ **Note**
      > To learn more about the service provider, click the button with the globe icon beside the field to open a link that takes you to the service provider's website. This link is configured by your administrator, as described in the Configuring pager service.

    - **Pager Type** — The application fills in this field automatically, using information already recorded about the receipt.
    - **Pager Number** — The application automatically fills in this field with the pager's telephone number, when possible. If the pager number is recorded, you must enter the pager number manually. See the Manual Pager Number description in this list.
    - **Pager Email** — If the pager has an email address, type it here. If you are sending the page to a person, this information is available on the Notifications tab, as described previously.
    - **Manual Pager Number** — If the pager's telephone number is not available automatically from the paging system, type the pager's telephone number here.
    - **Alphanumeric Pager Message** or **Numeric Pager Message** — Type your message in this field. Be aware that only one of these fields is enabled, depending on the type of pager the recipient carries.

Sending email

You can send messages about the current record using the Email System.

You can use this function to send email to any valid email address. This might include an SMS recipient or a wireless PDA user, if you can send email to the device.

To send an email message

1. Open the incident request or problem investigation record.
2. In the Navigation pane, choose **Functions > Email System**.

3. Indicate the recipient by selecting one of the following options:
    - **Current Contact** — If Incident Management assigned a current contact to the record when you open the Email System form, the contact's name with contact information appears in the table and is the default recipient.
    - **Current Assignee** — To select the current assignee, click **Select Current Assignee**. The current assignee's name with contact information appears in the table.
4. To select another recipient, perform the following steps:
    a. Complete the fields in the People Search Criteria area.
    b. Click **Search**.
    c. When the search finishes, select the recipient's name in the search results table.
    If you need help determining the correct name in the list, you can see more information about an individual by selecting their name from the list, and then clicking **View**. This opens the People form, which contains detailed information about the recipient.
5. Complete the email information fields. See the list that follows for a description of the fields.
    - **Internet Email** — This displays the recipient's email address. When you select the email recipient, as described in steps 3 and 4, the Internet email address updates from the people record.
    - **Email Subject Line** — By default, the subject line contains the incident ID number, to which you can append text or overtype.
    - **Email Message Body** — You type the message text here. By using the series of buttons to the right of the Email Message Body field, you can also automatically insert text from the record into the message text; you can insert the following values:
        - Status
        - Summary
        - Details
        - Resolution

        > ⚠ **Note**
        > If one or more of these buttons are dimmed, it means the corresponding field in the record contains no information.

    - **Email Attachment** — You can attach a file to the email message (BMC Service Desk limits you to one attachment). To do this, right-click inside the Email Attachment table, and then click **Add**. The Add Attachment dialog box appears. Browse to and select the file that you want to attach. Click **Open**. Details of the attached file appear in the table.
6. Click **Send Email Now**.

Record creation and updates by email

This topic provides conceptual information about how to use email to create incident requests and to add work information to incident requests, problem investigations, known errors, tasks and work orders.

For step-by-step procedures that describe how to create incident requests or add work information using email, see the following topics:

- Creating an email generated incident request
- Adding work information by using email

The Configuring the Email Rule Engine topic provides step-by-step procedures for enabling your system to create and update records by email.

Troubleshooting email record creation and updates tells you where to look for information that will help you to troubleshoot this feature.

⚠ **Note**
To create or update records using email, you must have your own email address recorded in the Email Address field of your People form record. Ask your system administrator to ensure that your People form record includes your email address.Configuring the Email Rule Engine

Depending on how your system is configured, you can create or update the following record types by using your email service:

- Incident request (create and add work information)
- Problem investigation (add work information only)
- Known Error (add work information only)
- Work Order (add work information only)
- Task (add work information only)

After the email message arrives in the in box, the Email Rule Engine checks incoming email messages based on a set of rules that are provided out-of-the-box as well as by rules the your system administrator configures. There are two sets of checks through which the email message must pass. The first check determines whether any text appears in the subject line that is part of an Excluded Subject list. For example, if the subject line contains *Delivery Error*, the email message is rejected, because that phrase is on the Excluded Subjects list.

If the email message passes the excluded subject test, the Email Rule Engine then evaluates the content of the email message according to the Email Rule Engine use cases that are configured by your system administrator. When the Email Rule Engine matches the email message with a use case, it processes the message according to the use case rules. After a match is made with a use case, the Email Rule Engine does not check any remaining use cases for and additional match. The Email Rule Engine only runs one use case against any given email message. If an email message does not match any of the configured or the default use cases, the Email Rule Engine rejects it.

Example of creating a request and updating it by using email

In an environment that is configured to create and update records using email, an Email Rule Engine use case is defined as follows:

- The key words are *locked* and *ID*.
- If the key words are in the subject line, the Email Rule Engine creates an incident request from the Locked User ID template (this is an example template name; your system might have different templates).

A customer submits an email message with the following text in the subject line: "incident request, locked ID for user singhr". When the email message arrives at the inbox, the following events take place:

1. The Email Rule Engine runs the following tasks:
   a. Scans the Subject field for excluded subject and finds none
   b. Evaluates the email message according to the configured use cases
   c. Discovers that the content of the Subject field matches the criteria in one of the use cases
   d. Creates an incident request, using the Locked User ID template
   e. Copies the details of the email message into the incident request's Work Information form.

2. The Incident Management assignment rules assign the new incident request to a help desk analyst.
3. The help desk analyst opens the new incident request, reviews the details, and has a question about some of the information in the request.
4. The help desk analyst sends the question to the incident request submitter directly from the incident request, using the Email function.
5. The submitter receives the email message and responds to it with an answer to the question.
6. The Email Rule Engine adds the response to the incident request as a work information entry.
7. The help desk analyst opens the incident request and reviews the work information.
8. With the information provided by the submitter, the help desk analyst can close the incident request.

Creating an email generated incident request

This topic describes how to use email to create an incident request.

⚠ **Note**
For BMC Remedy IT Service Management 8.1, you can create only incident requests by using email.

Before you begin

Check with your system administrator to ensure that your BMC Service Desk system is configured to work with email-generated service requests.

⚠ **Note**
Because the email feature is highly configurable, the procedure in this topic provides only general instructions. Check with your system administrator for the specific information that applies to your email environment.

To create an incident request by using email

1. Open your email editor and create a new email message.
2. In the **To** field, enter the email account that is registered with the BMC Remedy Email Engine to receive and generate incident requests.
3. Complete the **Subject** field and the body text according to the rules configured by your system administrator.
4. If you have an attachment, add it to the email message.
   The system adds attachments to the service request's Work Information form. If you add multiple attachments, the system creates a zip file and adds it to the Work Information form.
5. Click **Send**.
   If your email system is configured to send acknowledgments, you will receive a confirmation message containing the incident request ID number.

Related topics

Adding work information by using email
Configuring the Email Rule Engine
Troubleshooting email record creation and updates

Adding work information by using email

You can add work information to an existing records. Depending on how your system is configured, you can add work information to any of the following BMC Remedy ITSM record types:

- Incident request
- Problem investigation
- Known Error
- Work Order
- Service Requests (updates the Activity Log on the Service Request form)
- Task

This topic describes how to add work information notes to all record types by using email. It also contains the following information:

- Attachments
- Before you begin
- To add work information notes to a service request by using email
- Related topic

You can add work information by responding to a system-generated email message about the record, or you can create a new email message.

> ⚠ **Note**
> You can only *add* work information notes to a record. You *cannot update* existing work information notes.

When you send the email message, ensure that the subject line starts with *RE:*. Otherwise, the Email Rule Engine rejects the message. Also ensure that the subject line contains the request ID.

> ⚠ **Note**
> In some environments, the Email Rule Engine can parse the body of the email message for the request ID. If your system is configured to do this (check with your system administrator), then you do not need to put the request ID in the subject line. In all cases, however, the subject line must start with *RE:*.

Attachments

You can add an attachment to the email message, which is also added to the work information note. If you add more than one attachment, the email engine zips the attachments into a zip file and attaches it to the work information note.

Before you begin

Check with your system administrator to ensure that your BMC Service Desk system is configured to work with email-generated records.

To add work information notes to a service request by using email

1. Perform one of the following actions:
   - Reply to an existing email message about the record to which you want to add the work information note.
   - Create a new email message.
2. If you are creating a new email message, ensure the **To** field contains the correct email address for your email server.
3. Ensure that the **Subject** field starts with *RE:* and includes the request ID.
   Alternatively, if your system can read the request ID from the body of the email message, ensure the request ID appears in the body of the message.

   > ✓ **Tip**
   > If you are unsure whether your system can read request IDs from the body of an email message, put the request ID in the **Subject** field.

4. Type the work information text in the body of the email message.
5. If you have any attachments, add those to the email message.
6. Send the email message.

Related topic

Creating work information entries from the console

Using tasks

The information in this topic is for people who fulfill one or more of the following support roles:

- Service desk analysts
- Group coordinators
- Specialists

When working in BMC Service Desk, you access the Task Management system from the Incident Management feature.

A task is a unit of work that needs to be completed as a step in resolving an incident request. If the solution to an incident request involves more than one action, procedure, or process, consider dividing the solution into separate tasks. Dividing the solution into separate tasks can help you to better manage and to monitor the incident request as it moves toward resolution.

You can assign the tasks to the same person, to several people, or to a support group. The person or support group to whom the task is assigned is the task implementer. When the group coordinator sets the task status to **In Progress**, the task implementers are notified of the tasks assigned to them by email, pager, or some additional means. After a task is assigned to the task implementers, they can log their progress as they complete each task.

> ⚠ **Note**
> Tasks can have an **Assigned** status only if the associated incident request also has the status of **Assigned**.

You can use a task template to add a task to an incident request, or you can create an ad hoc task. Task templates are predefined tasks that you can quickly add to an incident request. For information about how to do this, see Adding tasks using task templates. An ad hoc task is any task that is not included in the list of task templates and, therefore, you must create it manually. For information about how to do this, see Creating ad hoc tasks.

When using task templates, you can also add tasks that are divided into sub-tasks. A task that has sub-tasks is called a task group. The sub-tasks of the task group are called "children" of the task group.

Although tasks and task groups are related to specific incident request records, information about the tasks and task groups is stored on a separate Task form. You can relate an unlimited number of tasks or task groups to an incident request.

After a task or task group is assigned to a task implementer, the task implementer receives notifications to perform each of the assigned tasks.

For information about using tasks, refer to the following topics:

- Adding tasks using task templates
- Opening the Task form
- Creating ad hoc tasks
- Accepting task assignments
- Opening and viewing individual task records
- Reassigning task sequence numbers
- Assigning and reassigning tasks
- Updating task record details
- Adding work information to a task
- Planning task times
- Tracking the time spent working on tasks
- Canceling tasks
- Closing tasks
- Resolving, closing, and canceling incident requests with open tasks

Adding tasks using task templates

To save time, you can use a task template to add a task to an incident request record. Task templates are created by your system administrator. A task template is a predefined task; usually for the most commonly performed tasks that your service desk handles. Because the Task form is predefined (that is, the fields are already completed), you do not need to spend time manually completing the form.

The following are the types of tasks that you can add to an incident request record when using templates: Task Template and Task Group Template. Task templates associate a single task to the incident request record. Task Template tasks can be either Manual or Automatic. Manual tasks must be performed by a person. Automatic tasks are preformed by a computer or automated system, but you must still assign automatic tasks to a person, so there is someone to monitor the task.
The Task Group template generates a task that has two or more sub-tasks. Task Group tasks can be defined either as *standard* or *sequencing*. Standard task group tasks can be performed in any order. In a sequencing task group, however, the tasks must be performed in the sequence indicated on the Task form.

To add a task using task templates

1. Open the Task form, as described in Opening the Task form.
2. From the Request Type list, select either Task Template or Task Group Template, and then click **Relate**.

> ✓ **Tip**
> To manage a large number of task templates, you can filter the list by selecting from the **Type** and **Category** lists at the top of the dialog box.

3. From the list of tasks in the Select Template dialog box, select the template for the task you are adding, and then click **Relate**.
   When you click **Relate**, the Task form closes.
4. Repeat steps 2 and 3 for all tasks you want to add to the incident.
   The templates you selected are displayed in the Tasks and Task Groups list. If there are no templates listed, click inside the list to refresh the table.
5. If necessary, redefine the numeric sequence of the children tasks created by any group template, as described in Reassigning task sequence numbers.
   The task management subsystem enforces the dependencies between tasks. These relate to the sequence order specified in the Incident Request form.
6. Click **Close**.
7. When you finish adding templates, save the incident.

Opening the Task form

How you open the Task form depends on whether you are using the Best Practice view or the Classic view:

When using the Best Practice view	When using the Classic view
1. Open the incident request record. 2. From the Navigation pane, select **Links > Tasks**.	1. Open the incident request record. 2. Click the **Tasks** tab.

Creating ad hoc tasks

Add hoc tasks are tasks that are not predefined by a task template and, therefore, must be created manually.

To create an ad hoc task

1. Open the Task form, as described in Opening the Task form.
2. From the Request Type list, choose **Ad hoc**.
3. Click **Relate**.
   The Create Task form appears. Certain fields in the form are already filled in with the data for the incident.
4. In the upper region of the form, fill in the following required fields:
   - **Name** — Enter a descriptive name of the task.
   - **Summary** — Enter a brief description of the task.
     The Type field is set to Manual by default when you create an ad hoc task.
5. On the General tab, fill in information about the company.

The Company field defaults to the contents of the Incident Location field in the Incident Request form. Your task can be assigned to an different department or a different company.

6. On the Requester tab, fill in information about the person creating the task (Requester) and the intended target of the task (Requested For).
   Some information is set by default from the Requested By information of the incident.
7. On the Categorization tab, fill in information about the product and operational categorizations.
8. In the Assignment/Dates tab, assign the task by completing the following fields:
   - **Assignee Group** — Optionally, select a task implementer group from the list.
   - **Assignee** — Optionally, select a task implementer from the list.
     The BMC Remedy Assignment Engine automatically assigns the task when the task is created according to how the administrator has configured Incident Management, but you can override this if necessary. For more information about assignment configuration, see Configuring assignments.
   - **Scheduled Start Date** — Optionally, enter an estimated start date.
   - **Scheduled End Date** — Optionally, enter an estimated end date.
     You can set the Start Date and End Date to be different from the dates of the parent incident.
9. On the Relationships tab, search for and then relate configuration items that are needed with this task.
   You can perform quick actions that are with the task, for example, get related relationships.
10. When you finish creating the task, click **Save**.
    The task information form closes and returns you to the Incident Request form. The task management subsystem enforces the dependencies between tasks. These relate to any Sequence order you might have specified in the Incident Request form.
11. Click **Save** on the Incident Request form.

Accepting task assignments

Depending on how your system is configured, you might receive notification of assigned tasks by email or by an alert. You can also use the Overview console to view all tasks assigned to you. Tasks are identified by the TAS prefix. To access the Incident Management console, the task implementer must have Incident Master, Incident User, Incident Submitter, or (at minimum) Incident Viewer permissions.

> ⚠ **Note**
> When you follow the recommended lifecycle of an incident, the status of a task must be Scheduled before you accept the task.

After you receive notification of a task assignment, you must accept it. Use the following procedure to accept a task assignment.

To accept an assigned task

1. Open the Task form, as described in Opening the Task form.
2. Select the task that you want to accept.
3. Click **View**.

   > ⚠ **Note**
   > To view the related incident request record, click Open next to the Request ID field on the Task form.

4. If the Status Field of the incident is set to In Progress, manually set the Status field to Work in Progress. This is an important step, because the task then moves into Work in Progress status. In addition, different escalations occur based on the task's status. If the task is still in the Scheduled state while you are working on it, an inaccurate escalation can occur.
5. Click **Save**.

Opening and viewing individual task records

You can open and view the contents of individual task records. This enables you to see detailed information about the individual records and to update them.

To view task records

1. Open the Task form, as described in Opening the Task form.
2. Click inside the Tasks and Task Groups table.
   A list of the tasks and task group appears in the table.
3. In the Tasks and Task Group table, select the task record you want to view, and then click **View**.

Reassigning task sequence numbers

When you relate tasks or task groups to an incident, they are automatically sequenced in the order in which you related them to the incident. This sequence is strictly enforced inside the incident.

You can, however, reassign the sequence in which tasks and task groups are performed. You can also assign the same sequence number to more than one task or children tasks of a task group. If two tasks or children tasks of a task group have the same sequence number, they are considered peers. You can work on peer tasks in any order.

The following procedures are described here:

- To reassign a sequence to task groups and tasks
- To reassign sequence numbers to task group children

To reassign a sequence to task groups and tasks

1. Open the Task form, as described in Opening the Task form.
2. In the Tasks and Task Groups table, select the task that you want to resequence.
3. Click either the up arrow or the down arrow located to the right of the table. This moves the selected task either higher or lower in the sequence.
4. Click **Close**.

To reassign sequence numbers to task group children

1. Open the Task form, as described in Opening the Task form.
2. In the Tasks and Tasks Groups table, select the task group.
   The tasks assigned to the task group appear in the Children of Selected Task Group table.

> ⚠ **Note**
> You might need to click inside the Children of Selected Task Group table to refresh its contents.

3. In the Children of Selected Task Group table, select the task you want to reassign.
4. Click either the up arrow or the down arrow located to the right of the table. This moves the selected task either higher or lower in the sequence.

Assigning and reassigning tasks

After creating a task or adding a task template to an incident request record, you assign it. You can assign tasks to individuals or to a support group.

If you cannot resolve one of your assigned tasks, you can reassign the task, or you can ask your group coordinator to reassign the task. For example, you might ask the group coordinator to reassign the task in situations where you want to reassign the task to someone outside your group.

To assign a task (Best Practice view)

1. Open the Task form as described in Opening the Task form.
2. Select the **Assignment** tab.
3. From the **Assignee** or **Assignee Group** lists, select the person or support group to work on the task as the task implementer.
4. Save and close the form.

The task implementer for that task is notified of the task assignment.

To reassign a task (Classic view)

1. Open the task form as described in Opening the Task form.
2. Click the **Assignment** tab.
3. In the **Assignee** or **Assignee Group** fields, choose the group or person to you want to reassign the task to.
4. Ensure that the **Notify Assignee** field is set to **Yes**.
5. Click **Save**.

The new task implementer is notified of the request assignment. Until the new implementer accepts the task assignment, you are still assigned to the task and have responsibility for it.

Updating task record details

After a task record is created, you can change the details that appear on the record.

To update details on the task form

1. Open the form as described in Opening the Task form.
2. Update the details as needed.
3. Save the changes and close the form.

Adding work information to a task

Work information is a note about any work you performed while completing or trying to complete the task. You can add work information to each task included in the incident. The work information for each task appears in the Work Info of Selected Task table on the Task form.

To add work information to a task

1. Open the task form as described in Opening the Task form.
2. Click the **Work Info** tab.
3. If needed, modify the work information type.
4. From the Source list, select the source of this information.
   Information sources can include, for example, email messages, system assignment, or the web.
5. Enter the details of your work information record in the **Summary** and **Notes** fields.
6. To add attachments to the record, right-click in the attachment table and select **Add** from the menu that appears.
7. From the Locked list, select **Yes** or **No** to lock the log.
8. Select the view access:
   - **Internal** — Only users within your organization can see the entry.
   - **External** — Everyone with access to the system can see the entry.
9. When you finish updating, save your changes.
   The **Save** operation adds your entry to the task's work history. You filter out specific work entries in the **Show** field, based on the type of activity that appears in the table.
10. To see a report of the activities you performed against this task, click **Report**.
11. To display all current entries for work information history, click **View**.
12. Close the Task form when you finish with it.
13. When you return to the Incident Request form, refresh the work information entry of the Assigned Task table to display all the entries.

Planning task times

You can plan the time for individual tasks. The **Dates** tab in the Task form includes fields where you can enter scheduling information. You can create the time segments that are required to complete individual tasks.

To plan the time for tasks

1. Open the task form as described in Opening the Task form.
2. Click the **Dates** tab.
3. In the **Dates/Time** region of the form, provide dates for the **Scheduled Start Date** and **Scheduled End Date** fields.
4. In the **Time Segment Action** field, select the following options:
   - Analyze Time Segments
   - Create Business Event Time Segment
   - Modify Business Event Time Segment
   - Create Categorizational Time Segment

- Modify Categorizational Time Segment
- Create/Modify CI Time Segment

5. Save and close the form.

Tracking the time spent working on tasks

You can track the time spent working on a task at any time after it is created. Use this feature between the time the task status is in Implementation In Progress and Closed. You can track the time spent working on a task in different ways.

- Using the Start and Stop buttons
- Manually entering the time
- Enter work into the effort log

Using the Start and Stop buttons

When you use this method, the time is automatically calculated based on when you click the start and stop clock buttons.

To use the start and the stop buttons to track the time spent working on a task

1. Open the task form as described in Opening the Task form.
2. Click the Assignment tab.
3. Click the **Start Clock** button.
   The current date and current time are displayed in the read-only Start Time field.
4. Click **Save**.
5. When you finish working on the task and want to stop tracking the time, click **Stop Clock**. You must repeat steps 1 and 2 first if you closed the task after saving it in step 4.
   A message reports the number of minutes spent working on the task. The time spent is also added to the value in the read-only Total Time Spent field.
6. Save and close the form.
   You can use the start and stop clock buttons as many times as is required. Each successive time, the new time is added to the value already in the Total Time Spent field.

Manually entering the time

When you use this menthod to record your time, you can enter a time into the Time Spent field directly.

To manually track the time spent working on a task

1. Open the task form as described in Opening the Task form.
2. Click the **Assignment** tab.
3. Enter a number of hours or minutes manually in the editable Time Spent fields.
4. Click **Save**.
   The time you entered is automatically added to the value already in the Total Time Hours and Minutes fields.

Enter work into the effort log

To use this method of time tracking, you create an effort log entry as described in the following procedure.

To use the Task Effort log to track the time spent working on a task

1. Open the task form as described in Opening the Task form.
2. Click the **Assignment** tab.
3. Click **Effort Log**.
   The Task Effort Log window appears.
4. Enter information into the effort log.
   For example, you can enter time spent in hours and minutes and additional details.
5. Click **Add to Effort Log**.
   An entry is added to the effort log. You can view the entry or delete it as needed.
6. Close the task effort log to return to the task.
7. Click **Save**.

Canceling tasks

You can cancel tasks by accessing them through the Incident Request form. This action does not delete the task; it sets the status of the task to **Closed** and the closure code to **Canceled**.

> ⚠ **Note**
> If you cancel an incident with open tasks, all the tasks associated with the canceled incident are also canceled. For information about canceling an incident with open tasks, see Resolving, closing, and canceling incident requests with open tasks.

To cancel tasks

1. Open the incident request record.
2. Click the **Tasks** tab.
3. In the Tasks and Task Groups table, select the task you want to cancel.
4. Click **Cancel**.
5. The status of the task is automatically set to **Closed**.
6. Save the incident request record.

Closing tasks

When you have completed a task, you are ready to close it.

> ⚠ **Note**
> Depending on how your system is configured, you might not be able to resolve the incident until you close the task.

To close a task

1. Open the task form as described in Opening the Task form.
2. Click the **Assignment** tab.
3. Update the time you spent on the task.
   You can create an entry in the effort log as needed.
4. Click the **Work Info** tab.
5. Make an entry in the Work Info History field.
6. At the top of the Task form, set the **Status** field to **Closed**.
   When a task is set to a status of **Closed** and certain conditions apply, you have the option of updating related CIs that might be affected by this modification.
7. Select a status reason to describe how the task was closed. The closure codes are:
   - Success
   - Failed
   - Canceled
8. Click **Save**.

Resolving, closing, and canceling incident requests with open tasks

You resolve and close incident requests with open tasks the same way that you close other types of incident requests. However, depending how your environment is configured, if you resolve or close an incident request with open tasks, you might receive either an error message or a warning message. Depending on your configuration, it is also possible to receive no message.

The following paragraphs describe what to do if you receive an error message, what happens when you receive a warning message, and when you receive no message:

- **Error message** — If you receive an *error* message when closing an incident that has open tasks, you must close all the open tasks before you can close the incident.

  When the Incident Resolution with Open Tasks rule is configured to generate an error message, the error condition stops all workflow processing and prevents the incident from being closed. This is the default configuration.
- **Warning message** — If you receive a *warning* message when closing an incident that has an open task, you can still close the incident successfully. The task remains open, however.
- **No message** — It is possible to close an incident that has an open task and receive no message, depending on how your installation is configured. If you receive no message when closing an incident with an open task, the task remains open.

If you cancel an incident that has an open task associated with it, the open task is also canceled.

Using BMC Service desk to manage incidents and problems

These topics describe how to use the Incident Management and Problem Management features to manage indicent requests and problem investigations through their lifecycles, as described by the BMC Service Management Process Model.

- Managing incident requests

- Managing problem investigations

Managing incident requests

The information in this section is for support personnel. It describes how to use the Incident Management feature to manage an incident request through its lifecycle; starting with registration, through assignment, resolution, and on to closure.

There are also topics for group coordinators and on-duty managers that include assigning incident requests as a group coordinator, tracking incident requests, and handling escalations.

Other topics related to the general management of incident requests are also covered in this section, as outlined in the following list:

- Registering and assigning incident requests
- Updating an incident request
- Resolving and closing incident requests
- Reopening a closed or resolved incident request
- Working with incident requests as a manager
- Viewing incident request records
- Reviewing the status of an incident request
- Managing service targets

Registering and assigning incident requests

The information in this section is for people who fulfill the support role of service desk analyst. *Group coordinators* and *on-duty managers* should also be familiar with this information to better understand the support staff tasks and so they can fulfill the role of support staff if necessary. Using the Incident Management console, support staff can create, track, and resolve incident requests.

- Registering incident requests
- Assigning incident requests

Registering incident requests

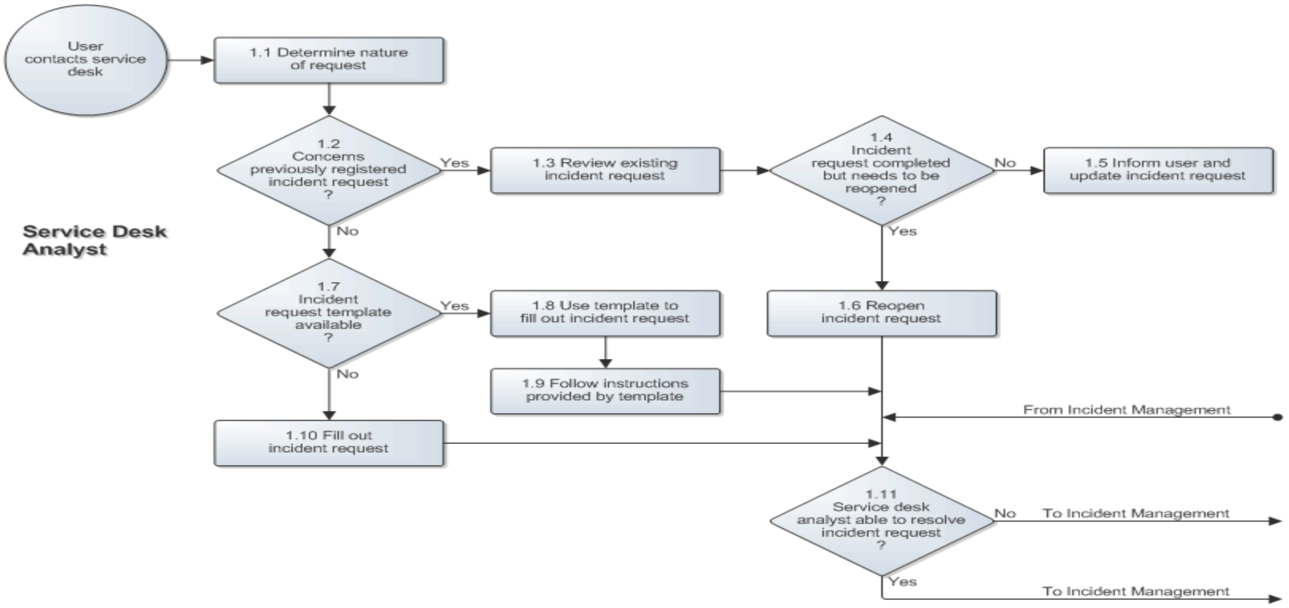
When a user contacts the service desk with an incident request, you first determine the nature of the request. If the request is about a previously registered request, you query the request and update the user with the current status.

If the request concerns an incident that was resolved, but for which the resolution was not effective, reopen the incident request record and assign the incident to a specialist.

If this is a new incident request, you create an new incident request record by capturing key information about the user and the incident. If possible, you resolve the incident immediately and then complete the incident request, otherwise you make sure the incident request is assigned to the appropriate group.

The following figure provides an overview of the registering incident requests process, as described by the BMC Service Management Process Model.

Registering incident requests


User contacts service desk
1.1 Determine nature of request
1.2 Concerns previously registered incident request ?
Yes
1.3 Review existing incident request
1.4 Incident request completed but needs to be reopened ?
No
1.5 Inform user and update incident request
Service Desk Analyst
No
Yes
1.7 Incident request template available ?
Yes
1.8 Use template to fill out incident request
1.6 Reopen incident request
No
1.9 Follow instructions provided by template
From Incident Management
1.10 Fill out incident request
1.11 Service desk analyst able to resolve incident request ?
No
To Incident Management
Yes
To Incident Management

The following topics are described in this section:

- Creating an Incident request record using a template
- Creating an incident request record without a template
- Adding or modifying a customer profile
- First call resolution
- Searching for matching records
- Searching for similar incident requests
- Accessing BMC Knowledge Management
- Creating a solution database entry from an incident
- Relating incident requests as duplicates

The following video presentation describes how to quickly create a fully qualified incident request.

Disclaimer
Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

Creating an Incident request record using a template

The purpose of this stage is to accurately record and recognize disruptions to services provided by IT to its customers. When creating a new incident request record, you classify the incident and record user information, CI information, and a description of the incident.

The key to this activity is the accuracy and completeness of the information recorded. To help ensure accuracy and completeness, BMC recommends that you use a template to help create the record. A template ensures consistency in the way information about the incident request is captured. A template can also set a relationship to a CI. Your administrator can define templates for commonly occurring incidents, as described in Creating templates.

To use a template

1. On the Incident Management console, click **Create** or **Create for Company** (in a Hub and Spoke environment).
2. If you are working in a Hub and Spoke environment, you are asked to identify the company you are creating the record for. Select the company from the drop down list, then click **Create**. The Incident form opens on the spoke server of the company you chose. Continue with the rest of this procedure.

   > ⚠ **Note**
   > The record that you create for the selected company is created and submitted on the spoke server where the company is defined.

3. Enter the Customer or Contact information as described in the following table:

When using the Best Practice view	When using the Classic view
In the **Customer** or **Contact** field on the new Incident Request form, type the customer's or the contact's information as described in Using the Customer and Contact fields in Best Practice view.	On the Incident Request form, type the customer's last name in the **Last Name** field and press **Enter**. If there are multiple customers with the same last name, you are prompted to select the appropriate customer. The **Company**, **First Name**, and **Phone Number** fields are completed from the customer record. The company drives the selection on other menus, such as **Operational**, **Product**, and **Resolution**.

4. Check the rest of the customer information for accuracy.
5. Type the incident request details in the **Notes** field.
6. Open the Incident Template Selection form as described in the following table:

When using the Best Practice view	When using the Classic view
If you know the template name Type a portion of the template name in the **Template** field and then press **Enter**. **If you don't know the template name** Click inside the **Template** field and then press **Enter**.	From the Quick Links section of the Navigation pane, click **Select Template**.

   A list of templates available to your default support group appears in the Viewing Templates for Support Group area of the Incident Template Selection form.

   > ⚠ **Note**
   > If you belong to multiple support groups, you can select a template from another of your support groups by selecting a different group from the Viewing Templates for Support Group menu at the top of the form.

7. From the hierarchical list, select the appropriate template and then click **Select**.

8. Type a brief description in the **Summary** field.
9. Select the business service CI from the Service list.
   You must select the business service CI from the menu. The business services that appear in this menu have a relationship type of Used By" either for the customer directly or the organization the customer belongs to.
10. If the incident request was caused by a CI, you can record the CI in the **CI** field. This creates a relationship between the incident request record and the CI record.
    The CIs that appear in the menu are all the other CIs related to the customer that are not business service CIs. If there are no CIs related to the customer, click the button beside the **CI** field to open a CI search form, from which you can search for all CIs.

    > ⚠ **Note**
    > When you associate a CI to an incident request, the Service Desk application automatically maps the incident request's resolution categorization to the CI's product categorization.

11. Complete the rest of the incident request form as appropriate.

    > ⚠ **Note**
    > Use the **Contact** field to record the name of someone who reports an incident on behalf of someone else. Use this field, for example, if an administrative assistant is reporting an incident on behalf of an executive.
    >
    > When using the **Contact** field to record the name of the person reporting the incident, use the **Customer** field to record the name of the person experiencing the incident. This is especially important if the person experiencing the incident is registered as a VIP or as a sensitive customer. It also ensures that the Incident Management application displays the set of business CIs in the **Service** field selection list that are directly related to the person experiencing the incident, and so on.

    > ✓ **Tip**
    > If your organization uses categorizations (Operational Categorization and Product Categorization) to help assign incident requests, but none are supplied by the template, click the Categorization tab (in Best Practice view) or the Classification tab (in Classic view) to open a dialog box where you can record this information. For a detailed discussion of Operational Categorization, see the BMC Communities article on this topic at https:\\communities.bmc.com
    > .

12. Click **Save**.

Creating an incident request record without a template

If your system does not have templates defined, use one of the following procedures to create an incident request:

- To create an incident request record without a template (Classic view)
- To create an incident request record without a template (Best Practice view)

To create an incident request record without a template (Classic view)

1. In the Navigation pane, select **Functions > New Incident**.
2. If you are working on a hub server in a Hub and Spoke environment, you are asked to identify the company

you are creating the record for. Select the company from the drop down list, then click **Create**. The Incident form opens on the spoke server of the company you chose (where it will be saved, also). Continue with the rest of this procedure.

3. In the Process Flow Status area, click the arrow in the Identification and Recording box.
4. Select **Next Stage > Investigation and Diagnosis**.
   You can move directly to the Resolution and Recovery stage or the Incident Closure stage by selecting the appropriate stage.
   The Incident Request form appears. The tabs on this form prompt you to enter required and optional information.

   > ⚠ **Note**
   > This is a dynamic form. The fields on the Required and Optional tabs depend on the information to move from the current stage or state to the selected stage or state.

5. On the Incident Request form, type the customer's last name in the Last Name field and press **Enter**.
   If there are multiple customers with the same last name, you are prompted to select the appropriate customer. The **Company**, **First Name**, and **Phone Number** fields are completed from the customer record. The company drives the selection on other menus, such as **Operational**, **Product**, and **Resolution** .
6. Type a brief description in the **Summary** field.
7. You can type additional details in the **Notes** field.
8. Select the business service CI from the Service list.
   You must select the business service CI from menu. The business services that appear in this menu have a relationship type of **Used By** either for the customer directly or to the customer's organization.
9. If the incident request was caused by a CI, you can record the CI in the **CI** field. This creates a relationship between the incident request record and the CI record.
   The CIs that appear in the menu are all the other CIs related to the customer that are not business service CIs. If the CI you are looking for does not appear in this list, click the button beside the **CI** field to open a CI search form, from which you can search for all CIs.

   > ⚠ **Note**
   > When you associate a CI to an incident request, the Service Desk application automatically maps the incident request's resolution categorization to the CI's product categorization.

10. Select values from the **Impact** and **Urgency** lists.
11. If appropriate, select a different service company.
    When you select the customer, the service company is set to the customer's company.
12. Select the appropriate service type:
    - **User Service Restoration** — Use this service type for typical service restoration requests (for example, a request to restore printing services).
      User Service Request — Use this service type if the incident request is a simple question or a request for information (for example, a request for how to information).
    - **Infrastructure Restoration** — Use this service type if the incident request is more focused on the restoration of infrastructure service. Typically, these types of incident requests are reported by system management tools (for example, if an incident is detected on a piece of network infrastructure by system monitoring software).
    - **Infrastructure Event** — Use this service type when a system management tool registers an event that does not require infrastructure restoration.
13. Click **Save**.
    If you did not assign the incident, the incident is automatically assigned based on predefined assignment

routing. If there is no appropriate predefined assignment routing, you are prompted to assign the incident.

14. If prompted, assign the incident; then click **Save**.

To create an incident request record without a template (Best Practice view)

Use the following procedure if you are using Best Practice view to create an incident request without a template.

1. In the Navigation pane, select **Functions > New Incident**.
2. If you are working from a hub server in a Hub and Spoke environment, you are asked to identify the company you are creating the record for. Select the company from the drop down list, then click **Create**. The Incident form opens on the spoke server of the company you chose (where it will be saved, also). Continue with the rest of this procedure.
3. In the Customer or Contact field on the new Incident Request form type the customer's or the contact's information as described in Using the Customer and Contact fields in Best Practice view.
4. You can type details about the incident in the **Notes** field.
5. Type a brief description in the **Summary** field.
6. Select the business service CI from the **Service** list.
   You must select the business service CI from menu. The business services that appear in this menu have a relationship type of Used By either for the customer directly or to the customer's organization.
7. If the incident request was caused by a CI, you can record the CI in the **CI** field. This creates a relationship between the incident request record and the CI record.
   The CIs that appear in the menu are all the other CIs related to the customer that are not business service CIs. If the CI you are looking for does not appear in this list, click the button beside the **CI** field to open a CI search form, from which you can search for all CIs.
8. Select values from the Impact and **Urgency** lists.
9. Select the appropriate incident type:
   - **User Service Restoration** — Use this service type for typical service restoration requests (for example, a request to restore printing services).
   - **User Service Request** — Use this service type if the incident request is a simple question or a request for information (for example, a request for how to information).
   - **Infrastructure Restoration** — Use this service type if the incident request is more focused on the restoration of infrastructure service. Typically, these types of incident requests are reported by system management tools (for example, if an incident is detected on a piece of network infrastructure by system monitoring software).
   - **Infrastructure Event** — Use this service type when a system management tool registers an event that does not require infrastructure restoration.
10. Select the reported source.
11. Select the assigned group and the assignee.
    If you do not assign the incident, the incident is automatically assigned based on predefined assignment routing. If there is no appropriate predefined assignment routing, you are prompted to assign the incident when you click **Save**.

    > ⚠ **Note**
    > The names that appear in the list of assignees depends on the assigned group you select.

12. If you use an external vendor, select the vendor's name from the list and, if used, the vendor's ticket number.
13. Click **Save**.

Adding or modifying a customer profile

Before you can record an incident, the customer must be listed in the People database. Customers are usually added to the People database by your administrator, as described in Configuring people information. However, if you have Contact People User or Contact People Admin permissions, and a customer is not listed in the database, you can add a customer's profile from the Incident Request form. (If you are unsure about your permissions, ask you system administrator.) You can also modify the customer and the contact phone number and site directly on the Incident Request form. A modification directly on the Incident Request form, however, applies only to the current incident, it does not update the People record permanently.

> ⚠ **Note**
> Although you can create a People record in the Proposed state with Incident User permissions, you need Contact People User or Contact People Admin permissions to move the record beyond the Proposed state; for example, to Enabled.

This topic describes the following procedures:

- To add a new customer profile
- To modify the customer profile on the current record
- To update the customer profile permanently

To add a new customer profile

1. From the Incident Management console, click **Create** to create a new incident request record.
2. If using the Best Practive view, perform the following actions.
   a. Click the magnifying glass icon to the right of the Customer or Contact field to open the People form.
   b. Click the magnifying glass icon to the right of the Customer or Contact field to open the People form.
3. If using the the Classic view, click **Create** on the Customer tab.
4. On the People form, complete or modify the required fields.
   If adding a customer record, you do not need to add all the information for this individual's profile, only what is necessary to submit the record.

   > ⚠ **Note**
   > You cannot define, or add, a **Support Staff Person** record here. For information about adding a Support Staff Person, see Adding a support staff person.

5. Click **Save**.
   If adding a new customer, the status of the person you added has a default value of **Proposed**. Your People/Contact administrator must verify those in proposed status, update them to **Enabled**, and add any other information that is necessary.

To modify the customer profile on the current record

Use this procedure to update the customer profile record on the current record.

⚠ **Notes**
This changes the customer profile on the current record only. It does not update the People record. To update the People record, see Updating the people record.

The following procedure is performed from an open Incident Request record.

1. Click the pencil icon beside the field you are modifying.
2. In the resulting dialog box, make the required changes.
3. Click **OK** to save the changes and to close the dialog box.
4. Click the double arrow link above the Customer Phone field to return to your starting point.
5. To modify the **Company** or **Customer** fields, click the eraser icon to the right of the **Customer** field to clear it and then complete the fields with the new information.
6. To modify the **Contact** field, click the eraser icon to the right of the field to clear it and then add the new information.
7. To update the **Customer** or **Contact** phone and site information, click the double arrow link above the **Incident ID** field. This toggles to an area that opens these fields.
8. Click the pencil icon beside the field you are modifying.
9. In the resulting dialog box, make the required changes.
10. Click **OK** to save the changes and to close the dialog box.
11. Click the double arrow link above the **Customer Phone** field to return to your starting point.
12. On the People form, complete or modify the required fields.
    If adding a customer record, you do not need to add all the information for this individual's profile, only what is necessary to submit the record.

    ⚠ **Note**
    You cannot define, or add, a **Support Staff Person** record here. For information about adding a Support Staff Person, see Adding a support staff person.

13. Click **Save**.
    If adding a new customer, the status of the person you added has a default value of **Proposed**. Your People/Contact administrator must verify those in proposed status, update them to **Enabled**, and add any other information that is necessary.

To update the customer profile permanently

Use this procedure to make a permanent update to the information on the People record.

1. From the Incident Management console, open a current incident request record belonging to the customer whose profile you are modifying.
2. Click either the **Customer** or **Contact** link.
3. On the People form, complete or modify the required fields.
   If adding a customer record, you do not need to add all the information for this individual's profile, only what is necessary to submit the record.

> ⚠ **Note**
> You cannot define, or add, a **Support Staff Person** record here. For information about adding a Support Staff Person, see Adding a support staff person.

4. Click **Save**.
   If adding a new customer, the status of the person you added has a default value of **Proposed**. Your People/Contact administrator must verify those in proposed status, update them to **Enabled**, and add any other information that is necessary.

First call resolution

Before you assign an incident request, determine if you can resolve the incident yourself. To do this, use the Incident Management Incident Matching feature, or the BMC Knowledge Management application, if you have access to it, to look for matching, or similar, incident requests, problem investigations, known errors, and solution entries.

> ⚠ **Note**
> BMC Knowledge Management is a separate application that must be integrated with Incident Management before you can use it. For information about accessing BMC Knowledge Management, see Accessing BMC Knowledge Management.

If you cannot resolve the incident request, assign the incident request to a specialist. For information about how to do this, see Assigning incident requests.

> ⚠ **Note**
> You can also use the Advanced Search feature to look for similar incident records. For information about how to do this, see Searching for similar incident requests.

Searching for matching records

By using the record matching features, you can search for existing records that describe incidents that are similar to the one you are currently trying to resolve. This helps you ensure that you do not spend time and effort trying to resolve issues that were resolved previously.

> ℹ **Best practice**
> Whenever possible, search for matching records while you are in conversation with the customer. This ensures that you have access to customer-specific information and context, which allows you to conduct a more effective search.

The following video presentation describes how quickly resolve an incident request using incident matching. For a written description of the procedure, see To search for matching records.

> ℹ **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

To search for matching records

1. Open or create an incident request.
2. Use one of the following methods to search for a solution:
    a. Incident Matching feature. To use this method, continue with step 3.
    b. BMC Knowledge Management application. When installed, this application is available from the Links area of the Navigation pane when the Incident Request form is open. For detailed information about how to open this application, see To access BMC Knowledge Management.
3. In the Navigation pane, choose **Functions > Incident Matching.**
4. To view details of a matching record, perform the following steps:
    a. In the search results list at the bottom of the search form, select a record.
    b. Click **View**.
5. If the matching record resolves the current incident, from the Relationship Type list, select Resolved by.
6. To relate the record in the search results list and to copy its solution to the resolution of the incident, click **Relate with Solution**.
7. Alternatively, to relate the record without the solution, click **Relate Without Solution**.

> ⚠ **Note**
> If you do not use the selected matching solution, the system returns you to the Incident Matching form that contains the list of matching records so that you can continue to look for a matching record.

Searching for similar incident requests

Another tool that you can use for finding similar incident request records is the Advanced Search feature, which is available from the Incident Management console.

To search for similar incident requests

1. From the Navigation pane on the Incident Management console, choose **Functions > Advanced Search**.
2. In the Advanced Search Selection dialog box, select the type of search that you want to perform, and then click **Select**.
    - **Search incident request by Work Info** — Searches for incident request using fields from the Work Details tab (Work Info when using the Classic view) tab.
    - **Search incident request by Relationships** — Searches for incident requests using fields from the Relationship form.
    - **Search Incidents by Assignment Logs** — Searches for Incidents using fields from the Assignment Log form.
3. On the search form, provide as much information as possible, and then click **Search**.

4. View the incident requests that match the search criteria in the table that appears.

> ✓ **Tip**
> You can use the advanced search bar to define a more complex set of criteria than you can specify by using only fields in a form. For example, you can search for all incident requests with two different values in the same field. Thus, you can search for all incident requests that have a status of **Resolved** or **Closed**.

Accessing BMC Knowledge Management

This procedure describes how to access the BMC Knowledge Management application from Incident Management.

To access BMC Knowledge Management

If you have access to BMC Knowledge Management, you can use that application to look for a solution, as described in the following table.

When using the Best Practice view	When using the Classic view
With the incident request record open, from the Functions area of the Navigation pane, click **Search Knowledge Base**.	With the incident request record open, from the Quick Links area of the Navigation pane, click **Search Knowledge Base**.

For information about using BMC Knowledge Management, see the BMC Knowledge Management documentation.

Related topics

If you have access to BMC Knowledge Management, you can use that application to help you with the following tasks:

- Performing a first call resolution
- Searching knowledge articles during a root cause analysis
- Performing a problem investigation by finding similar problem investigations
- Searching for matching or similar:
  - Incident requests
  - Problem investigations
  - Known errors or solution entries
- Performing a global search for records that match a key term
- Creating knowledge base articles from resolved incidents

Creating a knowledge base article

If you have access to BMC Knowledge Management, you can create knowledge base articles. These can be helpful to others who are trying to resolve similar requests.

For a description of the procedure to create a knowledge base article, see To create a knowledge base article.

Best practice
"Search early and search often!" This Knowledge Centered Support (KCS) maxim means that before you create a knowledge base article, you should search the knowledge base to determine if there are already articles on the issue. It also means that you should conduct multiple searches using different criteria. This increases the likelihood that you will find a match. For complete information about searching for knowledge base articles, see Searching for knowledge.

Creating a knowledge base article when you create the incident request ensures a tighter integration between incident management and the knowledge base, which is important for good knowledge management.

When you create the knowledge base article, it is important to capture the full context of the incident. This includes capturing technical information, such as hardware and software details, and non-technical information, such as what the customer *thinks* could be causing the incident and what impact the incident is having on them.

BMC recommends that you use the following information categories when capturing technical information.

- Incident — The situation (or question) in the customer's words; what are they trying to do or what is not working.
  It is important to capture the issue in the customer's words, because this is likely that the way that other customers view it the same of similar issues. If the customer's description is reworded or recategorized by technical staff subsequent to the incident request being recorded, it might not be found as a match when searching knowledge base articles the next time a similar issue arises.
- Environment — What technology does the customer have? Was anything in the environment changed recently?
- Resolution — The steps required to resolve the incident or answer the question.
- Metadata — High level categorization of the article's content aids searchability, maintenance, reporting, and other processes related to the handling of the article.

Over time, the way that a person who reports an incident remembers and interprets non-technical information can change. It is important, therefore, to capture non-technical information in a knowledge base article early in the incident handling process. For this reason, BMC also recommends that you create the knowledge base article and register the incident request simultaneously. Even if the incident resolution is not yet known, you can start the knowledge base article and then add resolution information later. This ensures that known details are captured and are available to others who might be working on the same or a similar incident request. By always creating incident requests and knowledge base articles simultaneously, you also ensure that knowledge articles become an integral byproduct of incident registration.

Note
For complete information about creating knowledge base articles, see Creating and editing knowledge articles.

To create a knowledge base article

1. Open the an incident request, problem investigation, or known error record.
2. Create the knowledge base article.

When using the Best Practice view	When using the Classic view
From the Links area of the Navigation pane, click **Create Knowledge**.	From the Quick Links area of the Navigation pane, click **Create Knowledge**.

3. Create the knowledge base article.

When using the Best Practice view	When using the Classic view
From the Functions area of the Navigation pane, click **Create Knowledge**.	From the Quick Links area of the Navigation pane, click **Create Knowledge**.

Creating a solution database entry from an incident

From Problem Management, you can publish the resolution from an incident into the solution database.

For a description of the procedure to create a database entry, see To create a solution entry from an incident.

Best practice
"Search early and search often!" This Knowledge Centered Support (KCS) maxim means that before you create a knowledge base article, you should search the knowledge base to determine if there are already articles on the issue. It also means that you should conduct multiple searches using different criteria. This increases the likelihood that you will find a match. For complete information about searching for knowledge base articles, see Searching for knowledge.

Creating a knowledge base article when you create the incident request ensures a tighter integration between incident management and the knowledge base, which is important for good knowledge management.

When you create the knowledge base article, it is important to capture the full context of the incident. This includes capturing technical information, such as hardware and software details, and non-technical information, such as what the customer *thinks* could be causing the incident and what impact the incident is having on them.

BMC recommends that you use the following information categories when capturing technical information.

- Incident — The situation (or question) in the customer's words; what are they trying to do or what is not working.
  It is important to capture the issue in the customer's words, because this is likely that the way that other customers view it the same of similar issues. If the customer's description is reworded or recategorized by technical staff subsequent to the incident request being recorded, it might not be found as a match when searching knowledge base articles the next time a similar issue arises.
- Environment — What technology does the customer have? Was anything in the environment changed recently?
- Resolution — The steps required to resolve the incident or answer the question.
- Metadata — High level categorization of the article's content aids searchability, maintenance, reporting, and other processes related to the handling of the article.

Over time, the way that a person who reports an incident remembers and interprets non-technical information can change. It is important, therefore, to capture non-technical information in a knowledge base article early in the incident handling process. For this reason, BMC also recommends that you create the knowledge base article and register the incident request simultaneously. Even if the incident resolution is not yet known, you can start the knowledge base article and then add resolution information later. This ensures that known details are captured and are available to others who might be working on the same or a similar incident request. By always creating incident requests and knowledge base articles simultaneously, you also ensure that knowledge articles become an integral byproduct of incident registration.

Note
For complete information about creating knowledge base articles, see Creating and editing knowledge articles.

To create a solution entry from an incident

1. Open the incident record.
2. In the **Quick Action** area on the left side of the Incident form, select **Create Related Request > Solution**

Database.
The Solution Database form opens with relevant information copied over from the incident request.

3. Supply information for the mandatory fields.
   a. In the **Solution** field on the **Details** tab, type a description of the solution.
   b. On the **Assignment** tab, complete the **Support Company**, **Support Organization**, and **Assigned Group** fields.
4. Review the fields on the other tabs for optional information that you can add, which would help others understand the solution.
5. Click **Save**.

Relating incident requests as duplicates

You can relate an incident request to another incident request as a *duplicate*.

When you change the status of the original incident request to Resolved, Closed, or Canceled, the system performs the following actions:

1. Copies the following fields from the original request to the duplicate request:
   - **Operational Categorization**
   - **Product Categorization**
   - **Resolution**
   - **CI**
2. Resolves all of the duplicate requests.

Also, if the service indicated in the **Service** field of the original incident request is a registered service of the company for which the duplicate request was submitted, and the duplicate record's **Service** field is empty, the system copies the service from the original incident request to the duplicate.

You can also relate an incident to an incident that is already resolved or closed. If you do this, the action of relating the two requests also copies the fields listed above from the original incident to the duplicate.

To relate an incident request as a duplicate

For information about creating relationships, see Defining relationships.

Consider the following points when creating the relationship:

- If the current incident is a duplicate of the original incident, from the **Relationship Type** list, select **Duplicate of**.
- If the current incident is the original incident, from the **Relationship Type** list, select **Original of**.

Assigning incident requests

Service desk analysts and Group Coordinators each play a role in assigning incident requests. The information in this section applies to service desk analysts. If you work as a Group Coordinator or in another management role, see Working with incident requests as a manager.

For information about the group coordinator's role, see Assigning incident requests as a group coordinator.

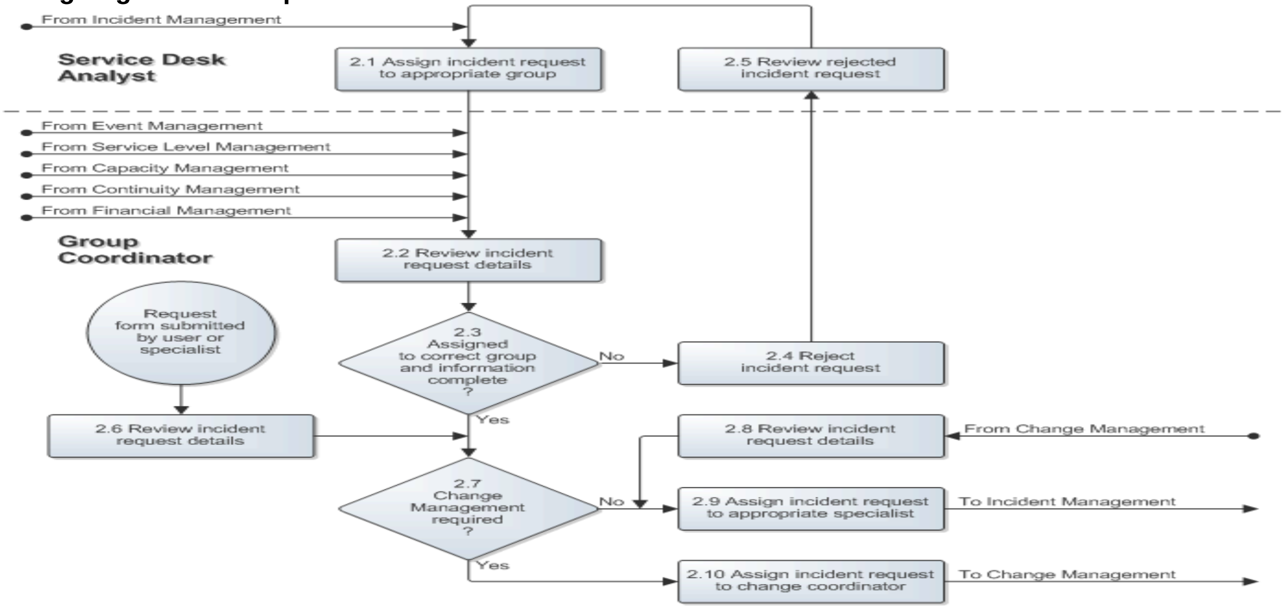
When you register a *new* incident request, one of the following actions happens:

- The routing rules used by Incident Management automatically assign the incident request to the most appropriate group when the incident request record is saved.
- If the incident request is created from a template that has an assignment group predefined, the incident request is assigned to the predefined assignment group.

If you reopen a *current* incident request, you manually reassign the incident request to the most appropriate group. For information about how to do this, see Reassigning incident requests. The coordinator of the group to which the incident request is assigned then reviews the request.

The following figure provides an overview of the incident request assignment process as described by the BMC Service Management Process Model:

Assigning incident requests


From Incident Management
Service Desk Analyst
2.1 Assign incident request to appropriate group
2.5 Review rejected incident request
From Event Management
From Service Level Management
From Capacity Management
From Continuity Management
From Financial Management
Group Coordinator
2.2 Review incident request details
Request form submitted by user or specialist
2.3 Assigned to correct group and information complete ?
No
2.4 Reject incident request
Yes
2.6 Review incident request details
2.8 Review incident request details
From Change Management
2.7 Change Management required ?
No
2.9 Assign incident request to appropriate specialist
To Incident Management
Yes
2.10 Assign incident request to change coordinator
To Change Management

Reassigning incident requests

You can reassign an incident to either an individual or a support group. Use the shortcut in the Quick Actions section (Quick Links in Classic view) of the Incident Request form to reassign an incident to yourself (Assign to Me) or to reassign an incident based on automatic routing (Auto Assign). This assigns the incident based on predefined mapping. Automated assignment can be based on the customer organization, location, operational categorization, or product categorization.

To reassign an incident

1. Open the incident request record.
2. Reassign the investigation:
   - *(Best Practice view)*
     a. On the Incident form, select the **Assigned Group** from the list associated with the **Assigned Group** field.
     b. Select the **Assignee** from the **Assignee** field list.
   - *(Classic view)*
     a. Click the **Assignment** tab.

   b. Select the **Assigned Group** from the list.
   c. Select the **Assignee** from the list.
3. Click **Save.**

Updating an incident request

Use this general procedure when updating an incident request.

To update an incident request

1. Open the incident request
2. Update the details as required.
3. Click **Save** when you finish.

Resolving and closing incident requests

The information in this section is for people who fulfill the role of specialist. *Group coordinators* and *on-duty managers* should also be familiar with the information in this section to better understand the support staff tasks and so they can fulfill the role of support staff if necessary. The tasks described by this section are organized according to the stages of the incident management lifecycle as described by the BMC Service Management Process Model. See Process flow status and the lifecycle of an incident request for an illustration of the incident management lifecycle.

- Resolving incident requests
- Closing incident requests

Resolving incident requests

You review an assigned incident request to determine whether the resolution requires a change.

If the preferred method of incident request resolution is through the change management process, you escalate the incident request by assigning it to the service owner. For information about how to do this, see Creating a change request.

Perform an incident request resolution by using the change management process when the resolution requires a change that will:

- Have a negative affect on the service during the service hours (defined by the SLA)
- Change the functionality of a service
- Require an update to the BMC Atrium Configuration Management Database (BMC Atrium CMDB)

If the incident request does not require the change management process, you resolve the incident.

After resolving the incident request, you update the incident request, to make sure the user is notified of the resolution.

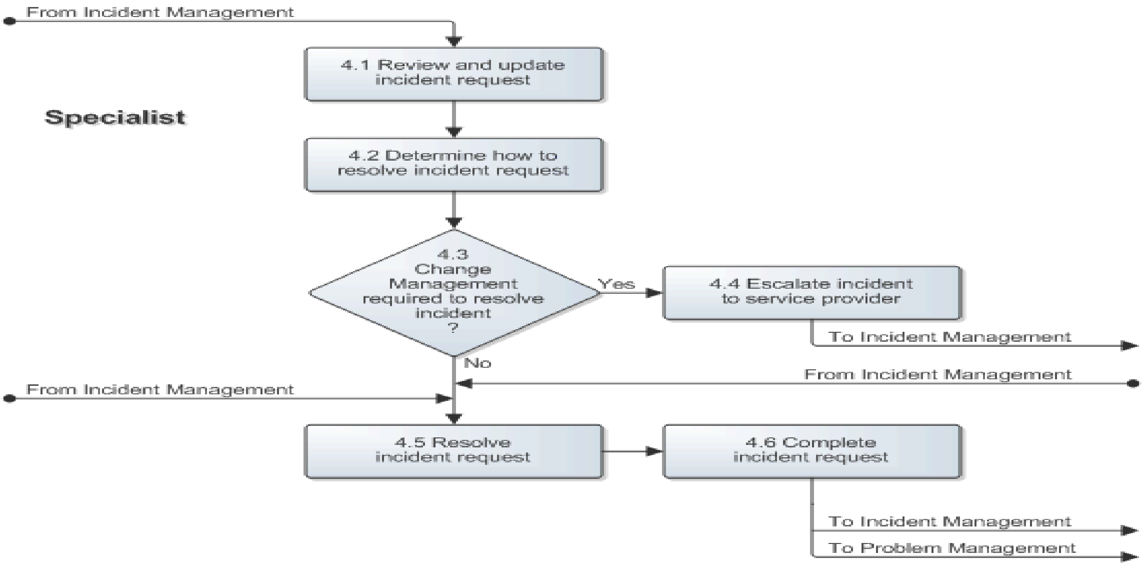
If the resolution information entered in the incident request might help users, service desk analysts, or other specialists resolve future, similar cases, you can create a solution database entry to document the solution.

If the incident request was resolved using a workaround, but the incident can recur, you notify the problem coordinator, so that a problem investigation record can be created.

The following figure provides an overview of the incident request resolution process as described by the BMC

Service Management Process Model.

Incident request resolution


From Incident Management
Specialist
4.1 Review and update incident request
4.2 Determine how to resolve incident request
4.3 Change Management required to resolve incident ?
Yes
4.4 Escalate incident to service provider
To Incident Management
No
From Incident Management
From Incident Management
4.5 Resolve incident request
4.6 Complete incident request
To Incident Management
To Problem Management

Accepting an incident request

There are several on-going tasks that you must perform when you accept and begin working on an incident request. These on-going tasks help to keep the incident request record up-to-date with the latest information about the work being performed to resolve the incident.

These on-going tasks include:

- Receiving notification of assignments
- Working with assignments
- Using tasks
- Recording time worked on an incident request
- Creating work information entries from the console
- Modifying work information entries

Working with assignments

When you work on open incidents, you are working on incidents assigned to you or to your support group. You can also assist with an incident assigned to another support group when a task is assigned to you.

To accept an assignment

1. Open the incident request record.
2. Assign the incident request record to yourself.
    - *(Best Practice view)* From the Quick Actions section of the Navigation pane, click **Assign to Me**.
    - *(Classic view)* From the Quick Links section of the Navigation pane, click **Assign to Me**.

3. Change the Status to In Progress.
4. Click **Save**.

Searching for a solution

You can search for information that might help resolve the current incident request in other incident requests, problem investigations, known errors, and solution database entries.

To find information that might help resolve the current incident request, use the methods for finding similar incident requests described in First call resolution. If BMC Knowledge Management is installed, you can also use this application to search for possible solutions.

For information about accessing BMC Knowledge Management, see First call resolution.

For information about how to use BMC Knowledge Management, see the BMC Knowledge Management documentation.

Recording time worked on an incident request

You must keep track of the time that you spend working on an incident request.

- If the incident request record is open on your desktop while you are working on it, you can use a timer to keep track of the time. Or, you can enter the time manually. See Recording your time.
- If you receive assistance from someone else, you can also keep track of their time through the Incident Assignment Log. The Incident Assignment Log contains a record of who created the current incident request as well as individual records for each group and person who was subsequently assigned to the request. Each record contains the total effort duration for each assignee (that is, the amount of time each group or person worked on the incident request), as well as other information. See Recording time for an assistant.

  > ⚠ **Note**
  > Because the Incident Assignment Log is historical, it does not contain a record for the current assignee, only for previous assignees. The system updates the Incident Assignment Log with a record for the most recent assignee each time the incident request is reassigned. When the incident request is moved to the **Closed** state, the system writes the final assignee record to the Incident Assignment Log.

- You can also update the amount of time you spent working on an incident request after it has been assigned to another assignee. See Updating your time after the incident request is reassigned.

Recording your time

Use the following procedure to record time against an incident request that currently is assigned to you.

To record your time

1. Open the incident request record.
2. Perform one of the following tasks.
   - *(Best Practice view)* In the Work Detail area, click the clock graphic beside the **Assignee** field to open the Effort Time Spent window.
   - *(Classic view)* Click the **Assignment** tab.
3. Enter the time you spent on the incident request in the **Effort Time Spent (Minutes)** field.

✓ **Tip**
Use the automatic timer to keep track of your time anytime you work on the incident request while the incident request record is open on your desktop. To start the timer, click the **Stopped** button (the text on the button changes to Started-the button's text reports the timer's current status). When you finish working on the incident request, make sure you click the **Started** button (the text on the button changes to **Stopped**).

4. When working in Best Practice view, click **Close**.

⚠ **Note**
The **Effort Time Spent Minutes** field is a data entry field only. When you click **Close**, the time value that you provided in **Effort Time Spent (Minutes**) is written to a database field called **Total Time Spent**, which totals the time spent on the incident request for the current assignee. After Incident Management writes the time value to **Total Time Spent**, it resets **Effort Time Spent Minutes** to zero. If you reassign the incident request or resolve it, the cumulative time is written from **Total Time Spent** to the **Assignment Log** and **Total Time Spent** is reset to zero.

5. To save the time entry, click the **Save** button at the bottom of the incident form.

Recording time for an assistant

Use the following procedure to record time against an incident request for someone who assisted you but who was not formally assigned to the incident request.

To record an assistant's time

1. Open the incident request record.
2. Perform one of the following actions.
   - *(Best Practice view)* In the **Work Detail** area, click the clock graphic beside the **Assignee** field to open the **Effort Time Spent** window.
   - *(Classic view)* Click the **Assignment** tab.
3. Click **Update Assignment Log** to open the Incident Assignment Log dialog box.
4. Add the assistant to the Assignment Log by selecting values for the following fields:
   - **Support Company** — The name of the assistant's support company
   - **Support Organization** — The name of the assistant's support organization
   - **Assigned Group** — The name of the assistant's assigned group
   - **Assignee** — The name of the assistant's name of the individual
5. In the **Effort Time Spent (Minutes)** field, enter the time the assistant spent on the incident request.
6. Click **Add**.

An entry containing this information appears in the table at the bottom of the Incident Assignment Log dialog box.

Updating your time after the incident request is reassigned

Use the following procedure to update the time that you spend on an incident request after it has been reassigned.

For example, if the person or group to which the incident request is reassigned asks for your help with some aspect of the incident request resolution, you can update your record in the Incident Assignment Log with the additional time.

> ⚠ **Note**
> You can update the time only for your own Incident Assignment Log records. You cannot update the records of other support groups or individuals.

To update your time after the incident request is reassigned

1. Open the incident request record.
2. Open the Incident Assignment Log dialog box.
   - *(Best Practice view)* In the Work Detail area, click the clock graphic beside the **Assignee** field to open the Effort Time Spent window.
   - *(Classic view)* Click the **Assignment** tab.
3. Click **Update Assignment Log**.
4. In the table at the bottom of the Incident Assignment dialog box, select your record.
5. In the **Effort Time Spent (Minutes)** field of the Update Assignee Effort Duration area, type the number of minutes that you are adding or subtracting from your recorded time.
6. Click the plus button ⊕ to add the time to the record's total amount of time, or click the minus button (-) to subtract the time.
7. Click **Close**.

   > ⚠ **Note**
   > You cannot delete a completed assignment log.

Creating work information entries from the console

When you begin working on an incident request or problem investigation, you must make sure that you keep careful work information entries in the Work Details area of the incident request or problem investigation record (or in the Work Info tab when using the Classic view), explaining what you have done.

For example, you might want to add a note that a particular CI was deployed, and include the date.

You can add work information entries to an incident request or problem investigation record directly from the Incidents or Problems table (as described in this procedure), or you can add them to open records. For information about how to do this, see Adding work information entries to the current record.

> ⚠ **Notes**
> If you are using the Best Practice view, you can view multiple work info entries at the same time by clicking the **History** icon. When you click this icon, the system displays a pop-up window with the Notes field entries arranged with the most recent entry at the top (a date and time stamp is also visible with each entry).
>
> If your user ID has Incident Viewer or Problem Viewer permissions, you can add and modify Work Info entries, however, you cannot create or modify incident requests, problem investigations, known errors, or solution database entries.

This section has information about the following topics:

- Adding work information entries from the console table
- Adding work information entries to the current record
- Modifying work information entries
- Modifying work information entries from an open incident request

Adding work information entries from the console table

Use this procedure to add an information entry to a record from either the Incident or Problem console table.

To add work information entries from the console table

1. From the console, select the record you need to add a work information entry to.
2. At the bottom of the console, if the Tasks table is visible, open the Detail area by clicking **Show Detail**.
3. Click **Create**.
4. Enter the work information details in the **Work Info** dialog box.
5. To add an attachment to the record, right-click in the attachment table and select **Add** from the menu that appears.
6. Choose whether to lock the work log.

   > ⚠ **Note**
   > If you select **Yes**, you cannot modify the work log after you save it.

7. Choose the type of view access:
   - **Internal** — Choose this if you do not want the customer to see the work information entry on the Requester console or the BMC Service Request Management console.
   - **Public** — Choose this if you want the customer to see the work information entry.

> **Note**
> The information in this note applies to environments that also run BMC Service Request Management.
>
> When a work note is created in a request that originated from the BMC Service Request Management console and is marked as *Public*, the work note also appears in the request's activity log in the Request Entry console of BMC Service Request Management. If the work note is updated, the *original* work note remains in the request's activity log, but the updated information is placed in a new entry in the request's activity log.
>
> If the work note is updated and the Assignee marks it as *Internal*, the original work note remains in the request's activity log, but the updated information is not displayed.

8. Click **Save**.

> **Note**
> To see a report of selected work information entries, select one or more entries, and click **Report**.

Adding work information entries to the current record

In addition to adding work information from the console, you can add work information to the record that currently is in view.

To add work information entries to an open record (Classic view)

1. With the record open, click the **Work Info** tab.
2. Complete the fields on the tab as described in the Classic view section of Creating work information entries from the console.

To add work information entries to an open record (Best Practice view)

1. Open the incident request or problem investigation record.
2. On the Work Details tab, click the **Create** icon.
3. Type the information in the **Notes** field at the bottom of the tab.

> **Note**
> If you want to add an attachment to the work information note, perform step 4 to step 6.

4. Click the button to the right of the **Attachment** field.
   The Add Attachment dialog box opens.
5. Click **Browse** and then navigate to the file you want to attach.
6. Select the file, click **Open**, and then click **OK**.
   The file name appears in the **Attachment** field.

⚠ **Note**

- To view the attachment, click the spectacles icon.
- To remove the attachment, click the eraser icon.
- By default, the **Work Info Type** is **General Informatio**n (the **Work Info Type** let's you categorize the type or source of the work info entry); the **Locked** status is **Yes** (the work note cannot be edited after you save it); the **View Access** is **Internal** (your customers cannot view the entry). If you want to change these settings, click the arrow beside More Details to reveal these fields and then update them appropriately. You can also make additional attachments-to a total of 3-in the More Details area. Clicking the arrow again hides the fields.

7. Click **Add**.
   The note text appears in the Work Details table.

⚠ **Note**
You can sort the table by clicking any of the column headings, except Notes. The table does not sort on the Notes column.

Modifying work information entries

If the work information entry is not locked, you can modify any field on it. The following procedure describes how to modify the notes, add attachments, lock the entry so it cannot be modified later, and change the viewing access level.

To modify a work information entry from the console table

From the Incident or Problem console, select the incident request or problem investigation record.

1. At the bottom of the console, if the Tasks table is visible, open the Detail area by clicking **Show Detail**.
2. From the list of work information entries, select the work information record that you want to update.
3. Click **View**.
4. Make the required modification as described in the following table:

Modification	Action
To update the note	Click inside the **Notes** field and type the changes.
To add an attachment	Right-click in the attachment table and select **Add** from the menu that appears, and then follow the onscreen instructions. **Note:** Attachments to work information entries created in BMC Service Request Management are not transferred with information sent to a back-end application, such as an incident, a change request, or a work order. You can access the attachments only from the service request.
To lock the entry	From the **Locked** list, select **Yes** or **No**. **Note:** If you select **Yes**, the work information entry cannot be modified after you save it.

To change the view access level	From the **View Access** list, select **Internal** or **Public** from the **View Access** list. In environments that also run BMC Service Request Management, when a work note with the Public access level is created in an incident request or a problem investigation that originated with the BMC Service Request Management console, the work note also appears in the request's activity log in the Request Entry console of BMC Service Request Management. If the work note is updated, the *original* work note remains in the request's activity log, but the updated information is placed in a new entry in the request's activity log. If the work note is updated and the Assignee marks it as *Internal*, the original work note remains in the request's activity log, but the updated information is not displayed. **Internal** — Select this if you do not want the customer to see the work information entry from the Requester console or the BMC Service Request Management console. **Public** — Select this if you want the customer to see the work information entry.

5. Click **Save**.

Modifying work information entries from an open incident request

You can also modify a work information entry from an open incident request.

To modify a work information entry from an open incident request (Classic view)

1. With the incident request record open, click the **Work Info** tab.
2. Select the work information entry that you want to update.
3. Complete the fields on the tab as described in Modifying work information entries.

To modify a work information entry from an open incident request (Best Practice view)

1. Open the incident request record.
2. On the Work Details tab, select the work information entry that you want to update.
   The **Notes** field updates to contain the work info text and the More Details area expands to reveal the hidden fields.
3. Make the required changes.

   > ⚠ **Note**
   > If you need to remove an attachment, click the Eraser icon beside the associated **Attachment** field.

4. Click **Save**.

Creating a change request

If infrastructure change is required to permanently resolve the incident request, assign the incident request to a Change Coordinator. For information about how to reassign a ticket to a Change Coordinator this, see Reassigning incident requests. If you have the correct change management permissions, you can create a change request from the Incident Request form. If you are not sure about your change management permissions, ask your system administrator.

To create change from an incident

1. Open the incident request record.
2. Create the change request from the incident request.
   - *(Best Practice view)*
     a. From the Quick Actions area, click the arrow beside **Create Related Request**.
     b. From the menu, select **Infrastructure Change**.
   - *(Classic view)* From the Navigation pane, select **Create Other Requests > Create Change.**

     A Change Request form appears. The Product and Operational Categorization are copied from the incident to the infrastructure change. A relationship is created between the change and the incident.
3. Complete the Change Request form.
   For information about creating change requests, see Initiate stage - Creating change requests.
4. Click **Save**.

Closing incident requests

When you resolve the incident request, move the incident request status to Resolved.

If you are in communication with the customer when you resolve the incident request, and can verify the resolution, move the request status to **Closed** immediately. For information about how to do this, see Closing an incident request.

If you cannot verify the resolution at the time you make it, complete the incident request with the **Resolved** status, and set the **Status Reason** field to **Customer Follow-up Required**. For information about how to do this, see Completing an incident request.

> ⚠ **Note**
> The customer must verify the resolution within a specified period of time, or Incident Management automatically moves the incident request status to **Closed**. The length of this period is configurable. Check with your system administrator to determine how much time your organization specifies. The default setting is 15 days.

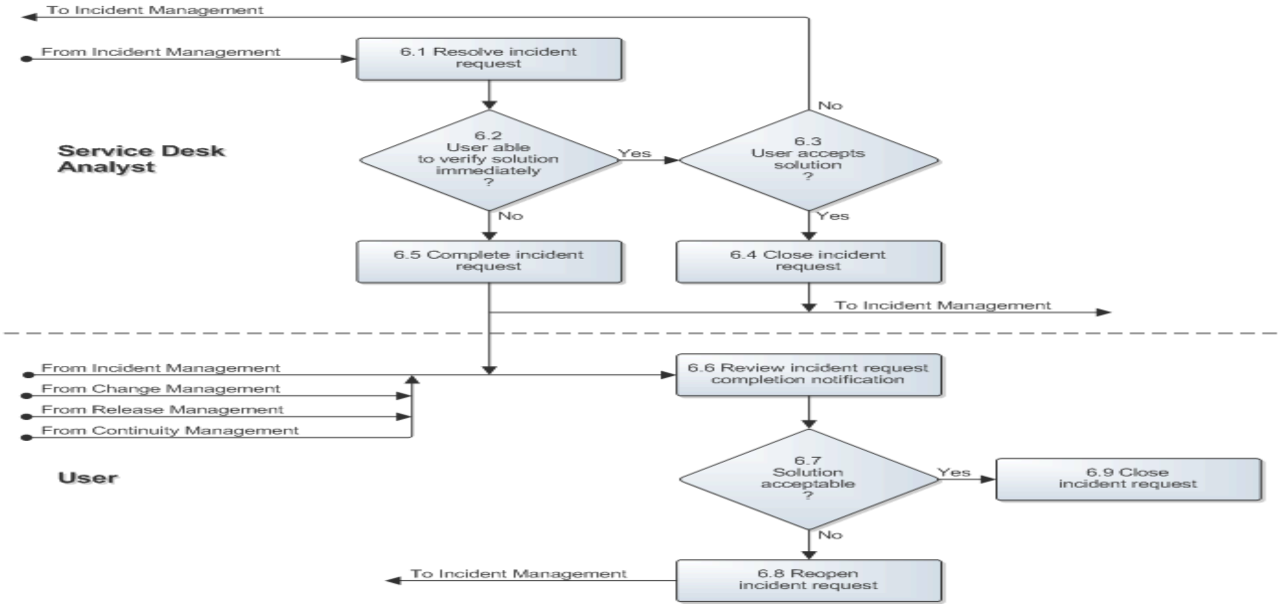
If the resolution information entered in the incident request can help users, service desk analysts, or other specialists resolve future, similar cases, you can create a solution database entry to document the solution. For information about how to do this, see Creating a solution database entry from an incident.

If the incident request was resolved using a workaround, but the incident can recur, notify the problem coordinator so that person can investigate the issue in a timely manner and then decide whether to create a problem investigation.

If the user does not accept the resolution, the user contacts the service desk and asks for the incident request to be reopened. Depending on the incident request's status refer to one of the sections listed at the bottom of the page.

The following figure provides an overview of the incident request closure process as described by the BMC Service Management Process Model.

Incident request closure


To Incident Management
From Incident Management
6.1 Resolve incident request
Service Desk Analyst
6.2 User able to verify solution immediately ?
Yes
No
6.3 User accepts solution ?
No
Yes
6.5 Complete incident request
6.4 Close incident request
To Incident Management
From Incident Management
From Change Management
From Release Management
From Continuity Management
User
6.6 Review incident request completion notification
6.7 Solution acceptable ?
Yes
6.9 Close incident request
No
To Incident Management
6.8 Reopen incident request

Completing an incident request

Use this procedure when you have resolved the incident request, but are unable to have the user verify the resolution.

To complete an incident request

1. Open the incident request record.
2. Change the **Status** field to **Resolved**.
3. Select the appropriate status reason.
   The status reason can indicate action required before the incident is closed, such as **Customer Follow-up Required**. See Incident status reason definitions for definitions of the status reasons.

   > **Note**
   > If the incident type is **User Service Restoration** or **Infrastructure Restoration**, you must perform the following step. If the incident type is User **Service Request** or **Infrastructure Event**, then the following step is recommended, but not required.

4. Provide a description of what you did to resolve the incident request. You can do this using one, or both, of the following methods.
   - **Resolution** field — Type a description of what you did to resolve the incident request.
   - **Resolution Categorization** fields — Select a predefined resolution from a set of menu choices on the **Resolution Categorization** area of the **Categorization** tab.
     a. Click the **Categorization** tab.
     b. Click **Show Resolution Categorization**.
     c. Select a resolution description from the Resolution Categorization Tier 1, Tier 2, and Tier 3 menus.

> ⚠ **Note**
> When you associate a CI to an incident request, the Service Desk application automatically maps the incident request's resolution categorization to the CI's product categorization.

5. Click **Save**.
   The status of the incident is set to Resolved.
   If CI unavailability was created from this incident and your support group is responsible for the CI unavailability, you are prompted to update the CI unavailability.
   - To update the CI unavailability, for example, if the CI is now available, click **Update**. For details about CI unavailability.
   - To continue resolving the incident without updating the CI, click **Close and Continue Save**.
   - To return to the Incident Request form without saving, click **Close and Cancel Save**.

> ⚠ **Note**
> When you resolve an incident request that has related duplicate requests, Incident Management also updates those duplicate requests as resolved. It can take up to several minutes to update duplicate requests, because Incident Management processes these updates in the background.

Incident status reason definitions

The content of the **Status Reason** menu is determined by the selection that you make in the **Status** field. In most cases, the status reason is for informational use and does not affect how the application behaves. This means that you can assign meanings to the status reasons that are appropriate to your organization's needs. The status reason definitions provided in the following tables, therefore, are recommended definitions only.

> ⚠ **Note**
> The Pending status reason of Client Hold affects the calculation of service level agreement metrics in BMC Service Level Management, if that application is integrated with your installation of BMC Service Desk. Refer to the Client Hold definition in the Pending table, which follows, for more information about how this status reason affects the service level calculations.

Pending status reason definitions

Status reason	Explanation
Local Site Action Required	Waiting for some type of action to occur at the location where the incident occured.
Purchase Order Approval	A purchase that requires approval is needed to move the incident request to the next status.
Registration Approval	The request requires approval from another department before proceeding.
Supplier Delivery	Awaiting the delivery of a good or service from a supplier before the incident request can be moved to the next status.

Support Contact Hold	The help desk agent assigned to the incident request is currently working on other Incident requests. Alternatively, the help desk agent is awaiting response from someone in a second or third tier support group.
Third Party Vendor Action Required	Some type of action from a third party vendor must occur before the incident request can be moved to the next status.
Client Action Required	Some type of action from the client (that is, the person indicated in the Customer field on the incident form) must occur before the incident request can be moved to the next status.
Infrastructure Change	The incident request cannot move to the next status until an infrastructure change occurs.
Request	Pending a generic request for support from some other third party.
Future Enhancement	The incident request cannot move to the next status until an enhancement to some part of the environment takes place.
Client Hold	The client has asked the service desk to temporarily stop working on the incident request. **Note:** If you select this status reason and your instance of Incident Management is integrated with BMC Service Level Management, the service level agreement metric collection stops until you change the status or status reason.
Monitoring Incident	The incident that triggered the incident request is ongoing and must be analyzed before further action can take place.
Automated Resolution Reported	The service desk received an automated report that the incident request was resolved, which needs verification.

Resolved status reason definitions

Status reason	Explanation
Future Enhancement	The root cause of the incident request will be addressed by future enhancements to the environment.
Monitoring Incident	The root cause of the incident cannot be determined, but the help desk is monitoring the situation to determine if it will recur.
Customer Follow-Up Required	The incident request was resolved by the help desk, but the customer needs to confirm the resolution.
Temporary Corrective Action	The incident request is resolved, but the action taken is only a temporary resolution, until a more permanent resolution can be implemented.
No Further Action Required	The customer is reporting that the reported incident is no longer an issue.
Automated Resolution Reported	The service desk received an automated report that the incident request was resolved.

Closed status reason definitions

Status reason	Explanation
Infrastructure Change Created	You created an infrastructure change request was created from the incident request when you closed the incident request .

Automated Resolution Reported	The service desk received an automated report that the incident request was resolved.

Canceled status reason definitions

Status reason	Explanation
No longer a causal CI	The CI against which the incident request was created is not the CI that caused the incident.

Closing an incident request

This activity ensures that the incident has successfully restored the service to the user and that the user is satisfied with the outcome. When the user agrees that the incident can be closed, review the incident request record for completion and, if appropriate, create a solution database entry.

If you leave an incident as resolved, after a period of time Incident Management closes the incident. The time for your installation to close the incident is configurable, so check with your administrator to find out the interval for your organization. The default setting is 15 days.

To close an incident request

1. Open the incident request record.
2. Review the Incident Request form to make sure that it is complete and accurate.
3. In the Status field, choose **Closed**.
4. Click **Save**.

The status is now set to Closed. If the incident was broadcast, the broadcast is removed.

Quickly closing an incident request

Under some circumstances, you can quickly close the incident request, without first passing it through the **Resolved** status.

For example, if you are on the phone with a customer and can confirm with the customer that the incident request has been resolved, you can use this procedure to close the incident request immediately.

> ⚠ **Note**
> You cannot perform this procedure if the status of the incident request is already set to **Resolved**.

To quickly close an incident request

1. With the incident request open, click the down arrow in the area of the process flow bar that corresponds with the current status of the incident request (for example, **Resolution** and **Recovery**).
2. From the menu, select **Next Stage > Close**.
   If any information is missing from the record that is required to close it, a dialog box appears asking for the information.
3. If prompted to, provide any missing information.
4. Click **Save**.

The incident request moves to the **Closed** status.

Moving a resolved incident request back to In Progress

If the recorded resolution did not resolve the incident, you can restore the incident request record to the In Progress status. This also moves the incident back to the Resolution and Recovery stage in the incident request lifecycle.

Use the following procedure to move an incident request record with a status of Resolved back to the In Progress status. You do this if the reported resolution did not resolve the incident request, and further work is needed.

To move a resolved incident request to In Progress

1. Open a resolved incident.
2. In the **Status** field, select **In Progress**.
3. Click **Save**.

The incident moves back to the **Resolution and Recovery** stage, and the status changes from **Resolved to In Progress**.

Reopening a closed or resolved incident request

Use the following procedure when you want to reopen a resolved or a closed incident request.

> ⚠ **Note**
> To reopen a closed incident request, you must have support group lead or support group manager permissions. People with these permissions can also modify a closed incident request if they are the support group lead or support group manager of the Incident Owner group. Someone with incident master permissions can modify any closed incident request.

To reopen a closed incident

1. Open a closed incident.
2. From the Navigation pane, select **Functions > Re-open incident**.
   A new Incident Request form appears with a new incident number. The basic details from the closed incident are copied to it and a relationship is created between the new and closed incident request.

   > ⚠ **Note**
   > The Re-open option is only enabled under Functions when the status of the selected record is Closed.

3. On the new Incident Request form, click **Save**.

To reopen a resolved incident

Anyone with Incident Master permissions, or anyone with Incident User permissions belonging to the Incident Assigned group or the Incident Owner group can use the Reopen Incident function to reopen a resolved incident request.

1. Open the resolved incident.

2. On the process flow bar, click the arrow on the **Incident Closure** stage and select **Reopen** from the menu.

Working with incident requests as a manager

The information in this section is for people who fulfill the management role of group coordinator. On-duty managers should also be familiar with the information in this section. Other people in your organization, who occasionally fulfill the role of group coordinators and on-duty managers, should also be familiar with the information in this section. Using the Incident Management console, managers can assign and track incident requests, make escalations when necessary, and approve solutions. The tasks described by this section are organized according to the stages of the incident management lifecycle as described by the BMC Service Management Process Model. For more information about the incident management lifecycle, see Incident Request lifecycle.

- Date fields on the Incident Request form
- Assigning incident requests as a group coordinator
- Tracking incident requests
- Handling incident escalations
- Approving solutions

Date fields on the Incident Request form

This topic provides an overview of the date fields on the Incident Request form. Understanding where the dates come from, what they mean, and how they relate to service level agreements (SLAs) can help you to prioritize the incident request assignments.

The **Required Resolution Date Time** field maps to the **Date Required** field on the Requester console. Someone using the Requester console can use the **Date Required** field to specify the date or time by which the request should be fulfilled. This is the *suggested* date or time that the customer wants the request to be fulfilled; no service level workflow is related to this field.

The **Target Date** field is the date or time by which the request *must* be resolved, according to the SLA targets. The **Target Date** field is set by the BMC Service Level Management application when SLA targets are defined. If SLA targets are not defined, you must set the **Target Date** field manually.

The **Responded Date** is the date on which the incident request was first responded to. Incident Management populates this field when one of the following conditions occurs:

- Someone sets the **Response** field on the Incident Request form to **Yes**.
- The incident request is created by a service desk analyst *and* the entry in the **Reported Source** field is configured to trigger an automatic update of the **Responded Date** field.

> ⚠ **Note**
> Under the second condition, Incident Management does not display the **Response** field.

Other date fields on the Incident Request form — **Reported Date**, **Closed Date**, and so on — are completed by the Incident Management system when the milestones represented by the field names occur.

Assigning incident requests as a group coordinator

This information in this section applies to group coordinators.

This topic contains the following information:

- Accepting incident requests

- Rejecting incident requests

Accepting incident requests

When an incident request is assigned to a group by the service desk analyst, you must review it before assigning it to a specialist.

If important information is missing from the incident request or if it is assigned to the wrong group, you send it back to the service desk for correction by reassigning it back to the service desk. For information about how to do this, see Reassigning incident requests.

If the incident request is accepted, you check whether the request requires the change management process. If it does, your escalate (or assign) the incident request to the service owner. For information about how to do this, see Assigning incident requests.

The resolution of an incident request is performed using the change management process when the resolution requires a change that will:

- Have a negative affect on the service during the service hours (defined by the SLA)
- Change the functionality of a service
- Require an update to the BMC Atrium Configuration Management Database (BMC Atrium CMDB)

If the incident request does not require the change management process, you assign the incident to a specialist within your group.

If a change is required, you assign the incident request to the change coordinator of the affected service. For information about how to do this, see Assigning incident requests.

For information about rejecting incident requests, see Rejecting incident requests

Rejecting incident requests

If the incident request does not contain enough information for the specialist to work with, or if it is assigned to the wrong group, you can reject the incident request by assigning it back to the service desk.

> ⚠ **Note**
> Ensure that you include a note in the Work Info section of the incident request record explaining why the incident request was rejected. Include the name of the correct group to which the incident request needs to be assigned, if known.
>
> For information about how to do this, see Reassigning incident requests.

Tracking incident requests

If BMC Service Level Management is installed, you receive a notification when the incident request is in danger of breaching the service terms. For example, this happens when:

- The target response time has elapsed and the incident is still assigned.
- The target resolution time has elapsed and the incident is still open (not resolved, closed, or canceled).

Note
You can view the Responded Date on the Date/System tab of the Incident Request form. For details about service target calculations, see Overview of BMC SLM calculations.

You can configure BMC Service Level Management to send notifications to incident assignees, assignee group coordinators, incident owners, or owner group coordinators, by using templates included with Incident Management when you integrate it with BMC Service Level Management. For details about configuring service targets and notifications in BMC Service Level Management, see Configuring service targets and Configuring the Notification Engine.

When you receive an escalation, you determine the cause of the notification and act accordingly.

For example, if the notification occurred because an SLA was breached, you escalate the incident request to the service owner of the affected service.

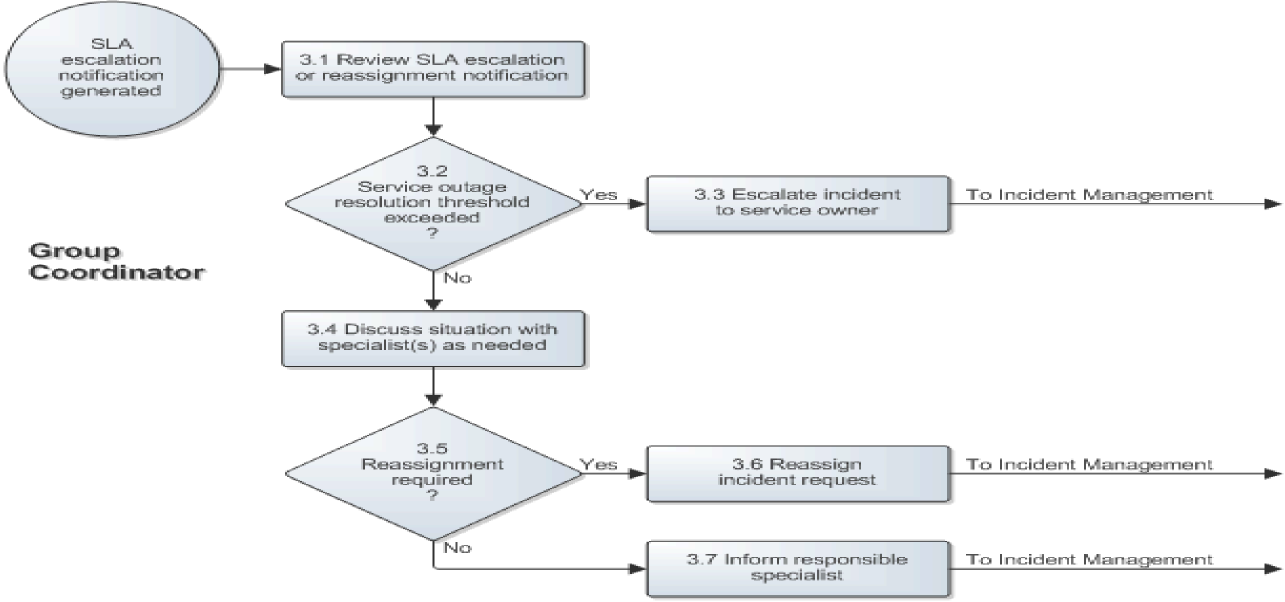
If, however, the escalation notification occurred because an SLA threshold is approaching a breach, you determine whether the incident request needs to be reassigned to another specialist with different skills, greater experience, or with different access rights.

If you decide not to reassign the incident request, then you must notify the assigned specialist that the incident request must be resolved quickly to avoid any service level objective (SLO) violations.

Beginning with Incident Management version 7.6.00, you can place incident requests that require special monitoring on the Watch List (see Working with the Watch List for information about using this new feature).

The following figure provides an overview of the tracking incident requests process, as described by the BMC Service Management Process Model:

Tracking incident requests


SLA escalation notification generated
3.1 Review SLA escalation or reassignment notification
3.2 Service outage resolution threshold exceeded ?
Yes
3.3 Escalate incident to service owner
To Incident Management
No
Group Coordinator
3.4 Discuss situation with specialist(s) as needed
3.5 Reassignment required ?
Yes
3.6 Reassign incident request
To Incident Management
No
3.7 Inform responsible specialist
To Incident Management

Overview of BMC Service Level Management calculations

From the Incident Request form, you can view incident service targets defined in BMC SLM. Service targets can be defined in BMC SLM for response time and resolution time. Service targets for an incident can be determined by related CIs, product and service categorization, and many additional criteria.

The service target response time applies when an incident request's reported source is one of the following choices:

- Email
- Fax
- Self Service
- Voice Mail
- Web
- BMC Impact Manager Event
- Other

In these cases, the Responded Date is blank until someone indicates that the incident has been responded to by updating the Response field on the Incident Request form to Yes. When support staff respond to an incident request from one of the previously noted sources, the Responded Date is set to the date that the incident was responded to.

The service target resolution time is configurable, a typical scenario would be from when the incident is recorded until it is resolved. The following scenarios can affect the calculated resolution time:

- When an incident is in a pending state, it might not be included in BMC SLM calculations if you select Client Hold for the status reason.
- When a resolved incident is reopened, the BMC SLM calculations account for time spent in the resolved state.

Handling incident escalations

If an incident request is escalated to the service owner, the service owner consults with the specialists who were handling the request to understand the request's current status and what solutions have been tried already.

If the service owner determines that the best way to restore service is through the continuity site, the service owner escalates the incident request to the on-duty manager to implement the continuity site strategy (see Reassigning incident requests for information about how to do this).

If activating a continuity site is not practical, the service owner determines whether service can be restored through the change management process. If possible, the service owner creates a change request (see Creating a change request for information about how to do this).

The resolution of an incident request is performed using the change management process when the resolution requires a change that will:

- Have a negative affect on the service during the service hours (defined by the SLA)
- Change the functionality of a service
- Require an update to the BMC Atrium CMDB

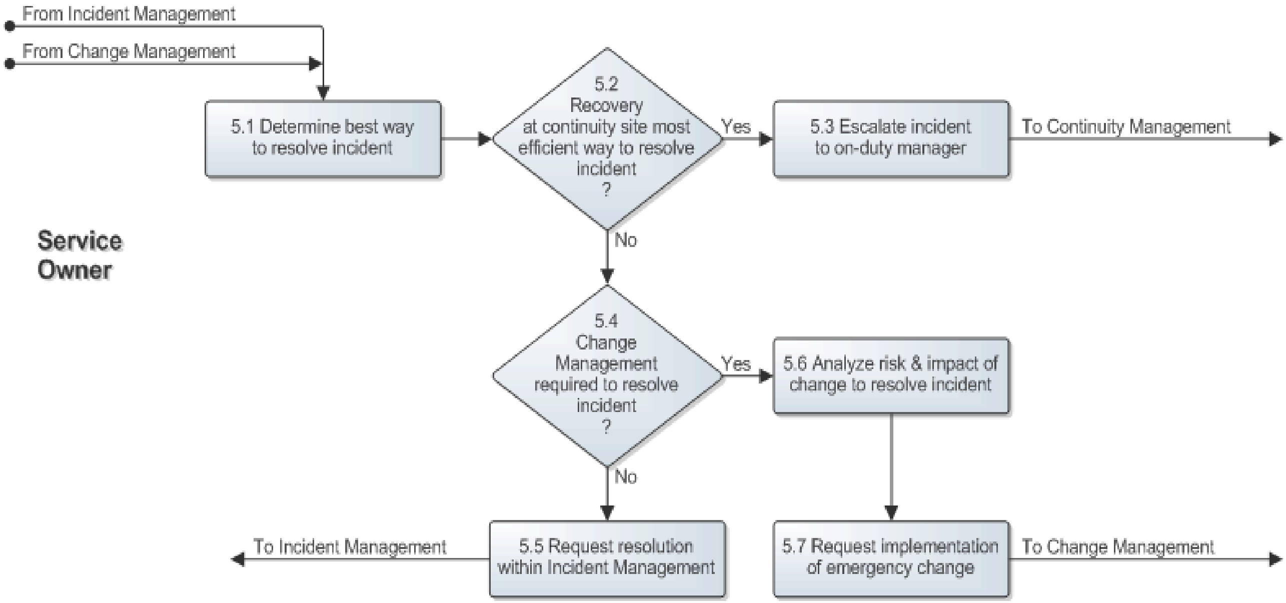
If the change management process is needed, the service owner also consults with the specialists assigned to the incident request to understand the risks that might cause the change implementation to fail, and what affect, if any, the change will have on the users. Through this consultation, they develop a strategy to minimize the affect of the change. When this is done, the service owner asks the specialist to implement the change as an emergency change.

If change management is not required, the service owner makes sure that the most appropriate specialists continue to resolve the incident within the incident management process.

> **Note**
> The role of service owner is performed by the on-duty manager when the service owner of the affected service is not available.

The following figure provides an overview of the escalation handling process as described by the BMC Service Management Process Model:

Escalation handling


From Incident Management
From Change Management
Service Owner
5.1 Determine best way to resolve incident
5.2 Recovery at continuity site most efficient way to resolve incident ?
Yes
5.3 Escalate incident to on-duty manager
To Continuity Management
No
5.4 Change Management required to resolve incident ?
Yes
5.6 Analyze risk & impact of change to resolve incident
No
To Incident Management
5.5 Request resolution within Incident Management
5.7 Request implementation of emergency change
To Change Management

Approving solutions

When the specialist proposes a solution, you must review the proposed solution to make sure the information is complete and accurate. You might need to contact the specialist for clarification or to better understand the proposed solution.

When you agree that the proposed solution is accurate and complete, and appropriate for the incident request, you approve the solution by changing the **Status** field on the Solution form from **Inactive** to **Active**.

If you do not agree that the proposed solution is appropriate for the incident request, you perform the following steps on the Solution form:

- Record the reason for disagreement in Work Info.
- Set the **Expiry Date** field to today's date.
- Leave the **Status** field reading **Inactive**.

To approve or reject a solution

1. Open the incident request record.
2. Click the **Relationship** tab.
3. From the Relationships table, select the solution database entry you are working on, and then click **View**.
4. To *approve* the solution, change the **Status** field from **Inactive** to **Active**.

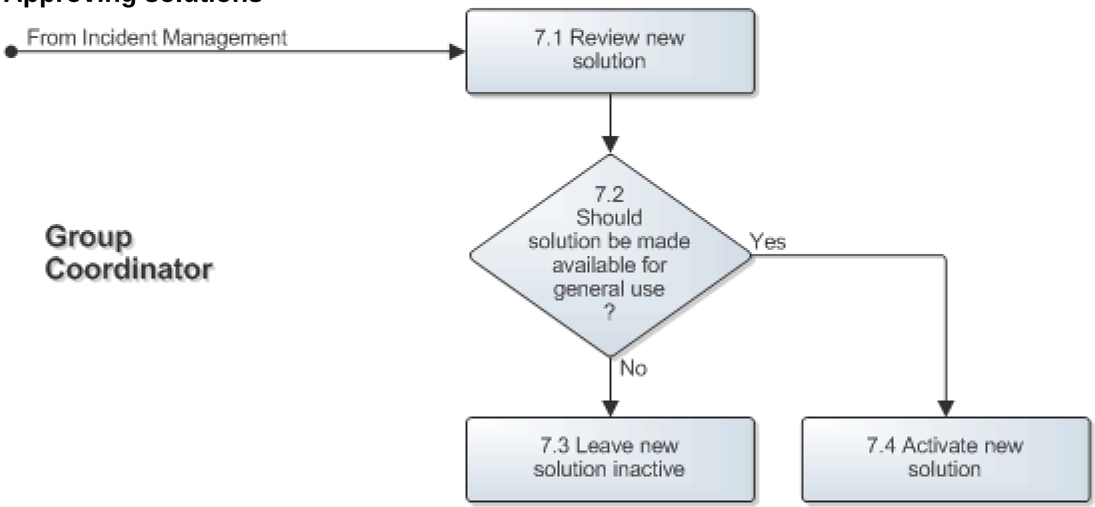
5. To *reject* the solution, perform the following steps:

- **# Leave the *Status** field at **Inactive**.
    1. On the Date/System tab, change the **Expiry Date** to today's date.
    2. Add a work information note to record the reason for disagreement.

1. Click **Save**.

The following figure provides an overview of the solution approval process as described by the BMC Service Management Process Model:

Approving solutions


From Incident Management
7.1 Review new solution
Group Coordinator
7.2 Should solution be made available for general use ?
Yes
No
7.3 Leave new solution inactive
7.4 Activate new solution

Viewing incident request records

When you want to view the an incident record in detail, double-click the incident request in the Incidents table.

Fields on the form display the incident status and other information that has been collected about the incident.

Reviewing the status of an incident request

If a customer calls to inquire about the status of a registered incident request, you can quickly review all of the customer's active records (that is, records that do not have a status of **Closed**) from the incident request form, using the following procedure.

To review the status of an incident request

1. From the Incident Management console, click **Create**.
2. In the **Customer** or **Contact** field on the new Incident Request form, type the customer's or the contact's information and then press **Enter**.
   The application updates the new incident request record with the customer's information.
3. In the Quick Actions area, click **Customer's Incidents**.
4. In the Customer's Incidents window, select the incident request you are reviewing the status for and click **View**.
   The Incident form opens in a Modify window.
5. When you finish reviewing the status, choose one of the following actions:
    - **Close** — Returns you to the Customer's Incidents window. Choose this if you need to review the status of another incident request record for the same customer.
    - **Close All** — Returns you to the Search form. Choose this when you finish reviewing the status of incident requests for the customer.

Managing service targets

If the BMC Service Level Management application is installed, the Incident Request form shows both overview and in-depth information about the incident in relation to the applicable service targets. You can view request-based service targets attached to incident requests. This enables you to see whether the service target has been met, missed, or is in a warning state.

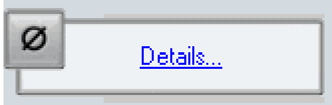
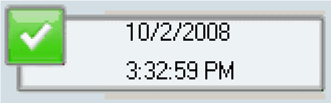
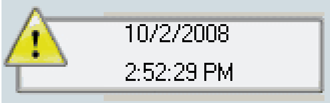
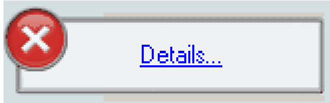
The following video presentation describes how to use service targets to prioritize incident requests.

> **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

View video on YouTube

To view service targets related to an incident request

1. From the Incident Management console, open the relevant incident request record.
2. View the **SLM Status** icon from the Navigation pane.
   The following table describes the **SLM Status** icon states:

Icon	Description
	**Status**: Not Attached No service target is attached to the incident.
10/2/2008 3:32:59 PM	**Status**: Attached Green: The service targets are in compliance.
10/2/2008 2:52:29 PM	**Status**: Warning Yellow: At least one service target is at risk.
	**Status**: Breached. Red: At least one service target did not meet its goal.

3. Click the icon to display the SLM:IntegrationDialog form to see in depth information about the incident in relation to the applicable service targets.
   The status gauge on the SLM:Integration Dialog form shows the current status of the selected service target. The following table explains the colors and fields on the status gauge:

Status gauge on the SLM:Integration Dialog form

Color or field	Description
Green	The service target is in compliance.
Yellow	The service target has a warning status.

Red	The service target has missed its goal.
Due Date and Time	The goal time within which either a response or a resolution for the incident must occur; otherwise the goal is missed.
Time Until Due	The amount of time left until the goal is considered missed.
Time Past Due	The amount of time that has passed since the goal was due.

The following table describes the information in the SLM:IntegrationDialog form.
Information about the SLM:IntegrationDialog form

Field	Description
Incident ID	The **ID** of the incident
Details	Click to see details about the selected service targets
Service Target table	
SVT Title	The name of the service target
Goal	The type of goal for the service target: Response-time goal — The incident request must be responded to within the time specified. Resolution-time goal — The incident request must be resolved within the time specified.
Hours/Min	The response or resolution time stipulated in the goal
Cost Per Min	The cost per minute for missing the response or resolution time goal
Due Date/Time	The goal time within which either a response or a resolution for the incident must occur; otherwise the goal is missed
Progress	The status of the service target: **Attached** — The service target has been attached to the incident. **Detached** — The service target has not been attached to the incident. **In Process** — Work on the request is taking place. **Pending** — Work on the request is stopped (for example, waiting for a part, or waiting for a response from the submitter). **Warning** — The service target is at risk. **Missed or Met** — The service target has either missed or met its goal. **Invalid** — The service target is disabled.
Milestones for SVT	
Title	The title of the milestone
Execution Time	The time that the milestone actions are executed
Status	The current status of the milestone. The status is either active or inactive (pending), or Action Performed.

For more information about service targets, see Working with service targets.

Managing problem investigations

These topics describe how to use the Problem Management feature to manage problem investigation through their lifecycle, as described by the BMC Service Management Process Model.

- Performing the incident request review
- Performing the root cause analysis
- Performing the analysis review
- Closing the problem investigation

Performing the incident request review

The information in this section is for people who fulfill the role of problem coordinator.

The tasks are organized according to the stages of the problem management lifecycle as described by the BMC Service Management Process Model. The following topics are included:

- Incident request review process
- Generating an incident request review
- Creating a problem investigation
- Assigning problem investigations

Incident request review process

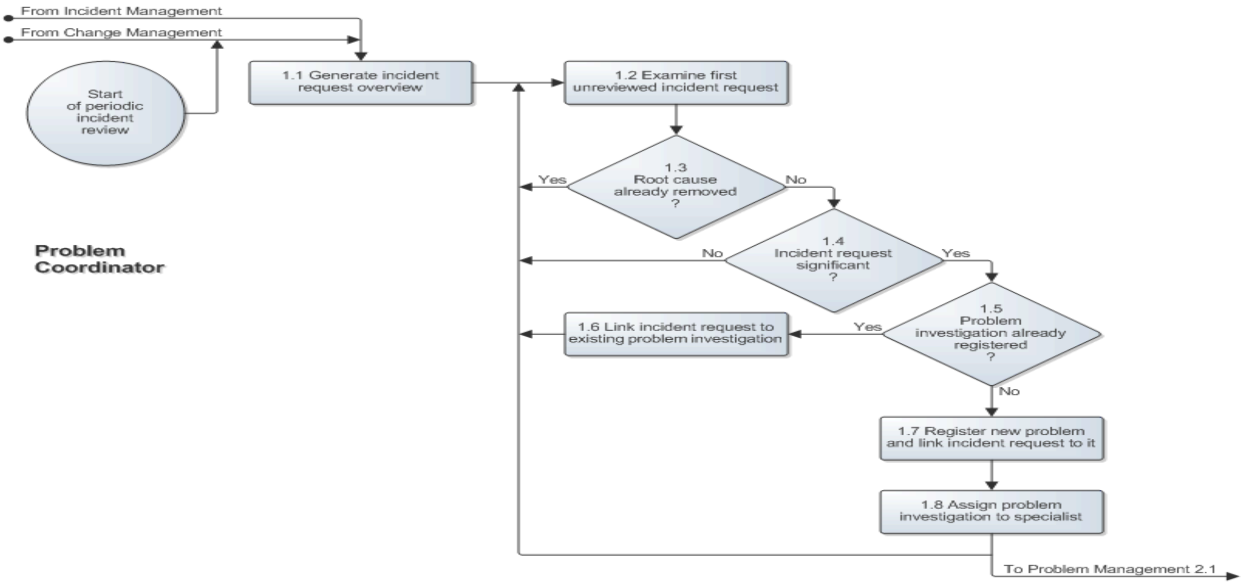
The incident request review is the first process in the problem management lifecycle. You perform incident request reviews periodically, according to your organization's schedule. When performing an incident request review, you analyze incident request information to identify potential problems in the services you are responsible for. This information is most often obtained from the Incident Management application. However, incident information can also come from specialists who have resolved incident requests with a workaround and who think the incident might recur if the root cause is not removed quickly.

After you identify a problem, create a new problem investigation. You link the problem investigation to the incident requests that were caused by the problem. You can also create a problem investigation from an incident request in the Incident Management application. See Creating a problem from an incident for information about how to do this.

✓ **Tip**
Creating a problem investigation from an incident request automatically creates a relationship between the incident request and the newly created problem.

You then assign the new problem investigation to a specialist for analysis. When assigning the problem investigation, choose a specialist whose skills, availability, and access rights make them the most appropriate person to perform the analysis.
If you find an incident request during the incident request review for which a problem investigation has already been registered, you should link the incident request to the problem investigation.

Incident request review


From Incident Management
From Change Management
Start of periodic incident review
1.1 Generate incident request overview
1.2 Examine first unreviewed incident request
1.3 Root cause already removed ?
Yes
No
1.4 Incident request significant ?
No
Yes
1.5 Problem investigation already registered ?
Yes
No
1.6 Link incident request to existing problem investigation
1.7 Register new problem and link incident request to it
1.8 Assign problem investigation to specialist
To Problem Management 2.1
Problem Coordinator

Generating an incident request review

The first step in the incident request review process is to generate an incident review overview. The overview helps you to identify problems that need to be investigated.

When generating the incident request overview, consider selecting all incident requests that have:

- Been linked to the service infrastructures, or business service records, for which you are the problem coordinator
- Their Impact field set to 2-Significant/Large or higher
- Been resolved in the past four months
- Not yet been linked to a problem investigation and were resolved with a workaround

If a specialist notifies you of a new problem, create an overview that includes the incident requests referred to by the specialist, and any similar incident requests.

After you generate an overview of unreviewed incident requests using the search criteria outlined in the preceding list, review the individual incident requests. When reviewing the incident requests, consider the following points when deciding whether the incident request should be linked to a problem investigation:

- Was the root cause of the incident request removed when the incident request was completed?
- Was the incident request significant? Consider an incident request significant when:
  - The service outage involved more than one person.
  - There were multiple occurrences.
  - You believe the incident might recur.
- Has the underlying problem already been identified? If it has, link the incident request to the problem.

In addition, consider whether analysis of your organization's capacity management or availability management systems indicates the potential for problems.If the incident request requires a new problem investigation, generate the problem investigation and link the incident request to it as described earlier in this section. After you create the problem investigation, assign it to a specialist. For information about how to do this, see Assigning problem investigations.

Creating a problem investigation

After you identify an incident request that indicates a problem, create a problem investigation.

Problem investigations should be created from the Incident Management application to ensure the information is copied from the incident request record to the problem investigation. See Creating a problem from an incident for information about creating problem investigations from Incident Management.

This section contains the following topics:

- Creating a problem from an incident
- Viewing problem investigations
- Recording additional investigation information

Creating a problem from an incident

If you fulfill the Problem Coordinator role, you can create a problem investigation from an incident request.

To create a problem investigation from an incident request

1. Open the incident request record.
2. Create the problem investigation.

When using Best Practice view	When using Classic view
a. From the **Quick Action** area, click the arrow beside **Create Related Request**. If you are working on a hub server in a Hub and Spoke environment, you are asked to identify the company you are creating the record for. Select the company from the drop down list, then click **Create**. The Problem Investigation form opens on the spoke server of the company you chose (where is will be saved, also). b. From the menu, select **Problem Investigation**.	From the Navigation pane, select **Create Other Requests > Create Problem**. If you are working on a hub server in a Hub and Spoke environment, you are asked to identify the company you are creating the record for. Select the company from the drop down list, then click **Create**. The Problem Investigation form opens on the spoke server of the company you chose (where is will be saved, also).

   The Problem form appears. The details are copied from the incident request to the Problem form and a relationship is created between the problem investigation and the incident request.

3. Complete the Problem form as described in Recording additional investigation information and in Indicating impacted areas.
4. Click **Save**.

Viewing problem investigations

This section describes how to open a problem investigation after it is created. You open problem investigations anytime you need to update the record.

To view problem investigations

1. On the **Problem Management** console, from the **Company** list, select the company for which you want to view problem investigations.
2. From the **View By** list, select one of the following filters:
   - Personal — Displays records assigned to you
   - Selected Groups — Prompts you to select any support groups to which you belong. You can select to display all records assigned to your group, or records assigned to your group that are not yet assigned to an individual.
   - All My Groups — Displays records assigned to all your support groups. You can choose to display all records, or records that are not yet assigned to an individual.
3. From the Defined Searches area, select **Problem Investigation** > **All Open Problems**.
4. To view additional details about an investigation, select the problem investigation record in the **Problems** table and then click **View**.
   The Problem Investigation form appears. You can modify the form and perform other actions, as appropriate.

Recording additional investigation information

You can use Problem Management to record additional information about the problem investigation after you create it.

For example, when using the Best Practice view, you might add or change the **Target Date** to indicate the estimated date for the problem investigation's resolution.

When using the Classic view, you might use additional classification information to determine whether to proceed with the investigation.

To record additional information (Best Practice view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Click the calendar icon beside the **Target Date** field.

   > ⚠ **Note**
   > The Target Date field is a required field when the problem investigation's status is not Draft.

3. Select the target resolution date and time.
4. Click **OK**, then click **Save**.

To record additional information (Classic view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Click the **Classification** tab.

3. Select an investigation driver.
4. In the **Investigation Justification** field, type the reason that you are requesting the problem investigation.
5. Enter the target resolution date.
6. Click **Save**.

Assigning problem investigations

An investigation can be assigned to an individual or a group.

- Viewing unassigned investigations
- Specifying a problem coordinator for the problem investigation
- Assigning an investigation to a specialist

⚠ **Note**
Known errors and solution entries can also be assigned by the same process.

Viewing unassigned investigations

A problem investigation might be assigned to your support group without being assigned to an individual.

View the unassigned problem investigations, then assign them as described in Specifying a problem coordinator for the problem investigation.

To view unassigned problem investigations

1. From the **Defined Searches** list on the **Problem Management** console, run **Defined Searches > Problem Investigation > All Open Problems**.
   For more information about running predefined searches, see Managing custom searches.
2. View the unassigned problem investigations in the **Problems** table.

Specifying a problem coordinator for the problem investigation

Problem coordinators are individuals who have the functional role of Problem Coordinator within the support group to which they belong.

To specify a problem coordinator (Best Practice view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. From the **Coordinator Group** menu, select the client company, organization, and support group that will coordinate the problem investigation.
   After you specify the client company, organization, and support group, only the support group name appears in the **Coordinator Group** field.
3. From the **Problem Coordinator** menu, select the name of the person you want to assign as the problem coordinator.

4. Click **Save**.

To specify a problem coordinator (Classic view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Click the **Assignment** tab.
3. In the **Problem Coordinator Assignment** area, select the problem coordinator from the **Assignee** field.
   - If you look at the **Set Assignment Using** menu and see that problem coordinator groups have been defined there, select the **Pblm Mgr Default Group** from the **Set Assignment Using** list, and then click **Set**. Then, select the problem coordinator from the **Assignee** field.
   - To assign yourself as the problem coordinator, click **My Default Group**.
4. Click **Save**.

Assigning an investigation to a specialist

You can assign the investigation to any specialist belonging to a support group.

For information about how to reassign the investigation to another support group or to an assignee in another support group, see Reassigning the problem investigation.

To assign an investigation to a specialist

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Indicate the appropriate assignee, as shown in the tables that follow:
   - To assign the investigation to yourself

When using the Best Practice view	When using the Classic view
In the Navigation pane, choose **Quick Actions > Assign to Me**.	In the Navigation pane, choose **Quick Links > Assign to Me**.

   - To assign the investigation based on predefined routing

When using the Best Practice view	When using the Classic view
In the Navigation pane, choose **Quick Actions > Auto Assign**.	In the Navigation pane, choose **Functions > Auto Assign**.

   - To assign the investigation to a specific person

When using the Best Practice view	When using the Classic view
a. Click the **Work Detail** tab. b. From the Assigned Group menu, select the support group. c. From the Assignee menu, select the name of the person you want to assign as the assignee.	a. Click the **Assignment** tab. b. In the Problem Assignment area, select the appropriate assignee.

3. Change the status to **Assigned**.
4. Click **Save**.

Performing the root cause analysis

The information in this section is for people who fulfill the support role of specialist.

The tasks described by this section are organized according to the stages of the problem management lifecycle as described by the BMC Service Management Process Model.

- Root cause analysis
- Reviewing and updating the problem investigation
- Proposing a temporary workaround
- Establishing the root cause
- Recording the root cause
- Proposing a structural solution
- Implementing the solution
- Notifying the problem coordinator

Root cause analysis

After a problem investigation is assigned to you for investigation, you perform a root cause analysis to determine the problem's cause.

If the problem has caused one or more incidents, you first try to find a temporary workaround to restore normal service operation as quickly as possible. If a temporary workaround is available, update the problem investigation record with details about the workaround, including how to implement it. This information can be used later to resolve other incidents caused by the same or similar problems until a structural solution is found and implemented.

After assessing temporary workarounds, begin to investigate the root cause of the problem. After finding the root cause, you update the problem investigation with a description of the root cause.

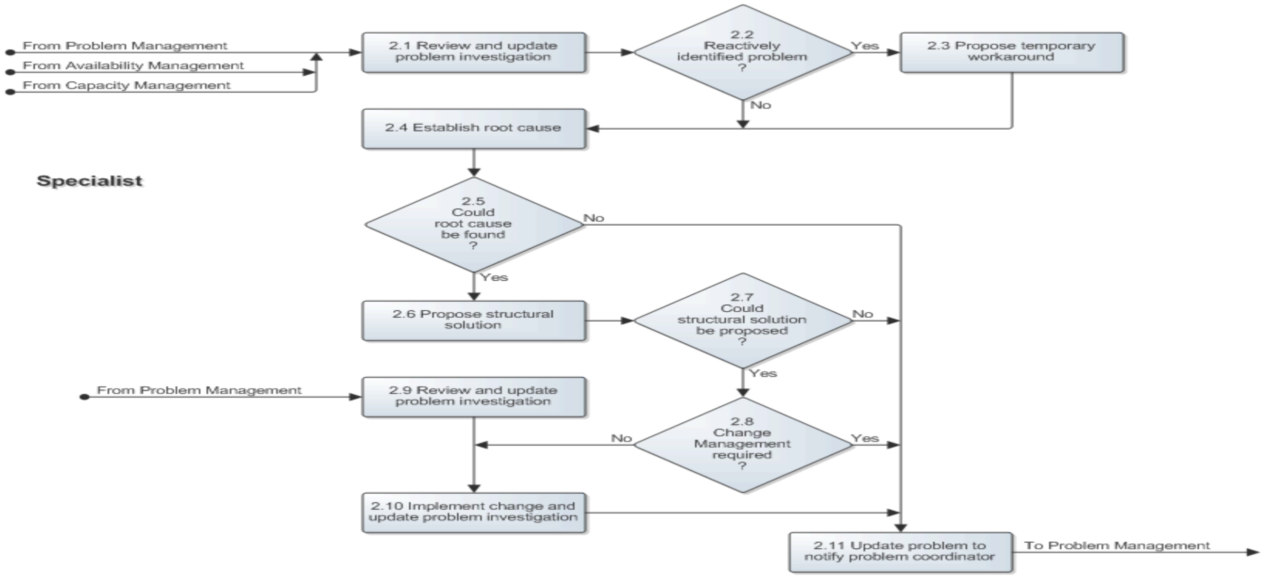
After determining what is causing the problem, you investigate possible structural solutions. Ensure you add a description of each option to the problem investigation along with a recommendation for the preferred solution.

If you can perform a structural solution, implement the solution and then update the problem investigation with the solution. If the change management process is needed to permanently work around or solve the root cause, ensure you inform the problem coordinator that change management must be involved with the analysis.

If you cannot determine the problem's root cause or cannot propose a structural solution, then record this in the problem investigation along with an explanation.

When you finish the root cause analysis, regardless of the outcome, you must inform the problem coordinator that your work is completed.

Root cause analysis


From Problem Management
From Availability Management
From Capacity Management
2.1 Review and update problem investigation
2.2 Reactively identified problem ?
Yes
2.3 Propose temporary workaround
No
2.4 Establish root cause
Specialist
2.5 Could root cause be found ?
No
Yes
2.6 Propose structural solution
2.7 Could structural solution be proposed ?
No
Yes
From Problem Management
2.9 Review and update problem investigation
2.8 Change Management required ?
No
Yes
2.10 Implement change and update problem investigation
2.11 Update problem to notify problem coordinator
To Problem Management

Reviewing and updating the problem investigation

When you are notified that a problem investigation is assigned to you and you are ready to start the root cause analysis, open the problem investigation record. Check that the status of the problem investigation is Assigned, and then set the status to Under Investigation.

> **Note**
> The problem investigation status must be Assigned before you can change the status to Under Investigation. If the problem investigation status is not Assigned, contact the problem coordinator to have the status changed.

Fields on the record display information that was collected about the problem or the status of the problem investigation.

Review the information included in the problem investigation and any related records, to gain a clearer understanding of the problem's, background, and how it is affecting the service infrastructures associated with it.

> **Note**
> If you receive an investigation that you think someone else is better suited to review, you can reassign it to that person. For information about how to do this, see Reassigning the problem investigation.

The tasks described by the following procedures are related to reviewing and updating the problem investigation:

- Receiving notification of assignments
- Viewing problem investigations assigned to you
- Accepting a problem investigation assignment
- Searching for similar problem investigations
- Searching knowledge base entries
- Authoring knowledge base entries with problem investigation results
- Documenting work with a vendor

Receiving notification of assignments

The Problem Management console displays all problem investigations, known errors, and solution entries assigned to you.

Depending on how your system is configured, you might receive an email notification that a problem investigation has been assigned to you.

Viewing problem investigations assigned to you

You can view the summary and detail of problem investigations assigned to you.

As a problem assignee, you assume responsibility for the problem investigation. You become the focal point for communication about the problem. You are responsible for coordinating activity to investigate the problem.
You can record the effort that you have spent working on an investigation. If you are not assigned to an investigation, you can record that you have assisted with the investigation.

> ⚠ **Note**
> If you do not accept the assignment, reassign the investigation, as described in Reassigning the problem investigation.

To view problem investigations assigned to you

1. On the **Problem Management** console, from the **View By** list, select **Personal**.

   > ⚠ **Note**
   > You can also view problem investigations assigned to other people in the support groups you belong to by selecting either **Selected Groups** , which enables you to select a subset of your groups, or **All My Groups** , which displays problem investigations for all the support groups you belong to.

2. From the **Defined Searches** area, select **Problem Investigation > All Open Problems**.
3. To view additional details about an investigation, select the problem investigation record in the **Problems** table and then click **View.**
   The Problem Investigation form appears. You can modify the form and perform other actions, as appropriate.

Accepting a problem investigation assignment

This topic describes how you can accept any problem investigation that is assigned to your support group.

To accept an assignment

1. Open the relevant problem investigation by selecting it from the **Problems** table and clicking **View**.
2. In the **Navigation** pane, perform one of the following actions:
   - *(Best Practice view)* Choose **Quick Actions > Assign to Me.**
   - *(Classic view)* Choose **Quick Links > Assign to Me.**

     If you belong to more than one support group, you are prompted to select the group you want the problem investigation assigned to.

3. Select the support group.
4. From the **Status** field, select **Under Investigation**.
5. Click **Save**.

Searching for similar problem investigations

After accepting a problem investigation assignment, if you remember having worked on a similar problem investigation, you can use the Advanced Search feature to find it. Viewing similar problem investigations might help you find the root cause of your current problem investigation.

> ✓ **Tip**
> If you have access to BMC Knowledge Management, you can also use that application to help you find information to help with the problem investigation. For information about using BMC Knowledge Management, see the BMC Knowledge Management documentation.

The following procedure helps you to find problem investigations that are already related to other records.

To search for similar problem investigations

1. From the Navigation pane on the Problem Management console, choose Functions > Advanced Search.
2. In the **Advanced Search Selection** dialog box, select the type of search you want to perform, then click **Select:**
   - **Search Problem Investigation by Work Info** — Searches for problem investigation using fields from the Work Detail tab (Work Info tab when using the Classic view)
   - **Search Problem Investigation by Relationships** — Searches for problem investigations using fields from the Relationship form
3. On the search form, provide as much information about the previous problem investigation as possible, and then click **Search**.
4. View the matching problem investigations in the table that appears.

Searching knowledge base entries

If you have access to the BMC Knowledge Management application, you can use information in the knowledge base to help perform tasks such as the root cause analysis.

Knowledge can be captured and structured for reuse in a knowledge base. BMC Knowledge Management provides a single, centralized, self-service knowledge base for creating, organizing, categorizing, using, updating, and managing structured, consolidated knowledge. For more information about knowledge bases, see A word about knowledge.

To search the knowledge base

1. With the problem investigation or known error record open, from the **Navigation** pane, choose **Quick Actions (Quick Links in the Classic view) > Search Knowledge Base**.
2. With the problem investigation or known error record open, from the **Navigation** pane, choose **Functions (Quick Links in the Classic view) > Search Knowledge Base**

3. Complete the Knowledge Management search form that appears. For detailed information about how to search for knowledge, see Searching for knowledge.

Authoring knowledge base entries with problem investigation results

When you finish the problem investigation, if you think that publishing the solution in the knowledge base can help future root cause analyses, you can do this from the problem investigation record.

To author a knowledge base entry

1. With the problem investigation record open, do one of the following:
   - **Classic view**: From the Navigation pane, select **Quick Links** > **Create Knowledge**
   - **Best Practice view**: From the Functions area of the Navigation pane, select **Create Knowledge**
2. Complete the Knowledge Management authoring form that appears. For detailed information about how to complete the form, see Creating and editing knowledge articles.

Documenting work with a vendor

Use one of the following procedures to track investigations that require vendor support, and to indicate when you assign an investigation to a vendor.

> ⚠ **Note**
> If you assign an investigation to a vendor, you must communicate with the vendor as appropriate. Problem Management does not notify the vendor.

To document work with a vendor (Best Practice view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. In the **Vendor** field, indicate the vendor's name.
   - If the vendor is already defined, select the vendor.
   - If the vendor is not listed on the menu, type the vendor's name.
3. If available, enter the Vendor Ticket Number.
   The Vendor Ticket Number is a tracking number issued by the vendor's tracking system for the problem investigation that you are assigning to that vendor.
4. Click **Save**.

To document work with a vendor (Classic view)

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Click the **Assignment** tab.
3. For Assign to Vendor, select **Yes**.
4. Click the **Vendor** tab.

5. Complete the Vendor Information tab, as appropriate.
   - If the vendor is already defined, you can select the vendor.
   - If the vendor is not listed on the menus, you can type the vendor contact information.

> ⚠ **Note**
> The **Internet Email** field is *only* informational. From this field, you can see who is currently working on the problem investigation and how to contact the vendor for an update.

6. Indicate the date that you assigned the investigation to the vendor.
7. Click **Save**.

Proposing a temporary workaround

Problem investigations can be created proactively or reactively. A proactive problem investigation comes from your capacity management system and is created to avoid incidents caused by capacity shortages. Reactive problem investigations are related to one or more incident requests.

If the problem investigation was created by the capacity management system, you can skip this step and go to Establishing the root cause. If the problem investigation is related to one or more incident requests, try to find a workaround to resolve the incidents. You might find useful information about the Resolution tab of the related incident request record. See Viewing incident request records for information about viewing incident request records. If you identify a workaround, carefully describe it in the Workaround field of the problem investigation record. Until a permanent solution is found, this information can be useful to service desk analysts and other specialists working on similar cases.

> ⚠ **Note**
> It is possible that a workaround from a previous analysis is already described in the **Workaround** field. If this is the case, review the workaround and update the description if necessary.

If you cannot find a practical workaround for the problem, make sure that you record this in a work information note on the **Work Detail** tab (**Work Info** tab when using the Classic view).

To record a workaround

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Enter the workaround information:
   - *(Best Practice view)* In the **Workaround** field, type a description of the workaround.
   - *(Classic view)*
     a. In the **Process Flow Status** area, click the **Investigation and Diagnosis** box, and choose **Generate Work Around/Root Cause**.
     b. In the **Problem Investigation Workaround** dialog box, type information in the **Workaround** field.
3. Click **Save**.

Establishing the root cause

When performing a root cause analysis, you try to establish the problem's root cause. Even if the problem investigation was triggered proactively by your organization's capacity management system, you must determine why the service infrastructure is running out of capacity.

After you determine the root cause, take the following steps:

- Record the root cause on the problem investigation form.
- If the root cause resides within a CI, relate the CI to the problem investigation. For information about how to do this, see Relating incident requests and problem investigations.
- Look at the Workaround field to review any previously proposed workarounds. With the root cause now known, if necessary, propose a better workaround and describe how to implement it. For information about how to do this, see Proposing a temporary workaround.

If you cannot determine the root cause, you must record this also in a work information note on the **Work Detail** tab (**Work Info** tab when using the Classic view). Ensure that you record why a root cause cannot be found, and be sure to record the activities that you performed to determine that a root cause cannot be determined.

⚠ **Note**
If the root cause analysis is temporarily unable to progress (for example, if you are waiting for information from a supplier), make sure you set the problem investigation's Status field to Pending, and then specify why in a work information note on the Work Detail tab (Work Info tab when using the Classic view). See Creating work information entries from the console for information about how to do this.

Related topic

Recording the root cause

Recording the root cause

This topic describes how to record the root cause. After you record the root cause, the problem investigation can be completed as a solution entry or a known error, as described in Creating a solution entry and Creating a known error .

To record the root cause

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Record the root cause:

When using the Best Practice view	When using the Classic view
Add a Work Detail note describing the root cause. **Note:** For information about how to do this, see Creating work information entries from the console	a. In the **Process Flow Status** area, in the **Investigation and Diagnosis** box, choose **Generate Work Around/Root Cause**. b. In the **Problem Investigation Workaround** dialog box, select the root cause. **Note:** The Root Cause options available for the selection depend on the product and operational categorizations. c. Click **Save**.

3. If a recent change is the root cause, and if BMC Change Management is installed on your system, relate the investigation to the change request with a Request Type of **Infrastructure Change**.
   For information about how to relate records, see Relating incident requests and problem investigations.
4. If a known error is the root cause, relate the investigation to the known error with a Request Type of **Known Error**.
   For information about how to relate records, see Relating incident requests and problem investigations.

Proposing a structural solution

After you determine the problem's root cause, if possible, determine the best way to permanently fix it. For example, if the problem is related to a CI that is still under warranty, contact the supplier for a replacement CI.

In a work information note on the Work Detail tab (Work Info tab when using the Classic view), describe the proposed structural solution. If there are multiple possible solutions, make sure you record all them.

After determining the best solution, based on technical, financial, and availability considerations, use a work information note to record the preferred solution, providing details about how to implement it.

If a service infrastructure change is required to resolve the problem, recommend that the problem coordinator create a known error to coordinate the change through the Change Management process. The Change Management process is required when:

- Services become unavailable or is degraded during service hours
- The functionality of a service changes
- The BMC Atrium CMDB requires an update

If you cannot find or implement a practical solution, make sure that you use a work information note to record the reasons why a solution is not currently available.

Implementing the solution

If you determine that a structural solution to the problem is available, or if you have found a permanent workaround, implement it. After you implement the solution or permanent workaround, record how the solution or permanent workaround was implemented using a work information note on the **Work Detail** tab (**Work Info** tab when using the Classic view).

- Resolving a problem investigation
- Creating a solution entry

Resolving a problem investigation

After you implement the solution, resolve the problem investigation. The end result of the investigation might be a known error record or solution record.

To resolve a problem investigation

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Change the **Status** to **Completed**.

> ⚠ **Note**
> If an infrastructure change is required to permanently resolve the problem, then select **Known Error** from the **Status Reason** list in the next step.

3. Select the appropriate status reason.
   If you select **Known Error** or **Solution Database**, the details of the problem investigation are copied to a new known error or solution database entry when you save your changes.
4. Open the **Categorization** tab (in Best Practice view) or the **Classification** tab (in Classic view) and select the appropriate product categorization.
5. Click **Save** to save your changes.
   The status of the investigation is set to **Completed**.
   - If the status reason for the investigation is Known Error, the Known Error form appears, and details from the problem investigation are copied into the form. Complete the form and save it, as described in Creating a known error.

     > ⚠ **Note**
     > If an infrastructure change is required to permanently resolve the problem, then in the Known Error form, assign the known error to the Change Coordinator to have the change implemented.

   - If the status reason for the investigation is Solution Database, the Solution Database form appears, and details from the problem investigation are copied into the form. Complete the form and save it, as described in Creating a solution entry.

     > ⚠ **Note**
     > If the problem investigation is related to an incident that is not yet closed or canceled, the incident assignee is notified that the investigation is complete.

Creating a solution entry

After you determine the root cause of a problem, you can create a solution entry. Typically, you might create a solution entry if you determine that the issue against the investigated CI is not a defect (that is, the CI is functioning as designed). In this scenario, a change request does not have to be issued for correcting the CI in question.

To create a solution entry

1. With the Solution Database form open, as described in Resolving a problem investigation, complete the Solution Database entry as appropriate. A description of the various required fields is provided in the following table:

Field	Explanation
Summary	A brief summary of the solution
View Access	Select one of the following choices: **Internal** — Users within your organization can see the entry **Public** — Everyone with access to Problem Management can see the entry, including users of the Requester console

Details tab	
Abstract	A brief description of the root cause and the solution
Solution	A detailed description of the solution
Assignment tab	
Support Company	The support company to which the problem investigation was assigned
Support Organization	The support organization to which the problem investigation was assigned
Assigned Group	The support group to which the problem investigation was assigned
Mappings tab	
Organization — Company	Select the client company from the menu. If the solution applies to all client companies, select **Global**.
Location — Company	Select the client company from the menu. If the solution applies to all client companies, select **Global**.
Date/System tab	
Submitter	Record the name of the person creating the Solution Database entry

2. Click **Save**.

Notifying the problem coordinator

When you finish the root cause analysis and have recommended a structural solution (and perhaps implemented the structural solution) use the Problem Investigation form to notify the problem coordinator that the problem has been solved.

To notify the problem coordinator

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Set the **Assignee** field to the name of the problem coordinator:
    - *(Best Practice view)* Ensure that the **Assignee** field is set to the name of the problem coordinator.
    - *(Classic view)* On the **Assignment** tab, ensure that the **Problem Coordinator Assignment-Assignee** field is set to the name of the problem coordinator.
3. From the **Status** field menu, select **Assigned**.

Performing the analysis review

The information in this topic is for people who fulfill the management role of problem coordinator.

The tasks described by this section are organized according to the stages of the problem management lifecycle as described by the BMC Service Management Process Model.

- Analysis review
- Reviewing the problem investigation
- Reassigning the problem investigation
- Creating a known error

- Reviewing known error details
- Monitoring a problem's status
- Canceling a problem investigation

Analysis review

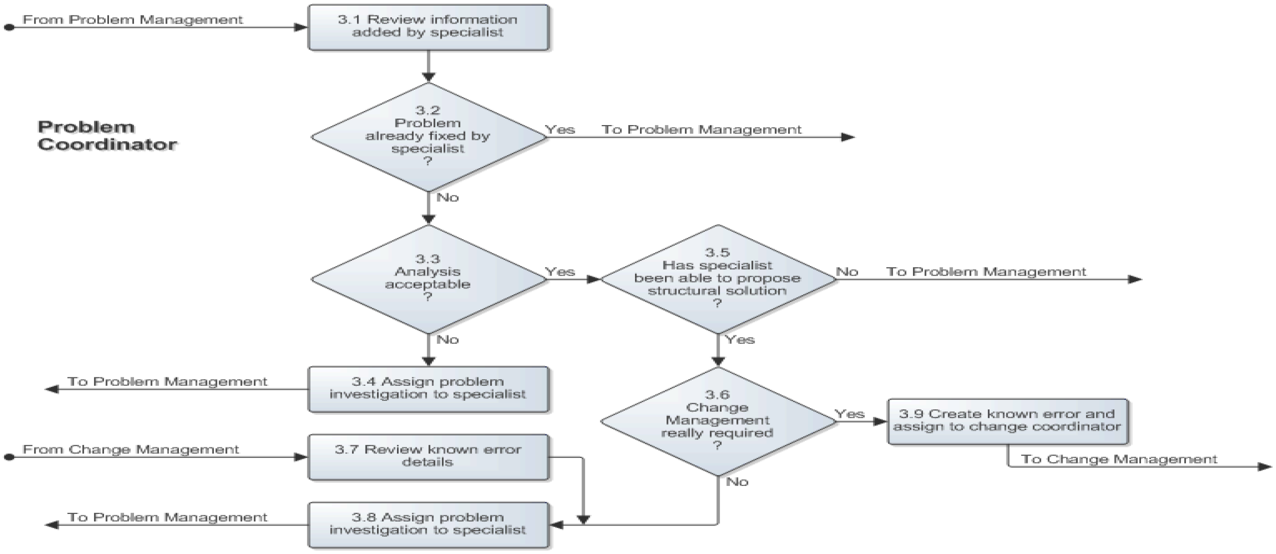
After the specialist completes a root cause analysis of the assigned problem investigation, you review the analysis.

If during the analysis review you determine that the specialist implemented a solution to the problem, you can start to close the problem investigation. For information about how to do this, see Closing the problem investigation.

You can close the investigation *without* a solution if you determine that the specialist thoroughly analyzed the problem, but was unable to find a root cause. If you determine the analysis was not adequate, then assign the problem investigation back the specialist for further analysis, or reassign it to another specialist. For information about how to do this, see Reassigning the problem investigation.

If the specialist proposes a structural solution that requires change management, review the proposal to determine if this is an appropriate course of action. If you agree that a change is required to solve the problem, generate a known error and passes it to the Change Coordinator of the affected service. If you do not agree that a change is required, assign the problem investigation back the specialist for further analysis, or reassign it to another specialist.

Analysis review


From Problem Management
3.1 Review information added by specialist
Problem Coordinator
3.2 Problem already fixed by specialist ?
Yes
To Problem Management
No
3.3 Analysis acceptable ?
Yes
3.5 Has specialist been able to propose structural solution ?
No
To Problem Management
No
Yes
To Problem Management
3.4 Assign problem investigation to specialist
3.6 Change Management really required ?
Yes
3.9 Create known error and assign to change coordinator
To Change Management
From Change Management
3.7 Review known error details
No
To Problem Management
3.8 Assign problem investigation to specialist

Reviewing the problem investigation

When specialists complete their root cause analysis, they assign the problem investigation to a problem coordinator to perform an analysis review.

As the assigned problem coordinator, you open the problem investigation and review the Work Detail tab entries (Work Info tab when using the Classic view).

During the review, determine whether the specialist:

- Implemented a structural change
- Recommended that a service infrastructure undergoes a change
- Was unable to find a root cause

When a structural change was implemented

If the specialist implemented a change and if your review determines the root cause analysis was satisfactory, close the problem investigation.

For information about how to start this process, see Closing the problem investigation.

If you determine the root cause analysis was not satisfactory, reassign the problem investigation back to the specialist, or to another specialist for further investigation. For information about how to do this, see Reassigning the problem investigation.

When Change Management is needed

If the specialist recommends an infrastructure change that requires the involvement of Change Management, determine independently whether the proposed change is justified. This can save time in resolving the problem if Change Management is not really needed.

Change Management must be involved when:

- Services become unavailable or are degraded during service hours
- Functionality of a service changes
- BMC Atrium Configuration Management Database (BMC Atrium CMDB) requires an update

If you agree that Change Management is needed, create a known error and assign it to the Change Coordinator. For information about how to do this, see Creating a known error.

Otherwise, reassign the problem investigation back to the specialist, or to another specialist for further investigation. For information about how to do this, see Reassigning the problem investigation.

When no root cause was found

If the specialist cannot find a root cause, make sure that the reason is recorded in a work information note on the Work Detail tab (Work Info tab when using the Classic view). Make sure, too, that the status of the problem investigation is set to Pending.

If you determine that the analysis was not adequate, reassign the problem investigation back to the specialist, or to another specialist for further investigation

Reassigning the problem investigation

If you determine the problem investigation was not adequate, disagree with the need for Change Management, or if Change Management rejects the known error, you reassign the problem investigation for further analysis.

You begin the reassignment process by explaining, using a work information note on the Work Detail tab (Work Info tab when using the Classic view), why the investigation is being reassigned. You then decide which specialist can perform a better analysis based on skill level, availability, and access rights. After determining the most appropriate specialist, reassign the problem investigation. You can assign the investigation to either the original specialist or to another specialist.

You can reassign an investigation to either an individual or a support group. Use the quick actions in the Navigation pane to reassign an investigation to yourself (Assign to Me) or to reassign an investigation based on automatic routing (Auto Assign).

To reassign an investigation

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. To assign the investigation to yourself, in the Navigation pane, choose one of the following actions:
    - **Quick Actions (Quick Links in the Classic view) > Assign to Me**
    - **Quick Actions (Quick Links in the Classic view) > Auto Assign**
      Auto Assign uses the automatic routing to assign the investigation based on predefined system mapping. Automated assignment can be based on the problem location, operational categorization, or product categorization.
3. To reassign the investigation to someone else, perform the following actions:
    - *(Best Practice view)*
        a. Select a new assignee from the **Assignee** list.
        b. To change the Assigned Group, select a new assigned group from the **Assigned Group** list
        c. Select a new assignee from the **Assignee** list.
    - *(Classic view)*
        a. Click the **Assignment** tab.
        b. Reassign the investigation with one of the following options:
            - Select the assigned group
            - After selecting an assigned group, select the assignee.
            - Select from **Set Assignment**.

              The following table describes the **Set Assignment** selections for the **Problem Assignee** area of the **Assignment** tab:

Set assignment using	Description
My Default Group	Assigns the investigation to you and your default support group.
My Group List	Opens a list of all groups to which you belong. Select the appropriate group from this list.
Favorite Groups	Lists the typical groups to which your support group assigns investigations.
Auto Assign	The same as the Auto Assign link in the Navigation pane, this assigns the investigation based on predefined system mapping.

4. Click **Save**.

Creating a known error

If you agree with the specialist's recommendation that a change is the best way to remove the root cause of the problem, initiate the change by creating a known error and assigning it to the change coordinator of the affected service.

To create a known error

1. Open the relevant problem investigation as described in Viewing problem investigations.

2. Set the **Status** field to **Completed** and the **Status Reason** field to **Known Error**.
3. Click **Save**.
4. When prompted by the system, click **Yes**.
   The Known Error form opens and a relationship is created between the known error and the problem investigation.
5. In the **Notes** field, enter a brief description of the known error and a detailed description of the change requirements.
6. Select the impact and urgency. The priority and weight are calculated based on the impact and urgency. If required, you can adjust the weight.
7. Select whether view access is internal or public.
   This field is for informational purposes to indicate whether the known error is for internal or public consumption.
8. Select the client company:
   - *(Best Practice view)* From the **Known Error Location** list, select the client company.
   - *(Classic view)* In the Known Error Details area of the **Classification** tab, select the company.
9. From the **Categorization** tab (Best Practice view) or the **Classification tab** (Classic view), select the operational and product categorizations.
   Operational categorization is based on a three-tier hierarchy that is defined in the Operational Catalog.
10. Ensure that the assignments are correct:

When using the Best Practice view	When using the Classic view
a. Ensure that your support group appears in the **Coordinator Group** field. b. Ensure that your name appears in the **Problem Coordinator** field. c. Ensure that the Change Coordinator's support group name appears in the Assigned Group field. d. Ensure that the Change Coordinator's name appears in the Assignee field.	a. Click the **Assignment** tab. b. Ensure that your name appears in the **Assignee** field in the **Problem Coordinator Assignment** area (Your name appears in this field, because you are the problem coordinator) c. Ensure that the Change Coordinator's name appears in the **Assignee** field in the **Known Error Assignment** area.

11. Ensure that the known error is related to all the affected service infrastructure and to the CI in which the problem resides. For information about how to do this, see Defining relationships.
12. Ensure that the **Status** is set to **Assigned**.
13. Click **Save**.

Reviewing known error details

If you submit a known error to change management, the Change Coordinator has the option to reassign the known error back to you if the Change Coordinator determines that the solution can be implemented within the problem management process.

If this happens, review the known error to determine why the Change Coordinator reassigned it, and then assign the problem investigation to the appropriate specialist. For information about how to do this, see Reassigning the problem investigation.

To review a known error

1. From the **Defined Searches** area of the **Navigation** pane on the **Problem Management** console, choose **Known Error > All Open Known Errors**.
2. Click **Refresh**.
   The **Known Errors** list refreshes with all open known errors for the selected **Company** and **View By** fields.
3. Select the known error and click **View**.
4. On the Known Error form, review the details as necessary.

Monitoring a problem's status

The Process Flow Status area on the Problem Investigation form indicates the current stage and state of an investigation. When using the Classic view, the effort tracking feature records the history of assigned work that has been performed on the investigation.

The Process Flow Status area provides a quick visual indicator of the current stage and state of an investigation. When you open an investigation, the Process Flow Status area appears toward the top of the form.

For additional information about the process flow lifecycle, see Process flow and the lifecycle of a problem investigation.

In the Classic view, the investigation effort log attached to the Problem Investigation form lists all individuals who have worked on the problem during its lifecycle. This information is not system-generated; staff record this manually, as described in Recording effort spent on an investigation.

Canceling a problem investigation

If an investigation is not justified or is a duplicate of a current investigation, you might want to cancel it.

To cancel a problem investigation

1. Open the problem investigation.
2. Update the form, as appropriate.
3. Select **Canceled** in the **Status** field.
4. Select a status reason from the **Status Reason** list.
5. Click **Save**.

Closing the problem investigation

The information in this topic is for people who fulfill the role of problem coordinator.

The tasks described by this section are organized according to the stages of the problem management lifecycle as described by the BMC Service Management Process Model.

- Verifying the structural solution
- Closing the problem investigation and known errors
- Indicating an impasse

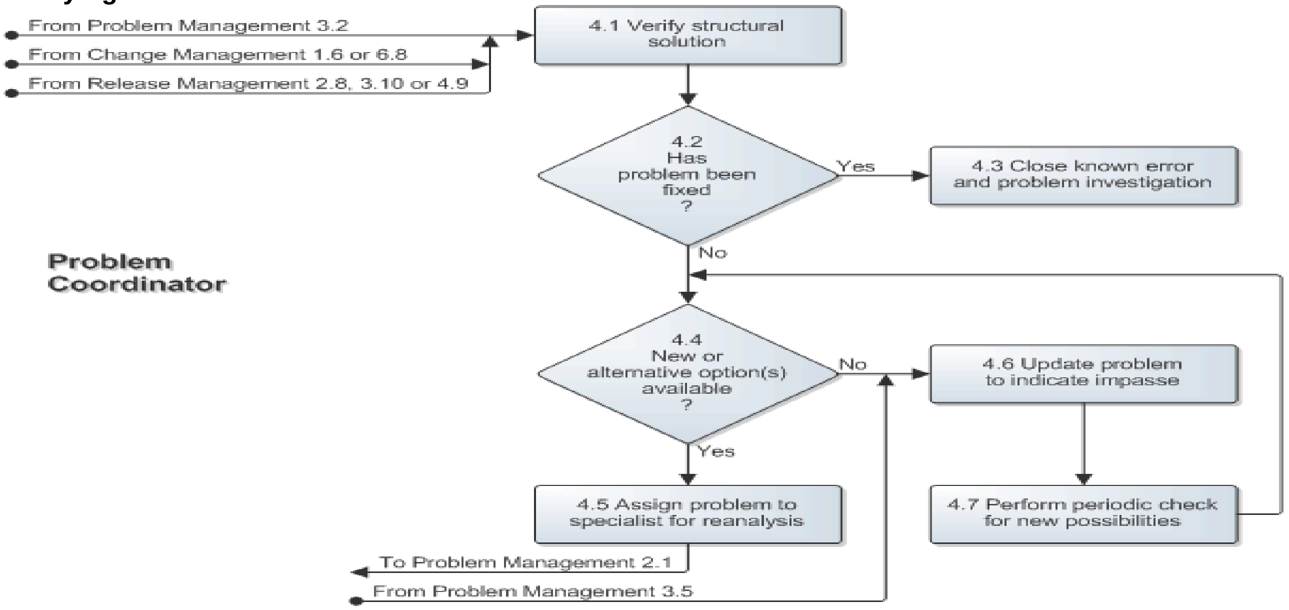
- Performing periodic checks

Verifying the structural solution

When you are notified that a problem is resolved, open the problem investigation and any related known errors to review the information about the respective Work Detail tabs (Work Info tabs when using the Classic View).

You do this to determine which structural solution was implemented to resolve the problem. After determining the nature of the structural solution, you must verify that the solution has solved the problem. One way to do this is to review the production test results. In cases where incidents caused by the problem under investigation exhibited only intermittent symptoms, the only way to verify the solution might be to monitor incident requests against the affected service, to see if any new incidents are being reported.

Verifying the structural solution


From Problem Management 3.2
From Change Management 1.6 or 6.8
From Release Management 2.8, 3.10 or 4.9
4.1 Verify structural solution
4.2 Has problem been fixed ?
Yes
4.3 Close known error and problem investigation
No
Problem Coordinator
4.4 New or alternative option(s) available ?
No
4.6 Update problem to indicate impasse
Yes
4.5 Assign problem to specialist for reanalysis
4.7 Perform periodic check for new possibilities
To Problem Management 2.1
From Problem Management 3.5

Closing the problem investigation and known errors

After verifying that the structural solution resolved the problem (a process that can take days or even weeks of monitoring), close the problem investigation and any related known errors.

This topic contains the following procedures:

- To close a problem investigation
- To close a known error

Notes
After you close a problem investigation, you can no longer modify it. Therefore, ensure that the root cause has been resolved and review all information about the problem investigation on the Problem Investigation form before you change the investigation's status to Closed.

If you do not close the problem investigation or the known error within a specified period of time, Problem Management automatically moves the status of the problem investigation or known error to Closed. The length of this period is configurable. Check with your system administrator to determine how much time your organization specifies. The default setting is 15 days.

To close a problem investigation

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. Review the Problem Investigation form to verify that the details are complete.
3. From the Status list, select **Closed**.
4. Click **Save**.
   The status is changed to Closed.

To close a known error

1. From the **Company** and **View By** lists on the Problem Management console, select the appropriate **Company and View By** criteria.
2. From the Defined Searches area of the Navigation pane on the Problem Management console, choose **Known Error > All Open Known Errors**.
3. Click **Refresh**.
   The Problems table refreshes with all open known errors for the selected **Company** and **View By** fields.
4. Select the known error and click **View**.
5. On the **Known Error** form, set the **Status** field to Closed.
6. Record a summary of how the known error was resolved:
   - *(Best Practice view)* Type the summary in the **Resolution** field.
   - *(Classic view)*
     a. Click the **Resolution** tab.
     b. Type the summary in the **Resolution** field.
7. Complete any other fields that will help someone else viewing the record to understand how the known error was resolved.
8. Click **Save**.

Indicating an impasse

If the specialist cannot find a root cause, or if the Change Management process rejected the known error, then the problem investigation is at an impasse and can not be resolved. If this occurs, update the known error and the problem investigation records to indicate this is the case.

This topic contains the following procedures:

- To indicate a problem investigation impasse
- To indicate a known error impasse

To indicate a problem investigation impasse

1. Open the relevant problem investigation as described in Viewing problem investigations.
2. In a work information note on the Work Detail tab (Work Info tab when using the Classic view), record why no further action currently is required.
3. Set the Status field to Pending.

> ⚠ **Note**
> If the problem investigation previously came to an impasse and the Status is already set to Pending, create a work information note indicating that a resolution is still not available. You must perform periodic checks of problem investigations at an impasse to see whether they can be resolved. For information about how to do this, see Performing periodic checks.

4. Click **Save**.

To indicate a known error impasse

1. To indicate a known error impasse, from the Defined Searches area of the Navigation pane on the Problem Management console, choose **Known Error > All Open Known Errors**.
2. Click **Refresh**.
   The Known Errors list refreshes with all open known errors for the selected Company and View By fields.
3. Select the known error and click **View**.
4. On the **Work Detail** tab of the Known Error form (Work Info tab when using the Classic view), create a work information note to explain why the problem was not fixed.
5. Set the **Status** field to **Canceled**.
6. Set the **Status Reason** field to **No Longer Applicable**.
7. Click **Save**.

Performing periodic checks

If a problem investigation results in an impasse, you must periodically check the problem investigation, to see if newer technology or another approach might provide a solution.

You can, for example, contact the supplier of the CI in which the root cause resides to see if the supplier has been able to determine a structural solution. You might also check websites that provide solutions for recognized, common errors or problems with specific versions of software or specific models of hardware.

If you determine that a structural solution or permanent workaround might now be possible, record this information in a work information note on the Work Detail tab and reassign it to a specialist for implementation (Work Info tab when using the Classic view); or if Change Management is required, create a known error. For information about how to do this, see Reassigning the problem investigation or Creating a known error.

If, after conducting the periodic check, it is apparent that a resolution is still not available, record this information in a work information note on the Work Detail tab (Work Info tab when using the Classic view). For information about how to do this, see Indicating an impasse.

Using flashboards

This section describes how to use flashboards.

- Using the KPI flashboards
- Using ROI flashboards
- Viewing and displaying data

Using the KPI flashboards

The KPI flashboards use graphs to show how well various business processes are performing against the application key performance indicators (KPIs). If you have BMC Service Management Process Model installed, you can also view the application KPI definitions there.

> ✓ **Tip**
> The BMC Service Management Process Model defines a key performance indicator as, "a vital and measurable result to track the efficiency, effectiveness, and predictability of a process."

The KPI flashboard component collects the data according to the selected customer company. Each KPI flashboard contains two graphs that present the following types of information:

- **Relevant historical data** — Use this graph for trending purposes. The most recent historical data displayed in the graph is collected from the previous month. Historical data goes back to a maximum of one year.

  > ⚠ **Note**
  > Historical data only appears in a graph when that historical data exists in the database. Typically, new or recent installations, or upgrades, of the ITSM applications might not have historical data available.

- **Current, or real time data** — Use this graph to see what is happening with the business process now. In most cases, the displayed real time data is collected from the first day of the current month to today's date. You can also view the individual request records that are reported by the real time flashboard graph. For example, you can view all of the incident or change request records that are reported by the Incident Backlog KPI or the Change Backlog KPI flashboard.

> ⚠ **Note**
> KPI flashboards are available only for version 7.6.00 (and later) of the BMC ITSM applications. If you are running a mixed environment, that is, if you are running some BMC ITSM applications at version level 7.5.01 (or earlier), you see flashboards with only the version 7.6.00 (or later) applications.

For information about how to do this, see Viewing and displaying data.

Related topic

Opening the KPI flashboards

KPI flashboard variables

KPI flashboards use variables to fetch the data that is used to create the flashboard graphs for the selected company. In most cases, you can control what data appears in the graph.

The following topics list the KPI graph types and the active variable names for Incident Management and Problem Management:

- Incident Management KPI flashboard variables
- Problem Management KPI flashboard variables

Incident Management KPI flashboard variables

The following tables list the Incident Management KPI graph types and the active variable names, and describes the information they provide. This helps you to understand the effects of hiding or displaying a specific variable.

Incidents resolved

Graph type	Variable name	Data displayed by the variable
Historical	HPD:INC:KPI_Incident_ResolvedHistory_V1	Displays the number of escalated incident requests that were closed in the past year. This data is shown in the blue portion of the graph.
Historical	HPD:INC:KPI_Incident_ResolvedHistory	Displays the number of non-escalated incident requests that were closed in the past year
Real Time	HPD:INC:KPI_Incident_Resolved_Real	Displays all of the closed incidents for the User Service Restoration service type that were closed without breaching the target date. This data is shown in the blue portion of the graph.
Real Time	HPD:INC:KPI_Incident_Resolved_Real_V1	Displays all of the escalated closed incidents for the User Service Restoration service type. This data is shown in the yellow portion of the graph.

Rejected solutions

Graph type	Variable name	Data displayed by the variable
Historical	HPD:INC:KPI_Rejected_SolnHistory	Displays the number of rejected solutions for the past year. This data is shown in the blue portion of the graph.
Historical	HPD:INC:KPI_Rejected_SolnHistory_V1	Displays the number of resolved incidents for the past year. This data is shown in the yellow portion of the graph.
Real Time	HPD:INC:KPI_Rejected_Soln	Displays the number of rejected solutions for the current reporting period. This data is shown in the blue portion of the graph.
Real Time	HPD:INC:KPI_Rejected_Soln_V1	Displays the number of resolved incidents for the current reporting period. This data is shown in the yellow portion of the graph.

Incident backlog

Graph type	Variable name	Data displayed by the variable
Historical	HPD:INC:KPI_BacklogHistory	Displays the number of incident requests that do not yet have Resolved, Closed, or Canceled status for the past year. **Note:** This graph uses only one variable. Hiding this variable prevents the graph from displaying any information.
Real Time	*You cannot select active variables for this graph.*	This real time graph does not use active variables. It displays the number of incident requests that do not have Resolved, Closed, or Canceled status for the current reporting period.

Service desk resolutions

Graph type	Variable name	Data displayed by the variable

Historical	HPD:INC:KPI_ServiceDeskHistory_v1	Displays the number of incident requests that were created by the service desk during the past year. This data is shown in the yellow portion of the graph.
Historical	HPD:INC:KPI_ServiceDeskHistory	Displays the number of incident requests that were created and resolved by the service desk during the past year. This data is shown in the blue portion of the graph.
Real Time	HPD:INC:KPI_ServiceDesk_V1	Displays the number of incident requests that were created by the service desk during the reporting period. This data is shown in the blue portion of the graph.
Real Time	HPD:INC:KPI_ServiceDesk	Displays the number of incident requests that were created and resolved by the service desk during the reporting period. This data is shown in the yellow portion of the graph.

Problem Management KPI flashboard variables

The following table lists the Problem Management KPI graph types and the active variable names, and describes the information they provide. This helps you to understand the effects of hiding or displaying a specific variable.

Problem Management KPI flashboards variables for incidents reported

Graph type	Variable name	Data displayed by the variable
Historical	PBM:PBI:KPI_ReportedIncidentsHistory	The number of registered incident requests that had the Service Type set to User Service Restoration or Infrastructure Restoration during the shown reporting period (This graph uses only one variable. Hiding this variable prevents the graph from displaying any information.).
Real time	*You cannot select active variables for this graph.*	This real time graph does not use active variables. It displays the number of registered incident requests with the Service Type set to User Service Restoration or Infrastructure Restoration.

Problem Management KPI flashboards variables for Problem Backlog

Graph type	Variable name	Data displayed by the variable
Historical	PBM:PBI:KPI_BacklogHistory	The number of problem investigations that were still open during the shown reporting period (This graph uses only one variable. Hiding this variable prevents the graph from displaying any information).
Real time	*You cannot select active variables for this graph.*	This real time graph does not use active variables. It displays the number of problem investigations that are still open.

Problem Management KPI flashboards variables for Problem Management Activity

Graph type	Variable name	Data displayed by the variable
Historical	PBM:PBI:KPI_ActivityHistory	The number of problem investigations that were still open during the shown reporting period. This data is shown in the blue portion of the graph.

Historical	PBM:PBI:KPI_ActivityHistory_V1	The number of problem investigations that were closed during the shown reporting period. This data is shown in the yellow portion of the graph.
Real time	PBM:PBI:KPI_Activity	The number of problem investigations that are still open. This data is shown in the blue portion of the graph.
Real time	PBM:PBI:KPI_Activity_V1	The number of problem investigations that are closed. This data is shown in the yellow portion of the graph.

BMC Service Desk KPIs

The following topics list and describe the incident management and problem management key performance indicators.

- Incident Management KPIs
- Problem Management KPIs

Incident Management KPIs

The following table lists and describes the incident management key performance indicators:

Incident Management KPIs

KPI name	Description of graph content
Incidents Resolved	This graph displays: • The number of closed incident requests with the Service Type field set to User Service Restoration and that were resolved without escalations • The total number of closed incidents
Rejected Solutions	This graph displays: • The number of times that an incident request was reopened because its solution was not accepted • The total number of resolved incident requests
Incident Backlog	This graph displays the number of incident requests that do not yet have their Status field set to Resolved, Closed, or Canceled.
Service Desk Resolutions	This graph displays: • The number of incident requests that were both registered and resolved at the service desk without assistance from another group • The total number of incident requests registered by service desk analysts

Problem Management KPIs

The following table lists and describes the problem management key performance indicators:

Problem Management KPIs

KPI name	Description of graph content
Incidents Reported	The number of registered incident requests with the Service Type set to User Service Restoration or Infrastructure Restoration
Problem Backlog	The total number of problem investigations that do not have their Status field set to Closed
Problem Management Activity	The number of new problems identified The number of solved problems. That is, the number of problem investigations with their Status field set to Closed.

Opening the KPI flashboards

Use this procedure when you need to open the KPI flashboards to view the information that they contain.

To open the KPI flashboards

1. Choose **Functions > KPIs**.
2. From the Company list select the customer company for which you want to view KPI flashboards.
3. From the Navigation pane, choose **Process KPIs > *KPIflashboardLink***.
   KPIflashboardLink is the link to the specific KPI flashboard that you want to see.

> ✓ **Tip**
> Click the triangle beside the Process KPI text to open and close this area of the Navigation pane.

Using ROI flashboards

The ROI flashboard provides a platform to compare the baseline costs that were incurred prior to implementing BMC Remedy IT Service Management with the actual costs incurred after installation. The Service Desk ROI flashboards include the baseline incident request call-handling and the baseline CI outage costs, while the BMC Change Management ROI flashboard provides the cost of failed changes.

> ⚠ **Note**
> In some cases, if the relative difference between the numbers reported in each graph is large enough, the smaller graph might not appear on the flashboard. However, a number representing the value of the smaller graph is always visible.

The information displayed in these graphs helps you to determine the return on investment (ROI) that your organization achieves from the BMC Remedy ITSM implementation.

> ⚠ **Note**
> To view the ROI console you must have ROI Viewer or ROI Admin permissions.

The ROI data is collected by the ROI flashboard component according to:

- The customer company that you select in the ROI console
- The date range that you specify in the ROI console
- A set of parameters that are configured by someone with ROI Admin permissions

For descriptions of what the configured parameters mean, see BMC Service Desk User documentation and BMC Change Management user documentation.

> ⚠ **Note**
> ROI flashboards are available only for version 7.6.00 of the BMC Remedy ITSM applications and later. If you are running a mixed environment, you see only the version 7.6.00 (or later) application flashboards listed on the ROI console. For example, if you are running version 7.6.00 of BMC Change Management and version 7.5.01 of BMC Incident Management, you see only the BMC Change Management flashboards on the ROI console.

Related topics

Configuring ROI flashboards
Opening the ROI flashboards

ROI active variables

The ROI flashboards use active variables to fetch the data that is used to create the graphs. The following tables list and describe the Cost of Incident Handling and the Cost of Outages active variable names and the meaning of the information they provide.

> ⚠ **Note**
> The active variable used to determine the *actual* cost of incident handling and the actual cost of outages depends on which value is selected for the Effort Input parameter (for incident handling) and Outage Input parameter (for outages) by the ROI administrator. For information about the ROI Administrator-configured parameters, see servicedesk81:Configuring parameters for the ROI flashboard.

The following tables describe the ROI active variables:

Cost of Incident Handling active variables (Effort Input = Specify Effort Estimate)

Active variable name	Meaning
ROI:Costofcallhandling_Baseline	Baseline costs
ROI:Costofcallhandling_Actual	Actual costs

Cost of Incident Handling active variables (Effort Input = Use Projected Effort)

Active variable name	Meaning
ROI:Costofcallhandling_Baseline	Baseline costs
ROI:Costofcallhandling_Usingprojectedeffort	Actual costs

Cost of Incident Handling active variables (Effort Input = Calculate Cumulative Effort)

Active variable name	Meaning
ROI:Costofcallhandling_Baseline	Baseline costs
ROI:Costofcallhandling_Usingcumulativeeffort	Actual costs

Cost of Outages — (Outage Input=Cumulative Resolution)

Active variable name	Meaning
ROI:CIUnavailability_Baseline	Displays the projected cost. The values for the cost are selected from the configuration form.
ROI:CIUnavailability_INC	Displays the Actual cost. The values are selected from Incident form and the configurations to arrive at the Actual Cost.

Cost of Outages — (Outage Input=Specify Estimated Outages)

Active variable name	Meaning
ROI:CIUnavailability_Baseline	Displays the projected cost. The values for the cost are selected from the configuration form.
ROI:CIUnavailability_Estimated	Displays the Actual cost. The values are selected from configuration forms directly for calculation.

Opening the ROI flashboards

This section describes the procedure to open the ROI flashboards from the BMC Remedy AR System IT Home page.

To open the ROI flashboards

1. In the Navigation pane of the BMC Remedy AR System IT Home page, select **Return on Investment > ROI Console** link.
2. From the lists at the top of the ROI console, select the following parameters:
   - **Company** — The client company for which you want to create a comparison
   - **Start Date** — The start date of the period for which the graph is created. The year of the start date must be 2000 or later.
   - **End Date** — The end date of the period for which the graph is created

   ⚠ **Notes**

   - The companies that you see in the **Company** list are controlled by your access level. The remaining fields are completed automatically by the application and are configurable by the system administrator.
   - Although you can enter a date range that includes a day of the month, the day of the month is ignored and only the month and the year are considered. For the purposes of the system calculations, start date is always assumed to be the first day of the selected month and year, and the end date is always assumed to be the last day of the selected month and year. For example, if you enter May 21, 2009, as the **Start Date**, and July 10, 2009, as the **End Date**, the system uses May 1, 2009, as the start date and July 31, 2009, as the end date.
3. In the ROI Navigation pane, select the ROI that you want to view.

⚠ **Note**
The links to ROI flashboards are based on the BMC Remedy ITSM applications that are installed.

Viewing and displaying data

Controls on the open flashboard help you view and display the data. The actions that you can perform and the procedures that you use to perform them are described in the following table.

⚠ **Note**
Not all of the flashboards support all of these procedures.

Viewing and displaying data

Action	Procedure
View specific records used to create the real time flashboard data Use this procedure, for example, to view all of the change request records with the **Status Reason** field set to Successful. This does not work on the historical data graph.	1. Click anywhere inside the real time graph. 2. In the search results list, select the record you want to view.
Zoom a graph Use the zoom feature to enlarge a section of the graph. You can also use full screen mode to enlarge the entire graph as described by View a graph in full screen mode which appears later in this table. The zoom functionality allows you to closely view each category on the X axis. For example, if the X axis has 5 categories, you can use the zoom functionality to view only 2 categories. The maximum zoom is a single category. For KPI reports with a single category, the zoom function is disabled.	1. Click the arrow in the lower left corner of the graph to expand the bottom control panel. 2. Click the magnifying glass icon, then follow the onscreen instructions.

Hide or display the graph legend The default setting is to show the graph legend. The legend provides information about how to interpret the graph. Not all graphs have a legend.	1. Click the arrow in the lower left corner of the graph to expand the bottom control panel. 2. Deselect or select the **Show Legend** check box to either hide or display the legend.
Change the graph style There are a number of different graph styles from which you can choose. For example, you can select to display the data in a line graph, a bar graph, a stacked bar graph, an area chart, and so on. Not all graphs support all graph styles.	1. Click the arrow in the lower left corner of the graph to expand the bottom control panel. 2. Click the double-arrow button, then select the graph style you want.
Change the graph titles You can customize the title text that appears on the graphs to suit your organization's needs. For example, you can change the titles of the X and Y axis.	1. In the upper right corner of the graph, click the Titles icon. 2. Change the label text appropriately to your organization's needs. 3. Click **Apply** when you finish updating the text.

Hide or display active variables The flashboards use active variables to fetch the data that is used to populate the graphs. If you choose to hide a variable, then the part of the graph that uses the variable is hidden. This gives you the ability to further customize the flashboards appearance. Not all graphs have active variables that you can turn on or off.	1. In the upper right corner of the graph, click the Titles icon. 2. Select or deselect the active variables that you want to display or hide.
View a graph in full screen mode You can display the selected graph across the entire screen for better visibility. Not all graphs display in full screen mode.	1. In the upper right corner of the graph, click the Full Screen icon. 2. When you finish viewing the graph in full screen mode, press **ESC** to restore regular display mode.

Using BMC Atrium Service Context

> ⚠ **Note**
> To use BMC Atrium Service Context, the BMC applications and BMC Atrium Core must be configured to support it. For information about the configuration procedures, see Configuring BMC Atrium Service Context for BMC Remedy ITSM applications.

This topic provides the following information:

- To open the Service Context Summary window from a console
- To open the Service Context Summary window from the record
- Interpreting the information
- Related topic

To use the Service Context Summary window, you must have the correct role:

- **Asset User** (when working from BMC Asset Management)
- **Work Order User** (when working from BMC Service Request Management)
- **Incident User** or **Problem User** (when working from BMC Service Desk)
- **Infrastructure Change User** or **Release User** (when working from BMC Change Management)

You must also have view permissions for the form from which you launch the Service Context Summary window.

BMC Atrium Service Context provides information for business service, application, and computer system CIs.

You can also see summary information about CIs that are related to the business service, but you must have view permissions for each related CI to see details about those CIs. If you cannot use the BMC Atrium Service Context feature, ask your system administrator to ensure that you have the correct permissions.

> **Notes**
> BMC Atrium Service Context displays information about the CI related to the record you are currently viewing. The types of information shown can include new work orders, recently completed changes, recent open incidents, related outage records, and so on. In addition, you can see CIs that are related to the business service, which helps you to understand the relationship that the business service has with its environment.
>
> The time threshold that determines how recently the recent changes, recent incidents, or new work orders were made or submitted, as well as the criteria used to determine other information types is configurable. Contact your system administrator for information about how the content of the information types is determined.

Understanding this relationship helps you to prioritize your incident investigations and align your decisions with your service level agreements and the overall goals of the business.

BMC Atrium Service Context information is displayed in the Service Context Summary window, which you can open from a variety of locations. The details that you see from, for example, the incident request form, are the same details that are shown in the other applications of the BMC IT Service Management Suite and Business Service Management solution, which ensures that everyone in your organization is working with the same information.

You can view the Service Context Summary window from one of the following locations:

- Application consoles
- Forms

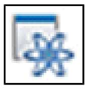
To open the Service Context Summary window from a console

1. With the application console open, in the summary table, select the record you want to see the BMC Atrium Service Context information for.
2. On the tool bar at the top of the summary table, click **Service Context**.
   The Service Context Summary window opens for the selected record.

To open the Service Context Summary window from the record

- **BMC Service Desk, BMC Change Management, and BMC Service Request Management** (for Work Order records) — With the record open, click the Service Context icon beside the Service field. The Service Context Summary window opens for the selected record.

  Service Context icon

- **BMC Asset Management** — With the record open, from the Quick Links area of the navigation pane, click **Service Context**. The Service Context Summary window opens for the selected record.

⚠ **Note**
In BMC Asset Management, BMC Atrium Service Context is available from the Business Service, Computer System, and Application CI forms.

Interpreting the information

The information panel at the top of the Service Context Summary window identifies the service name. The other information that appears in the information panel is configurable by your system administrator and comes from the CI form.

⚠ **Note**
For information about the **Owner** field, see Setting up the Owner field.

Below the information panel is a list of the key attributes. Next to each attribute is a counter that shows the number of active records of that type that are related to the selected service. If you click the counter, another Service Context Summary window opens with a table of detailed information about the records.

For example, if one of the configured attributes is "Recent Incidents" and the counter shows 3, there are 3 incidents currently related to the selected service. If you click the counter, a Service Context Summary window opens with a table that shows summary information about each of the incidents.

The information that appears in the Service Context Summary window is configurable. Ask your system administrator for detailed information about how BMC Atrium Service Context is configured in your environment.

Related topic

For information about configuring BMC Atrium Service Context, see Configuring BMC Atrium Service Context for BMC Remedy ITSM applications.

Working with reports

BMC Remedy ITSM provides a variety of predefined reports to give you quick and easy access to information about your system. Use the Report console to generate these reports. If the predefined reports return more information than you need, you can manage the scope of the report using qualifications. See the following topics:

- Generating a standard report
- Using qualifications to generate a report
- Using advanced qualifications to generate a report
- Incident Management predefined reports
- Problem Management predefined reports

From the Applications menu, choose **Quick Links > AR System Report Console** to view customized reports. This release of BMC Remedy ITSM integrates the Crystal Reports from version 7.6.00 and Web reports from version 7.6.01. On the web interface, a number of reports are available in the Web format. Additional Crystal Reports are available only if users have a valid Crystal Reports license and have chosen to install them for the web at the time of installation.

> ⚠ **Note**
> Customer Support can only provide limited assistance if you modify predefined reports and have a reporting problem. In addition, there is no guarantee that BMC Customer Support can solve problems that result from these modifications. The standard reports included with the BMC Remedy ITSM application are designed to be used without modification.

> ⛔ **Warning**
> If your database does not support the Not Equal To argument in this format: "!=", the content of your reports can be affected. Reports that have additional qualifications that filter out Group By fields (for example, 'Department' != "Engineering") also filter out the specified conditions and records that have Group By fields set to Unspecified or Null. Check with your system administrator to determine whether your database supports this form of the Not Equal To argument.

Generating a standard report

Use the following procedure to generate a standard report without qualifications. To generate a report with qualifications, see one of the following topics:

- Using qualifications to generate a report
- Using advanced qualifications to generate a report

To generate a report without qualifications

1. In the navigation pane on the application console, choose **Functions > Reports**.
2. On the Reporting console, select one of the options under **Show**:
   - **All Reports**, which displays all available reports
   - **Created by me**, which displays reports that you created
3. Under **Category**, select ***applicationName > reportCategory > reportName***.
   A list of available reports is displayed. Reports are organized by category, some of which contain subcategories. The reports that you see vary according to which applications are installed.
4. Select the report that you want to run.
5. Click **Run**.
   If you select a report that requires additional parameters, you are prompted to enter the required parameters. For example, if the selected report requires a date range, the date range field appears.
6. Enter the required parameters, and click **OK**.
7. If the report displayed is a web report, you can specify the following additional options:

Toggle Table of Contents TOC	Display the table of contents for the current report

Export Report	Export the report to a file of the specified format To export the report, select the appropriate page options, and click **OK**. The following formats are available under the Export Format list: • Excel • PostScript • PDF • Word • PowerPoint
Print Report	Print the report to HTML or PDF format

Using the web based reporting console to create and run adhoc reports (video)

> **Disclaimer**
> Although the concepts and procedures presented in this video are correct, the user interfaces shown are not current.

Related topics

For more information on creating reports, see Creating reports in the BMC Remedy AR System server documentation.

Using qualifications to generate a report

You can manage the scope of a report by adding qualifications to the criteria that the report engine uses to generate the report content. You can tell the report to search only certain specified fields for particular values, or you can build advanced qualifications by using field names, keywords, and operators.

This procedure describes how to generate basic qualifications by using the Show Additional Filter option. To generate a report by using advanced qualifications, see Using advanced qualifications to generate a report.

To use qualifications to generate a report

1. From the navigation pane in the application console, choose **Functions > Reports**.
2. On the Report Console, select one of the options under **Show**:
   - **All Reports**, which displays all available reports
   - **Created by me**, which displays reports that you created
3. Under **Category**, select ***applicationName > reportCategory > reportName***.
   A list of available reports is displayed. Reports are organized by category, some of which contain subcategories. The reports that you see vary according to which applications are installed.
4. Select the **Show Additional Filter** option.
   Along with a list of available fields, two sections are displayed-the simple query builder and the advanced query builder. You use the simple query builder to quickly construct a simple query. Alternatively, advanced users can use the advanced query builder to build the query by using BMC Remedy AR System query syntax.
   For additional information about the BMC Remedy AR System Report Console, see Reporting on BMC Remedy AR System data.

5. Select a field name from the **Available Fields** list, and click **Add** next to the simple query builder.

> **Note**
> Click ⛔ to remove a qualification.

6. Click the down arrow next to the field name listed in the qualification box, and select the appropriate operator. Enter or select a value for the field in the right column.

> **Example**
> If you want to enter the qualification **Cost Center = 001**, select the **Cost Center** field, click the down arrow next to the field and select =, and then enter 001 in the right column.

7. Repeat steps 5 and 6 for each field that you want to include in the report.
8. When you finish defining your additional qualifications, click **Run**.
9. If the report displayed is a web report, you can specify the following additional options:

Toggle Table of Contents	Display the table of contents
Export Report	Export the report to a file of the specified format To export the report, select the appropriate page options, and click **OK**. The following formats are available under the Export Format list: • Excel • PostScript • PDF • Word • PowerPoint
Print Report	Print the file to HTML or PDF format

Using advanced qualifications to generate a report

You can manage the scope of a report by adding qualifications to the criteria that the report engine uses to generate the report content. You can tell the report to search only specified fields for particular values, or you can build advanced qualifications by using field names, keywords, and operators.

To generate a report by using advanced qualifications

1. From the Navigation pane in the application console, choose **Functions** > **Reports**.
2. On the Report Console, select one of the options under **Show**:
   - **All Reports**, which displays all available reports
   - **Created by me**, which displays reports that you created
3. Under Category, select ***applicationName > reportCategory > reportName***.
   A list of available reports is displayed. Reports are organized by category, some of which contain subcategories. The reports that you see vary according to which applications are installed.

4. Select the **Show Additional Filter** option.
   Along with a list of available fields, two sections are displayed-the simple query builder and the advanced query builder. You use the simple query builder to quickly construct a simple query. Alternatively, advanced users can use the advanced query builder to build the query by using BMC Remedy AR System query syntax.
   For additional information about the BMC Remedy AR System Report Console, see Reporting on BMC Remedy AR System data.
5. Select a field name from the **Available Fields** list, and click **Add** next to the advanced query builder. Use the BMC Remedy AR System query syntax to build your qualification.
6. Construct your qualification by using the various operators provided by the qualification builder.
7. Repeat steps 5 and 6 for each field that you want to include in the report.

   ⚠ **Note**
   Select the qualification and press **Delete** to remove a qualification.

8. When you finish defining your advanced qualification, click **Run** to view the updated report.

Incident Management predefined reports

You first select the type of report that you want to run. The report type pulls information from the appropriate BMC Remedy ITSM application form. After you select a report type, you select the individual report that you want to run.

The **Web reports-names and descriptions** table describes the predefined Web reports, and the **Crystal Reports-names and descriptions** table describes the predefined Crystal Reports included, organized by the type of report.

Web reports — names and descriptions

Report name	Description
All Incidents > Incident Details (Dynamic – By Status and Assigned Groups)	
All Incidents by Status and Assigned Groups	Lists details of all incidents. Details include summary and work information. The report provides a summary of all incidents by status. You can drill down to the assigned groups for the selected incident status. You can also select an assigned group to see incident details. For additional details about the incident, you can select the incident record in the report to view the Incident form and take required action.
Open Incidents > Count By Assignee Group	
Open Incident Count by Assignee Group and Assignee	Provides a count of the incident by assigned group and the each assignee for the group. Management can use this report to review the current workload.
Open Incidents > Count By Product Categorization	
Open Incident Count by Product Categorization	Provides a breakdown of the number of incidents for each product category (for example, under Hardware, the count for Processing Unit)
Resolved Incidents > Resolved Incidents	

Resolved Incident Volume by Product Categorization	Displays details of all resolved incidents based on Tier 1 product categorization

Crystal Reports — names and descriptions

Report name	Description
Asset > Configuration Items with Open Incidents	
Configuration Items with Open Incidents	Lists CIs that have open incidents on them
Incident Information > Aging	
Incidents By Activity Time	Lists all open incidents and the amount of time since the reported date
Incident Information > All Incidents	
High Volume Incident by Company Chart	Displays a pie chart of all incidents based on the company. This report is intended for use with multi-tenancy.
High Volume Incident by Departments Chart	Displays a pie chart of all incidents based on the department
High Volume Incident Requester Chart	Displays a pie chart of all incidents based on the user
Incident Details by Date Range	Lists details of all incidents based on a specified date range. Details include Summary and work information.
Incident Volume By Product Categorization Chart	Displays a bar graph illustrating all incidents based on Tier 1 product categorization
Monthly Incident Volumes	Provides a count of all incidents by month
Weekly Incident Volume Chart	Provides a count of all incidents by week
Incident Information > Assignee Charts	
Open Incident Volume by Assignee	Displays a bar chart of the number of open incidents for each assignee
Resolved and Closed Incident Volume by Assignee	Displays a bar chart of the number of resolved and closed incidents for each assignee
Incident Information > Assignment Log Data	
Group Assignment to Incidents	Displays a history of the groups assigned to each incident request
Incident Information > Open Incidents	
Incident Volume By Priority and Status Charts	Displays a bar graph illustrating all open incidents based on Tier 1 product categorization
My Open Incidents	Reports all open incidents that are assigned to the ID from which the report is run

Open Incidents – Current / by Date Range	Provides a list of all open, current incidents or a list of incidents based on a particular date range
Incident Information > Resolved Incidents	
My Resolved Incidents	Displays all resolved incidents that are assigned to the ID under which the report is run
Resolved Incident Counts by Product Categorization	Provides a count of all resolved incidents based on product categorization
Resolved Incident Volume by Company Charts	Displays a pie chart illustrating all resolved cases based on company. This report is for multi-tenancy clients.
Resolved Incident Volume By Department Charts	Displays a pie chart illustrating all resolved cases based on a department
Resolved Incident Volume By Priority and Status Charts	Displays pie charts illustrating all resolved and closed cases--one based on status, and the other based on priority of all resolved cases
Resolved Incident Volume By Product Categorization Chart	Displays a pie chart illustrating all resolved incidents based on Tier 1 product categorization
Relationship Information > Change	
Change Induced Incidents	Lists incidents that were caused by changes **Note:** This report is available only if BMC Change Management is installed.
Incident Information > Related Configuration Items	
Incidents with Related Configuration Items	Returns a list of incident requests that have a related CI. Included is the type of CI, a summary of the incident request, and the reported date

Problem Management predefined reports

You first select the type of report that you want to run. The report type pulls information from the appropriate BMC Remedy ITSM application form. After you select a report type, you select the individual report that you want to run.

The **Web reports-names and descriptions** table describes the predefined Web reports, and the **Crystal reports-names and descriptions** table describes the predefined Crystal Reports included, organized by the type of report.

Web reports — names and descriptions

Report name	Description
Problem Investigation > All	
All Problem Investigations by Coordinator Group	Lists all problem investigations, based on the problem coordinator's group
Problem Investigation > Open by Service	
Open Problem Investigations by Service	Lists open problem investigation records grouped by service
Problem Investigation > Resolved by Product Categorization	

Resolved Problem volume by Product Categorization	Lists resolved and closed problem investigation records grouped by product category
Known Error > All by Coordinator Group	
All Known Errors by Coordinator Group	Lists all known errors, based on the problem coordinator's group

Crystal Reports — names and descriptions

Report name	Description
Known Error > Resolved > Resolved Known Errors by Coordinator Group	
Resolved Known Errors by Coordinator Group	Lists resolved known errors, which includes known errors with a status of canceled, closed, and corrected. The listing is grouped by status and problem coordinator group
Known Error > Open > Open Known Errors by Coordinator Group	
Open Known Errors by Coordinator Group	Lists open known errors records grouped by status and problem coordinator group
Problem Investigation > Open	
Open Problem Investigations by Coordinator Group	Lists open problem investigation records grouped by status and problem coordinator group
Problem Investigation > Resolved	
Resolved Problem Investigations by Coordinator Group	Lists resolved and closed problem investigation records grouped by status and problem coordinator group
Problem Investigation > Root Cause	
Problem Investigations by Root Cause	Lists problem investigations grouped by root cause
Resolved Problem Investigations by Root Cause	Lists all resolved problem investigations, grouped by the root cause of the problem

Using social collaboration

This release of BMC Remedy ITSM integrates chat functionality, RSS feeds, and Twitter notifications with the BMC Remedy ITSM applications. Users can now use these tools to collaborate with IT support users, such as Service Desk agents, or as additional notification options.

> **Note**
> For information about configuring social collaboration options, see Configuring social collaboration.

The following topics are discussed:

- Chat integration
- RSS feeds
- Twitter integration

Chat integration

The chat functionality enables BMC Remedy ITSM users to initiate one-on-one or group live chat sessions in the context of a specific record (for example a change record) from within the BMC Remedy ITSM applications. Using this functionality, IT support users can chat with other IT support users and initiate collaborative resolution of an incident or management of a change, among other actions. Administrators can configure the application to save these chat sessions as a work info entry within the record.

> ⚠ **Note**
> This integration is not intended for chat sessions between end users and IT.

For more information about using chat, see Using chat.

RSS feeds

BMC Remedy ITSM enables users to broadcast certain events using the Broadcast Messages functionality.

BMC Remedy ITSM integration with RSS feed enables access to specific BMC Remedy ITSM information using an RSS reader as an alternative mechanism. Administrators can configure different RSS feeds to which users can subscribe to. Out of the box, an RSS feeds for Global Public Broadcast messages is provided.

For more information about subscribing to RSS Feeds, see Subscribing to RSS feeds.

Twitter integration

The Twitter integration enables IT support users to propagate public and global BMC Remedy ITSM broadcast messages to a Twitter account so that users who follow the account receive the messages. The Twitter account must be configured before users can receive updates. Out of the box, this feature is supported only for broadcast messages that are Public and provided for the Global company.

For more information about receiving BMC Remedy ITSM broadcasts on Twitter, see Receiving BMC Remedy ITSM broadcasts on Twitter.

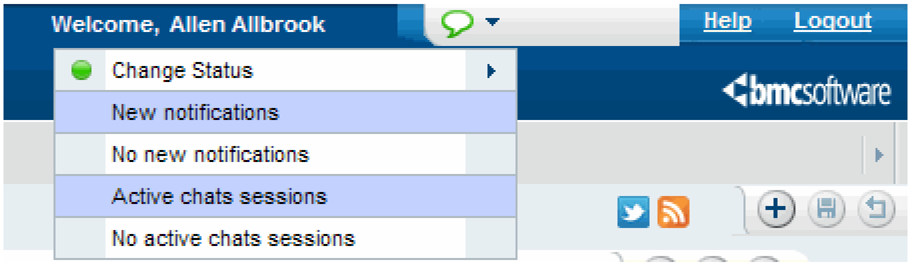
Related topics

Enabling chat, Twitter notifications, and RSS feeds
Configuring chat settings
Defining RSS feeds
Configuring the Twitter integration

Using chat

Using the chat feature, users can collaboratively work on BMC Remedy ITSM records. For example, you can collaboratively resolve issues by initiating a chat conversation related to the incident with other technicians who might be able to help resolve the issues faster. An IT Support technician can start a chat conversation with other members of the group to get help resolving an issue. When the chat initiator closes the conversation, it is saved as a Work Info entry and maintained as a part of the record.

The chat icon is displayed on the landing console when chat is configured for BMC Remedy ITSM, as shown in the following figure:



- Click this icon to open the chat initiation window.
- The color of the icon reflects your current chat status. Click the arrow beside the icon to view all chat conversations and to change your status. The status options are as follows:
  - Online
  - Busy
  - Away
  - Offline

The application displays a pop-up window when you receive an event like a chat invite or friend invite.

Related topics

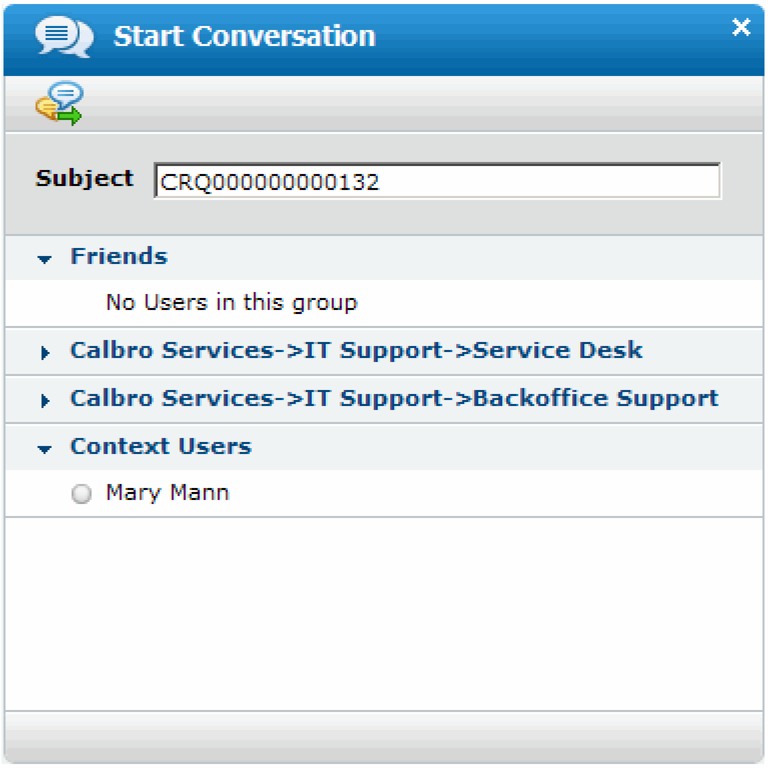
Initiating a chat conversation
Adding BMC Remedy AR System users who are not present in the Friends list
Configuring chat settings

Initiating a chat conversation

Follow this procedure to initiate a chat procedure with another user from within the BMC Remedy ITSM application.

To initiate a chat conversation

1. Within a record (for example a change record), click the chat icon.
   The **Start Conversation** window is displayed with a list of users related to the record.


Start Conversation
Subject
Friends
No Users in this group
Calbro Services->IT Support->Service Desk
Calbro Services->IT Support->Backoffice Support
Context Users
Mary Mann

Subject: CRQ000000000132

The following user lists are displayed:

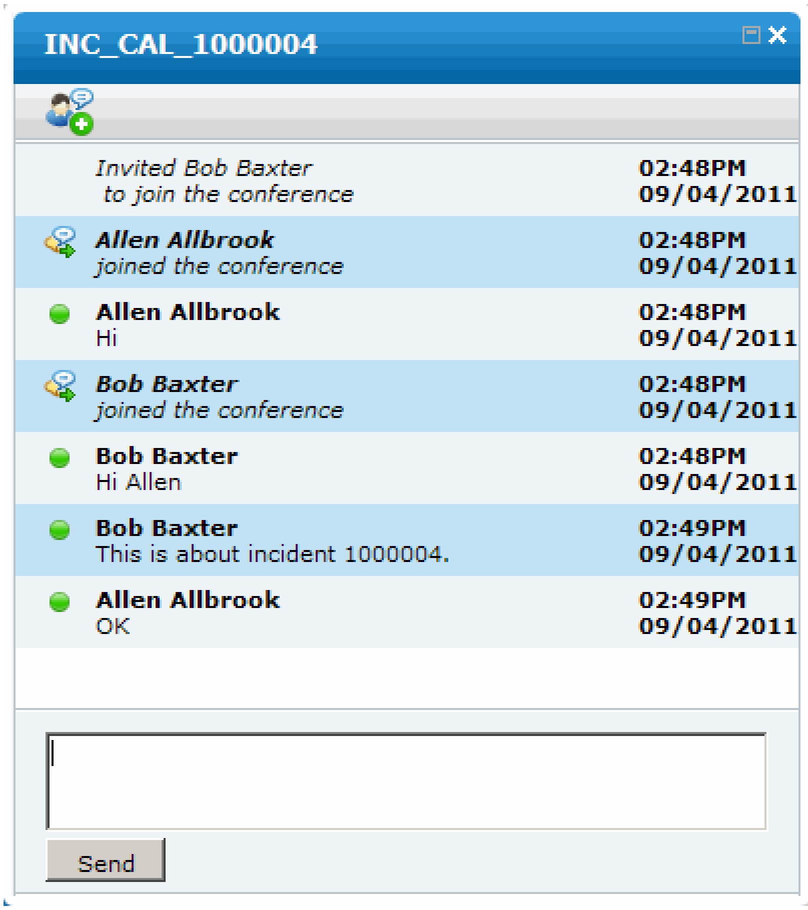
- **Friends** — Lists your friends from the configured chat client. For more information about configuring the friend list, see Mapping the BMC Remedy AR System users to the chat server in the BMC Remedy Action Request System documentation.
- **Support group users** — If the conversation is initiated within a record, the list displays users who belong to the same support group as the chat initiator.
- **Assigned users** — The user to whom the record is assigned. This list is displayed when you initiate the conversation from a record.
- **Context Users** — Lists users from the support groups that the user belongs to.

Form name	User	Support Groups
Activity	• Requested By • Activity Assignee	• Requested By • Assignee
Asset CI	All users from the **People** tab	All support groups on the **People** tab
Contract	Manage by Contract	Manager By
Change	• Change Coordinator • Change Manager	• Coordinator group • Manager group
Incident	• Assignee • Owner	• Assigned group • Owner group
Problem	• Problem Coordinator • Assignee	• Coordinator group • Assigned group

Known Error	• Problem Coordinator • Assignee	• Coordinator group • Assigned group
Solution DB	Assignee	Assigned group
Knowledge Article	• Author • Owner • Assignee	• Owner group • Assigned group
Release	Release Coordinator	Coordinator group
Task	• Requester • Assignee	• Support group • Assignee group
Work order	• Request Manager • Request Assignee	• Request Manager support group • Request Assignee support group

> **Note**
> When you launch a conversation from the landing console, a list of context users is displayed instead of assigned users.
>
> To add a user from another list to your friends list, click the **Send buddy request** icon displayed next to the user's name when you hover the mouse pointer on the user name.

2. Select the user you want to chat with from the relevant list and click the **Start Conversation** icon.
   The chat window that is displayed provides the following information:
   - User name of the person who initiated the conversation.
   - Subject of the conversation. The subject includes the ID of the record from which the conversation was initiated, the user who initiated the conversation, and other users included in the conversation. The subject can be a reference for users being invited to the conversation.
     Users can accept or reject the chat invitation. If they accept the invitation, a chat window is opened in their console. Their chat window displays only a list of users included in the chat and the conversation.
3. To invite additional users to the conversation, click the **Invite Users** icon displayed on the top right corner of the chat window. All participants can invite other users to the conversation.



INC_CAL_1000004

Invited Bob Baxter to join the conference 02:48PM 09/04/2011

Allen Allbrook *joined the conference* 02:48PM 09/04/2011

Allen Allbrook Hi 02:48PM 09/04/2011

Bob Baxter *joined the conference* 02:48PM 09/04/2011

Bob Baxter Hi Allen 02:48PM 09/04/2011

Bob Baxter This is about incident 1000004. 02:49PM 09/04/2011

Allen Allbrook OK 02:49PM 09/04/2011

> **Note**
> To add BMC Remedy AR System users who are not present in the Friends list, see Adding BMC Remedy AR System users who are not present in the Friends list.

When the conversation is complete and the chat initiator closes the chat window, the conversation is either saved as a Work Info entry in the **Work Detail** tab of the record from which the conversation was initiated, or not saved at all. This depends on the option you selected when Configuring chat settings.

> **Note**
> If the conversation was not initiated from within a record, the conversation is not saved.

Adding BMC Remedy AR System users who are not present in the Friends list

On the regular form where you have configured the BMC Remedy AR System server to work with the chat server, create an active link that executes on the Event type CHAT_SET_CONTEXT_RESP. For more information about events, see the following tables.

This active link sends an event to the **AR System Chat Data Visualization** field with Event type as CHAT_SET_CONTEXT_RESP and Event Data as given below:

ContextUsers=*ACommaSeparatedListOfBMCRemedyARSystemUsers***;ContextGroups=** *ACommaSeparatedListOfGroupIDs***;DisplayName=***SubjectOfTheChatConversation*;

For example:

- **ContextUsers**= John,Max,Amy;**ContextGroups**=1,2
- **ContextGroups**=1,2;**DisplayName**=Resolving an IT ticket;
- **ContextUsers**=John,Max,Amy;**ContextGroups**=1,2;**DisplayName**=Resolving an IT ticket;

List of events sent from the AR System Chat Data Visualization field to the parent form

Event name	Description
DVF_ON_READY	The Data Visualization Field (DVF) is loaded and is ready to interact. This is not specific to the chat DVM. No response expected.
CHAT_SET_CONTEXT_REQ	Sent to the parent form for the parent form to supply any contextual information. If the parent form chooses to provide this information, it later raises a corresponding event, CHAT_SET_CONTEXT_RESP.
CHAT_SESSION_START	Sent to the parent form to provide information on the chat progress. No response expected.
CHAT_INVITATION_SEND	Chat invitation sent. No response expected.
CHAT_USER_JOIN	A person is joining a chat session. This event occurs as many times as anyone joins a chat session. No response expected.
CHAT_USER_LEFT	A person is leaving a chat session. This event occurs as many times as anyone leaves a chat session. No response expected.
CHAT_INVITE_RECVD	A person is receiving a chat invitation. This event occurs as many times as anyone receives a chat session invitation. No response expected.
CHAT_DATA_AVAILABLE	When the chat widget has a chat conversation transcript available, this event is raised prior to chat session end, so that the parent form has an opportunity to save the transcript.
CHAT_SESSION_END	End of the chat session. No response expected.
CHAT_GET_SESSION_TRANSCRIPT_RESP	Provides a specific chat session transcript to the parent form.

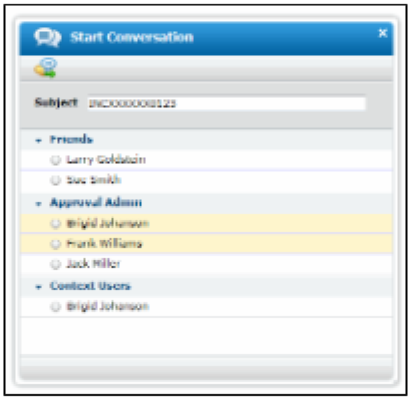
List of events sent from the parent form to the AR System Chat Data Visualization Field

Event name	Description
CHAT_SET_CONTEXT_RESP	Raised by the parent form's workflow during or after processing the CHAT_SET_SESSION_REQ event. No response expected.
FORM_EVENT_LOGOUT	Indicates to the DVF about things happening on the host form or the application. This is not specific to the chat DVM.
CHAT_GET_SESSION_TRANSCRIPT_REQ	Gets the chat session text transcript that is accumulated in the chat widget's buffer. This request event causes the DVF to raise the CHAT_GET_SESSION_TRANSCRIPT_RESP event.

When you create an active link that runs on the Event type CHAT_SET_CONTEXT_RESP, the Start Conversation window is displayed as follows:

> **Note**
> Click here to view a **.def** file sample that uses the above information through the BMC Remedy AR System form, "ChatTestForm" and it's related active links. Import this **.def** file using BMC Remedy Developer Studio and access the "ChatTestForm" from BMC Remedy Mid Tier to view it.

Start Conversation window
(Click the image to expand it.)



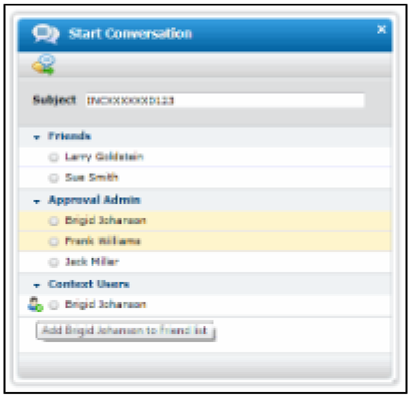
Start Conversation

Subject INC000000000123

- Friends
  - ○ Larry Goldstein
  - ○ Sue Smith
- Approval Admin
  - ○ Brigid Johanson
  - ○ Frank Williams
  - ○ Jack Miller
- Context Users
  - ○ Brigid Johanson

To add users to the Friends list, hover the pointer over the user name that is not present in your Friends list and click the **Add to Friend list** icon that appears to the left of the user name.

Add user to Friend list on the Start Conversation window
(Click the image to expand it.)



Start Conversation

Subject INCXXXXXX0123

- Friends
  - ○ Larry Goldstein
  - ○ Sue Smith
- Approval Admin
  - ○ Brigid Johanson
  - ○ Frank Williams
  - ○ Jack Miller
- Context Users
  - ○ Brigid Johanson

Add Brigid Johanson to friend list

> **Note**
> BMC Remedy AR System does not allow searching and adding friends without context. For example, to see how BMC Remedy ITSM Suite has defined context users, see Initiating a chat conversation.

Subscribing to RSS feeds

Users can to subscribe to configured RSS feeds from within the BMC Remedy ITSM applications. The RSS feed option must be enabled in the System Settings configuration. To enable RSS feeds, see Enabling chat, Twitter notifications, and RSS feeds.

For additional information about configuring RSS feeds, see Defining RSS feeds.

To subscribe to RSS feeds

1. On the IT Home Page, click the RSS feeds icon.
   A list of the RSS feeds that have been configured is displayed.
   RSS Feed URLs
   Click the following figure to expand it.

2. Copy the URL of the RSS feed that you want to add to your RSS feed client (for example, Microsoft Outlook RSS feeds).
3. Replace the user name and password in the URL with the appropriate values.
   You are now subscribed to receive updates for the selected RSS feeds.

Receiving BMC Remedy ITSM broadcasts on Twitter

The integration with Twitter enables users to receive BMC Remedy ITSM notifications directly to their Twitter accounts. Users can follow the functional BMC Remedy ITSM Twitter notification account.

To receive BMC Remedy ITSM broadcasts on Twitter:

- The functional BMC Remedy ITSM notification account must be created in Twitter, and configured and authenticated, before users can follow the account.
- Users must have a Twitter account that can receive the BMC Remedy ITSM notifications.

For more information about configuring a functional BMC Remedy ITSM Twitter notification account, see Configuring the Twitter integration.

To follow ITSM notifications on Twitter

1. On the IT Home Page, click the Twitter icon.

   > ⚠ **Note**
   > If the Twitter icon is not displayed, make sure that you configured the twitter integration (see Configuring the Twitter integration and enabled the Twitter notification functionality (see Enabling chat, Twitter notifications, and RSS feeds).

2. If you are not logged on to the Twitter account, the logon screen is displayed.
3. Log on to Twitter using your account details.
   The Twitter website is opened in a new browser window with the Twitter account that was configured for the broadcast.
4. On the displayed Twitter page, click **Follow** to receive broadcast messages posted to this BMC Remedy ITSM Twitter notification account.

For information about sending BMC Remedy ITSM broadcasts using Twitter, see Creating broadcast messages.

Administering

This section contains information about managing configuration items.

⚠ **Notes**

- For information about using Data Management to load data, see Data Management.
- For information about BMC Service Desk permissions, see Incident Management and Problem Management permissions.
- The main configuration tasks for application administrators are documented in Configuring after installation; for example:
  - Configuring Incident Management
  - Configuring Problem Management
  - Selecting the application preferences

Managing configuration items

A *configuration item* (CI) is a physical, logical, or conceptual entity that is part of your IT environment and has configurable attributes.

Some CI types are virtual, while others are physical and include hardware and software. The Service CI type is an example of a virtual CI. In this context, a service can be provided from one business or organization within a business to another. Service CIs can include customer support, employee provisioning, web farms, storage, and so on.

You can use the information in CIs to diagnose user problems and to determine if a change to a CI or the IT infrastructure must be made. For example, if a user calls in with a printing problem, you can check the printer's CI to see whether the printer is down.

To record information against CIs, such as CI unavailability, or to relate an problem investigation to a CI, the CI must be recorded in the BMC Atrium Configuration Management Database (BMC Atrium CMDB). If you do not have BMC Asset Management, then BMC Service Desk provides limited ability to manage CIs and inventory.

⚠ **Note**
You can manage configuration items even if your environment does not run BMC Asset Management. To manage configuration items, including creating and modifying CIs and managing inventory for bulk and non bulk CI's, you do not need a BMC Asset management license. However, if you are running BMC Asset Management, then you have access to additional functionality. See the BMC Asset Management Key concepts page for more information about BMC Remedy Asset Management functions.

To make use of this additional functionality, you will need either Asset Admin or User permissions and a BMC Remedy AR System fixed or floating license.

This section contains the following topics:

- Creating CIs
- Inventory management

Creating CIs

To create a CI, you must have Asset Admin permission. If you have Asset User permission and you are modifying a CI, your administrator must open the appropriate CI, and then relate your support group to the CI.

There are many different types of CIs that you can create. While the general procedure for creating each CI type is similar, only the specific fields on the CI form change depending on the CI type.

These pages provide examples of how to create different types of CIs:

- Creating a business service
- Creating a computer system CI
- Creating a bulk inventory CI
- Creating an inventory location CI

Creating a business service

This topic describes how to create a business service.

> ⚠ **Note**
> This procedure both creates the business service and relates the service to a company. This is necessary to make sure the service appears in the **Service** field menu on the main form (Best Practice view) or the Classification tab (Classic view), when relating the problem investigation to a company.

To create a business service

1. From the Navigation pane of the console, choose **Functions > Manage CIs**.
2. From the CI Type list , select **Logical Entity > Business Service** and then click **Create**.
3. On the Business Service form, type the CI name in the **CI Name** field.
   When creating a CI name, BMC recommends that you follow a consistent naming convention. According to ITIL guidelines, identifiers should be short but meaningful. For example, Payroll or Network. The name can be followed by a numeric code, such as NETWORK100.
4. Complete the optional fields that appear on the form in a way that is appropriate for the service you are creating.

   Optional fields when creating a business service

Field name	Description
CI ID	A customer specified identifier. You can use this to augment the CI Name.
Company	The company that owns the service
Impact, Urgency, and Priority	Used to determine service levels when assigning support
Supported	Indicates whether the service currently is supported
System Role	A description of the role the service fulfills in the organization
Additional Information	A place to record any additional information about the service
Users Affected	The number of users who use this service

Product Categorization	Use this file to categorize the business service through multiple tiers. This hierarchy is used to drive assignment routing.
Location	The location of the support group that supports the service
Lifecycle	The date on which the service became active

5. Click **Save**.

   ⚠ **Notes**

   - Depending on how your application is configured, after you click **Save** to create a Service CI, the Service CI form might be redisplayed in a Modify window.
   - The People tab referred to in the following step does not appear on the Business Service form until you create and save the CI. The Relationships tab, Outage tab, and Impact tab also appear after you save the new CI. If the People tab does not appear after you click **Save**, then search for and open the CI record as described in To search for CIs from the console, and then continue with step 6.

6. Open the People tab and click **Add**.
7. From the Type list in the CI Person Type, select People Organization and then click **OK**.
8. From the Company list in the Organization Search window, select the company to which you are relating the service and then click **Search**.

   ⚠ **Note**
   If you are relating the service to the entire company, then skip step 9.

9. If you must relate the service either to an organization within the company or to a department within the organization, select the organization and, if necessary, the department from the Organization and Department lists.
   - Organization — If you choose Organization, the service is related to the specified organization within the specified company.
   - Department — If you choose Department, the service is related to the specified department within the specified organization.
10. From the Choose a Relationship Level list, select how much of the company will be related to this service. For example, if you are relating the service to the entire company, then select Company. If you specified department in the preceding step, then select Department, and so on.
11. Click **Select**.
12. From the Role list in the Asset Person Role window, select Used By and click **OK**.
13. Click **OK** to dismiss the confirmation note.
14. Click **Save** and then click **Close**.

Related information

For information about designing, developing, and maintaining service models that enable you to manage your IT resources from the perspective of the business services that they provide, see Planning a service model.

Creating a computer system CI

This topic describes how to create a computer system CI.

To create a computer system CI

1. From the Navigation pane of the console, choose **Functions > Manage CIs**.
2. From the CI Type list of the CI Type dialog box, select **System > Computer System**.
3. Click **Create**.
4. In the **CI Name** field of the Computer System form, type a name for the CI.
   When creating a CI name, BMC recommends that you follow a consistent naming convention. According to ITIL guidelines, identifiers should be short but meaningful, and for hardware they should not based on supplier device names. For example, the name can include an indicator of the CI's function (such as Workstation or Monitor) followed by a numeric code, such as MONITOR100.
5. In the **CI ID** field, type a unique alphanumeric value for the CI.
6. Select the company to which this CI belongs.
7. From the Primary Capability and Capability lists, select the roles this CI performs in your company's topology.
8. Select a status from the Status list.
   The default value is Deployed. You can select one of the following options:

Status	Description
Ordered	The CI was ordered from the supplier.
Received	The CI was received in shipping.
Being Assembled	The CI is being assembled.
Deployed	The CI was installed.
In Repair	The CI is down for maintenance.
Down	The CI is down, but not yet in maintenance.
End of Life	The CI is no longer being deployed.
Transferred	The CI was transferred to another place.
Delete	The CI is marked for deletion. You must be a member of the APP-Management or APP-Administrator group to mark a CI for deletion.
In Inventory	The CI is in inventory but not yet deployed. When you select this status, you are prompted to select the inventory place.
On Loan	The CI is on loan to another location.
Disposed	The CI is no longer available and was disposed of.
Reserved	The CI was reserved and taken out of inventory.
Return to Vendor	The CI must be returned to the vendor as damaged or unwanted.

9. Specify whether the CI is supported by selecting Yes or No from the Supported list.
10. Select what impact or urgency this CI will have if it goes down.
11. In the **Users Affected** field, specify the number of people who use this CI or will be affected if it goes down.
12. Complete the other fields in this area:

Field name	Description
Tag Number	The CI tag number; this is the number usually placed on the product by a member of your IT department to track the CI.
Serial Number	The CI serial number
Part Number	The CI part number
System Role	The role this CI plays in your company
Status Reason	The reason this CI has the status it does

13. Click the General tab.
14. Categorize your CI using the lists and fields in the Product Categorization area.
15. Specify the place of the CI using the lists and fields in the Location area.
16. Enter the dates of the CI in the lifecycle area.
17. Click the Specifications tab.
18. Add more information about the CI.
19. Click **Save**.

Creating a bulk inventory CI

This topic describes how to create a bulk inventory CI.

⚠ **Note**
Bulk inventory items are not tracked by an separate record for each item. Instead, bulk items are tracked by quantities of an item type. For example, cables used to connect desktop computers to the network do not require individual records but rather, one record for a bulk quantity of the specific cable type.

To create a bulk inventory CI

1. From the Navigation pane of the console, choose **Functions > Manage CIs**.
2. From the CI Type list of the Manage CI Information dialog box, select **Bulk Inventory > Bulk Inventory**, and click **Create**.
3. In the Bulk Inventory form, complete the following required fields.

Field name	Description
CI Name	Enter the name of the bulk inventory item, for example, Microsoft Windows XP.
Tier 1, **Tier 2**, and **Tier 3**	Categorize the item.
Received Quantity	Enter the number of items received.

4. Click **Save**.

Creating an inventory location CI

This topic describes how to create an inventory location CI. You can use inventory location CIs to indicate where bulk inventory and other CIs are located.

To create an inventory location CI

1. From the Navigation pane of the console, choose **Functions > Manage CIs**.
2. From the Type list of the Manage CI Information dialog box, select **System > Inventory Location**, and click **Create**.
3. In the **CI Name** field of the Inventory Location form, enter the location name.
4. Complete the optional fields.
5. Click **Save**.

Inventory management

You can use the Manage Inventory function to track bulk inventory items and other CIs that are available for deployment.

Before you can manage inventory, you must:

- Create bulk inventory CIs, or other CIs to be tracked as inventory.
- Create inventory location CIs.
- For bulk inventory, specify the received quantity and the inventory locations. For information about how to do this, see Placing bulk CIs in inventory.
- For non-bulk inventory CIs, set the inventory status to In Inventory, and select a location. For information about how to do this, see Placing non-bulk CIs in inventory.

Placing bulk CIs in inventory

To place bulk CIs in inventory, you must specify the location or locations for them.

> ✓ **Tip**
> If you do not see a location, ensure that the CI has a CI type of inventory location, and not physical location. For information about creating inventory locations, see Creating an inventory location CI.

To place bulk CIs in inventory

1. Open a bulk CI, as described in To search for CIs from the console.
2. On the **Inventory Location** tab, click **Add**.
3. In the Search Inventory Locations dialog box, specify the search criteria and click **Search**.
4. Select a location, and click **Relate**.
5. In the message about the relationship, click **OK**.
6. If the inventory is stored in multiple locations, for each location, repeat step 4 and step 5.
7. Click **Close**.
   On the Bulk Inventory form, the **Inventory Location** tab lists each of the related locations.

8. Click in the **Quantity Per Location** field for a location, and type the quantity in that location.
9. Continue to enter the quantity for each location, until all the quantity in stock for the bulk CI is accounted for.
10. Click **Save**.

After items are in inventory, you can use the Manage Inventory function to view, relocate, and reserve and use CIs and bulk inventory items. See Managing inventory.

Placing non-bulk CIs in inventory

You can place non-bulk CIs that you want to manage in inventory by changing the status of the CI to In Inventory, and then designating a location for that CI.

To place non-bulk CIs in inventory

1. Open a CI, as described in To search for CIs from the console.
2. From the **Status** list, select In Inventory.
3. Click **OK** in the confirmation message that appears.
4. In the Search Inventory Locations dialog box , from the **Location** list, select a location, make sure other values are correct, and click **Search**.
5. Select a location and click **Return**.

Managing inventory

This topic describes how to perform inventory management tasks that you most commonly use.

- To search for CIs from the console
- To view inventory locations
- To relocate CIs
- To reserve and use inventory

To search for CIs from the console

1. From the Functions area of the console Navigation pane, click the Manage CIs link.
2. From the CI Type list on the Manage CI Information window, select the type of CI you are looking for and click **Search**.
3. On the form that appears, provide as much information about the CI you are searching for as possible and click **Search**.
4. From the search results list at the top of the window, select the CI.
   The details appear in the CI form below the search results.

To view inventory locations

1. From the Navigation pane of console, choose **Functions > Manage Inventory**.
2. Enter your search criteria in the Manage Inventory dialog box, and click **Search**.

Results matching your search criteria appear in the table.

3. Select a CI or bulk inventory item from the table, and click **View Location**.
4. View the CIs in the inventory listed in the Inventory Location form.
5. Click **Close**.

To relocate CIs

1. From the Navigation pane of the console, choose **Functions > Manage Inventory**.
2. Search for inventory in the current location using the Manage Inventory dialog box.
3. Select the CI or bulk inventory item you want to relocate, and click **Relocate CIs**.
4. For the location where you want to relocate the CI, specify search criteria, and click **Search** in the Search Inventory Locations dialog box.
5. Select the location where you want to relocate your CI.
6. In the **Quantity** field, enter the number of CIs you want to relocate.
7. Click **Relocate**.

To reserve and use inventory

1. From the Navigation pane of console, choose **Functions > Manage Inventory**.
2. From the CI Type menu in the Manage Inventory dialog box, select the CI or bulk inventory item you want to reserve and use.
3. Click **Search**.
4. Click in the Transaction Qty column and enter the number of assets or bulk inventory items you want to use.
5. Click **Reserve/Use Inventory**.
   The number of CIs or bulk inventory items in the Qty in Stock column is reduced by the number reserved and used.

Developing

This topic contains information for developers who need to customize their BMC Service Desk environment.
Sub-topics include:

- Developing integrations
- Incident Management integrations
- Problem Management integrations

Other development information related to the BMC Service Desk application is available in the Developing section of the BMC Remedy IT Service Management Suite documentation.

Developing integrations

This section of the information is for developers who want to use the application interfaces associated with BMC Remedy ITSM to enable external applications, such as web services, to create, modify, and search for tickets within the BMC Remedy ITSM applications.

- Integration model
- BMC Remedy ITSM integrations
- Testing web services using soapUI

This section focuses particularly on web services. For information about other integration types, see Integrating.

To take full advantage of the information presented, you should have a working knowledge of the BMC Remedy Action Request System (BMC Remedy AR System) and the BMC Remedy ITSM applications' common foundation.

Web services information is provided for the following applications:

- BMC Service Desk: Incident Management
- BMC Service Desk: Problem Management
- BMC Asset Management
- BMC Change Management

> ⚠ **Note**
> The Release Management module is also described in Change Management and Release Management web services.

For information on integration with the BMC's Task Management System module, see Task Management web services.

This information includes:

- Descriptions of inputs and outputs for the interface form
- Descriptions of the web services inputs and outputs, which provide a real working example of how to use the interface forms

For information related specifically to BMC Service Desk Integrations, see the following sections:

- Incident Management integrations
- Problem Management integrations

Related topic

For conceptual information about integrations, see Integrating.

Incident Management integrations

You use the interface forms in Incident Management to:

- Create or modify an incident
- Query an incident or a list of incidents

When creating an incident, if necessary, you can also associate the incident to an existing CI and create a work information entry.

⚠ **Note**
You can also create a work information entry during an incident modification.

The following web service functions are available for Incident Management. These functions are described in the rest of this section.

- **HelpDesk_Submit_Service** creates and submits incident tickets with work information and CI associations.
- **HelpDesk_Modify_Service** modifies incident tickets with work information.
- **HelpDesk_Query_Service** and **HelpDesk_QueryList_Service** allow searches for specific incident tickets (using the query service) or a set of incident tickets (using the query list service).
- **HelpDesk_GetWorkInfoList** retrieves a list of work info records for a list of incidents.
- **GetListOfRelatedIncidents** retrieves a list of related incidents.

HelpDesk_Submit_Service

The following tables list the values needed to submit an incident through the **HPD:IncidentInterface_Create** form. You can create incident records either through web services, or through the interface form.

Required input fields to return customer information

This table lists fields that are required to get the customer information from the People form.

DB field on interface form	Displayed on web services	Field value	Notes
Last_Name	Last_Name		Used to populate the customer information section on the HPD:Help Desk form
First_Name	First_Name		Used to populate the customer information section on the HPD:Help Desk form
Middle Initial	Middle_Initial		Used to populate the customer information section on the HPD:Help Desk form
Login_ID	Login_ID		Used to populate the customer information section on the HPD:Help Desk form
Contact_ Company	Customer_Company		Used to populate the customer information section on the HPD:Help Desk form
Corporate ID	Corporate_ID		Used to populate the customer information section on the HPD:Help Desk form

⚠ **Note**
You can pass all of the fields in this table to the interface to get the customer information from the People form, or just one of the following subsets:

- Login_ID (Login_ID is considered a unique identifier on its own)
- Customer_Company and Corporate_ID (when used together, these two fields are consider a unique identifier)
- First_Name, Middle_Initial, and Last_Name (this subset of fields might not guarantee a unique identification, depending on how data is delimited in your system)

Required core attribute fields
This table lists the required core attribute fields.

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	CREATE	Keyword triggers workflow that initiates the submit operation
Status	Status		
Service_Type	Service_Type		
Impact	Impact		
Urgency	Urgency		
Description	Summary		Maps to Summary on the HPD:Help Desk form
Reported Source	Reported_Source		

Optional input field values
The following table lists optional input field values:

DB field on interface form	Displayed on web services	Notes
Detailed_Description	Notes	
Status_Reason	Status_Reason	
Assigned Support Company	Support_Company	Required when status is set to greater than or equal to Assigned
Assigned Support Organization	Support_Organization	Required when status is set to greater than or equal to Assigned
Assigned Group	Assigned_Group	Required when status is set to greater than or equal to Assigned
Assigned Group Shift Name	Assigned_Group_Shift_Name	Required when status is set to greater than or equal to Assigned
Assignee	Assignee	Required when status is set to greater than or equal to Assigned

Product Categorization Tier 1	Product_Categorization_Tier_1	Displayed under the Product Categorization section on the interface and main forms
Product Categorization Tier 2	Product_Categorization_Tier_2	
Product Categorization Tier 3	Product_Categorization_Tier_3	
Product Name	Product_Name	
Product Model/Version	Product_Model_Version	
Manufacturer	Manufacturer	
Categorization Tier 1	Categorization_Tier_1	Displayed under the Operational Categorization section on the interface and main forms
Categorization Tier 2	Categorization_Tier_2	
Categorization Tier 3	Categorization_Tier_3	
Closure Product Category Tier1	Closure_Product_Category_Tier_1	Displayed under the Resolution Product Categorization Section on the interface and main forms
Closure Product Category Tier 2	Closure_Product_Category_Tier_2	
Closure Product Category Tier 3	Closure_Product_Category_Tier_3	
Closure Product Name	Closure_Product_Name	
Closure Product Model/Version	Closure_Product_Model_Version	
Closure Manufacturer	Closure_Manufacturer	
Resolution Category Tier 1	Resolution_Category_Tier_1	Displayed under the Resolution Categorization Section on the interface and main forms
Resolution Category Tier 2	Resolution_Category_Tier_2	
Resolution Category Tier 3	Resolution_Category_Tier_3	
Direct Contact Company	N/A	
Direct Contact First Name	Direct_Contact_First_Name	
Direct Contact Last Name	Direct_Contact_Last_Name	
Direct Contact Phone Number	N/A	
Direct Contact Internet E-mail	N/A	
Direct Contact Organization	N/A	
Direct Contact Department	N/A	
Direct Contact Site	N/A	
CI Name	CI_Name	For more information about this element, see Associating entries with configuration items.

Lookup Keyword	Lookup_Keyword	For more information about this element, see Associating entries with configuration items.
z1D_WorklogDetails	Work_Info_Summary	Required for creating work information
z1D_ActivityType	Work_Info_Type	Optional for creating work information. Defaults to General Information if left null.
z1D_Secure_Log	Work_Info_Locked	Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_View_Access	Optional for creating work information. Defaults to Internal if left null.
z1D_Details	Work_Info_Notes	Optional for creating work information
z1D_ActivityDate_tab	Work_Info_Date	Optional for creating work information
z1D_CommunicationSource	Work_Info_Source	Optional for creating work information
Flag_Create_Request	Create_Request	A Yes or No selection. Used to automatically generate a request entry when set to Yes. For more information about this, see Creating a service request entry.
ServiceCI	ServiceCI	For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items
HPD_CI_ReconID	HPD_CI_ReconID	
Middle Initial	Middle_Initial	If specified, the Middle Initial can make the customer information more unique. Otherwise, it will get populated automatically, if applicable.
Status_Reason	Status_Reason	
Direct Contact Middle Initial	Direct_Contact_Middle_Initial	If specified, the Middle Initial can make the direct contact information more unique. Otherwise, it will get populated automatically, if applicable.
TemplateID	TemplateID	Optional for creating an incident using Incident Templates. Specify the Template InstanceID (FieldID 179) which can be found on the HPD:Template form.

Fields set through workflow
The following table lists the fields set through workflow:

DB field on interface form	Notes
Incident Number	
Contact_Company	
Company	
Client Type	
Client Sensitivity	
VIP	

Middle Initial	
Priority	Set from impact and urgency values
Priority Weight	Set from impact and urgency values
Person ID	
Site Group	
Site	
Site ID	
Organization	
Region	
Desk Location	
Mail Station	
Internet E-mail	
Phone_Number	
Department	
Reported Date	
CC Business	Label is--Country Code
Area Business	Label is--Area Code
Local Business	Label is--Local Phone
Extension Business	
Incident_Entry_ID	
Assignee Login ID	Set from the Assignment workflow
Schema Name	Set from the CI Association
HPD_CI	Set from HPD_CI_ReconID value
HPD_CI_FormName	Set from HPD_CI_ReconID value
z1D_CI_FormName	Set from HPD_CI_ReconID value
State Province	Set by the specified customer information
Street	Set by the specified customer information
Zip/Postal Code	Set by the specified customer information
Corporate ID	Set by the specified customer information
Time Zone	Set by the specified customer information
Direct Contact Region	Set by the specified direct contact information
Direct Contact Site Group	Set by the specified direct contact information
Direct Contact Street	Set by the specified direct contact information
Direct Contact State/Province	Set by the specified direct contact information
Direct Contact City	Set by the specified direct contact information

Direct Contact Zip/Postal Code	Set by the specified direct contact information
Direct Contact Time Zone	Set by the specified direct contact information
Direct Contact Desk Location	Set by the specified direct contact information
Direct Contact Mail Station	Set by the specified direct contact information
Direct Contact Site ID	Set by the specified direct contact information
Direct Contact Country Code	Set by the specified direct contact information
Direct Contact Area Code	Set by the specified direct contact information
Direct Contact Local Number	Set by the specified direct contact information
Direct Contact Extension	Set by the specified direct contact information

HelpDesk_Modify_Service

The following table indicates the values required to modify an incident through the **HPD:IncidentInterface** form. You can modify incident records either through web services or the interface form.

When modifying an incident record through web services, observe the following points:

- All fields mapped with values on the Help Desk form must be populated by the interface form, otherwise a null value is sent, and the current values are overwritten.
- The Assignee must be set through the **HPD:Help Desk** form to move past the Assigned status.

Input fields

DB field on interface form	Displayed on web services	Field value	Notes
z1D Action	Action	MODIFY	Keyword triggers workflow that initiates the modify operation
Incident Number	Incident_Number	ID of Incident to modify	This qualification determines which incident to modify.
Company			
Impact	Impact		
Urgency	Urgency		
Description	Summary		Appears in Summary on the Help Desk form
Detailed Description	Notes		Appears in Notes on the Help Desk form
Status	Status		
Service Type	Service_Type		
Reported Source	Reported_Source		
Product Categorization Tier 1	Product_ Categorization_Tier_1		

Product Categorization Tier 2	Product_ Categorization_Tier_2		
Product Categorization Tier 3	Product_ Categorization_Tier_3		
Product Name	Product_Name		
Product Model/Version	Product_Model_Version		
Manufacturer	Manufacturer		
Categorization Tier 1	Categorization_Tier_1		
Categorization Tier 2	Categorization_Tier_2		
Categorization Tier 3	Categorization_Tier_3		
Closure Product Category Tier1	Closure_Product_Category_Tier1		
Closure Product Category Tier2	Closure_Product_Category_Tier2		
Closure Product Category Tier3	Closure_Product_Category_Tier3		
Closure Product Name	Closure_Product_Name		
Closure Model/Version	Closure_Product_Model_Version		
Closure Manufacturer	Closure_Manufacturer		
Resolution	Resolution		
Resolution Category	Resolution_Category		
Resolution Category Tier 2	Resolution_Category_ Tier_2		
Resolution Category Tier 3	Resolution_Category_ Tier_3		
Resolution Method	Resolution_Method		
z1D_ WorklogDetails	Work_Info_Summary		Required for creating work information
z1D_Activity_Type	Work_Info_Type		Optional for creating work information. Defaults to General Information if left null.
z1D_Secure_Log	Work_Info_Locked		Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_View_Access		Optional for creating work information. Defaults to Internal if left null.
z1D_Details	Work_Info_Notes		Optional for creating work information
z1D_ActivityDate_tab	Work_Info_Date		Optional for creating work information
z1D_CommunicationSource	Work_Info_Source		Optional for creating work information
Status_Reason	Status_Reason		
ServiceCI	ServiceCI		For more information about this element, see Associating entries with configuration items.

ServiceCI_ReconID	ServiceCI_ReconID		For more information about this element, see Associating entries with configuration items.
HPD_CI	HPD_CI		
HPD_CI_ReconID	HPD_CI_ReconID		
HPD_CI_FormName	HPD_CI_FormName		
z1D_CI_FormName	z1D_CI_FormName		

HelpDesk_Query_Service and HelpDesk_QueryList_Service functions

The following two functions are web service specific. To perform a search outside of web services, do it directly from the **HPD:Help Desk** form.

Input values

Web service field	Field value	Notes
Incident_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service and HelpDesk_GetWorkInfoList operation.

The following table lists the output values:

Output values

Web service field	Notes
Incident_Number	Returned only in the HelpDesk_QueryList_Service
Status	
Status_Reason	
Summary	
Notes	
Service_Type	
Reported_Source	
Impact	
Urgency	
Priority	
Priority_Weight	
First_Name	
Contact_Company	
Last_Name	
Middle_Initial	

VIP	
Contact_Sensitivity	
Phone_Number	
Internet_Email	
Company	
Organization	
Department	
Site	
Country	
Region	
City	
Site Group	
Assigned_Support_Company	
Assigned_Support_Organization	
Assigned_Support_Shift_Name	
Assigned_Group	
Assignee	
Product_Categorization_Tier_1	
Product_Categorization_Tier_2	
Product_Categorization_Tier_3	
Product_Name	
Product_Model_Version	
Manufacturer	
Categorization_Tier_1	
Categorization_Tier_2	
Categorization_Tier_3	
Closure_Product_Category_Tier1	
Closure_Product_Category_Tier2	
Closure_Product_Category_Tier3	
Closure_Product_Name	
Closure_Product_Model_Version	
Closure _Manufacturer	
Resolution	
Resolution_Category	
Resolution_Category_Tier_2	

Resolution_Category_Tier_3	
Closed_Date	
Estimated_Resolution_Date	
Reported_Date	
Required_Resolution_DateTime	
Submit_Date	
ServiceCI	For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items.
HPD_CI	
HPD_CI_ReconID	
HPD_CI_FormName	
z1D_CI_FormName	

HelpDesk_GetWorkInfoList function

The following table lists the values needed to retrieve a list of work info records for a list of incidents:

Input values

Web service field	Field value	Notes
Incident_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values:

Output values

Web service field	Notes
Incident_Number	Incident number that the work info belongs to
WorkInfoCommSource	
WorkInfoInstanceID	
WorkInfoNotes	
WorkInfoStatus	
WorkInfoSubmitDate	
WorkInfoSummary	
WorkInfoType	
WorkInfoAttachment1Data	Attachment Information
WorkInfoAttachment1Name	

WorkInfoAttachmetn1OrigSize	
WorkInfoAttachment2Data	
WorkInfoAttachment2Name	
WorkInfoAttachmetn2OrigSize	
WorkInfoAttachment3Data	
WorkInfoAttachment3Name	
WorkInfoAttachmetn3OrigSize	

GetListOfRelatedIncidents function

The following table lists the values needed to retrieve a list of related incidents:

Input values

Web service field	Field value	Notes
Incident_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values in addition to the output values mentioned in the **Output values** table in HelpDesk_Query_Service and HelpDesk_QueryList_Service functions:

Output values

Web service field	Notes
Association_Type01	The relationship type from the incident to its related record
Request_ID01	The ID of the record related to the incident
Request_Type01	The type of ticket related to the incident

Problem Management integrations

This topic describes the functions associated with the following Problem Management subsystems:

- Problem Investigation
- Known Error
- Solution Database

The following table provides a list of the available web services for each Problem Management subsystem:

Available web services

The following list displays the available web services for each subsystem.

Problem Investigation

- Problem_Submit_Service

- Problem_Modify_Service
- Problem_Query_Service and Problem_QueryList_Service
- GetListOfRelatedProblems function
- Problem _GetWorkInfoList function

Known Error

- KnownError_Submit_Service
- KnownError_Modify_Service
- KnownError_Query_Service and KnownError_QueryList_Service
- KnownError_GetWorkInfoList function
- GetListOfRelatedKnownErrors function

Solution Database

- Solution_Submit_Service
- Solution_Modify_Service
- Solution_AddKeyword_Service
- Solution_Query_Service and Solution_QueryList_Service

You can also add a work information entry at the time you create or modify any of these records. In the Solution module, you can also add keywords to a Solution record.

When using web services, you can query one, or a set of records from each sub-system.

⚠ **Note**
The mappings on the **PBM:ProblemInterface_Create** form are shared among the Problem Management sub-systems, and therefore you should be cautious about which keywords you send into the action field.

The following is a list of the web service functions available for Problem Management. These functions are described in the sections that follow.

- Submit (submit with work information, add a keyword in solution database)
- Modify (modify with work information, add a keyword in solution database)
- Query/Query List
- Add Keyword Service (Solution database sub-system only)

Problem investigation records

This topic describes how to:

- Make and modify problem investigation records
- Query a problem investigation
- Query a list of problem investigations

You submit Problem Investigation entries through the PBM:ProblemInterface_Create form.

See the following topics for detailed information about the individual services and functions:

- Problem_Submit_Service
- Problem_Modify_Service
- Problem_Query_Service and Problem_QueryList_Service functions
- GetListOfRelatedProblems function
- Problem _GetWorkInfoList function

Problem_Submit_Service

This interface form uses shared fields between Problem Investigation, Known Error, and Solution Database.

Successfully creating a Problem Investigation entry through web services returns the newly created Problem Investigation ID.

The following tables describe the values needed to create a Problem Investigation entry:

Required input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	PROBLEM	Keyword triggers workflow that initiates the submit operation
First Name	First_Name		
Last Name	Last_Name		
Description	Summary		
Status	Status		
Impact	Impact		
Urgency	Urgency		
Investigation Driver	Investigation_Driver		
Assigned Group Pblm Mgr	Problem_Coordinator_Assigned_Group		If Assignment engine is configured, you may not need to specify the Problem Coordinator values
Support Company Pblm Mgr	Problem_Coordinator_Support_Company		
Support Organization Pblm Mgr	Problem_Coordinator_Support_Organization		

The following table lists the optional input field values:

Optional input field values

DB field on interface form	Displayed on web services	Notes

Detailed Description	Notes	
Investigation Justification	Investigation_Justification	
Product Categorization Tier 1	Product_Categorization_ Tier_1	
Product Categorization Tier 2	Product_Categorization_ Tier_2	
Product Categorization Tier 3	Product_Categorization_ Tier_3	
Product Name	Product_Name	
Product Model/Version	Product_Model_Version	
Manufacturer	Manufacturer	
Temporary Workaround	Workaround	
Generic Categorization Tier 1	Generic_Categorization_ Tier_1	
Categorization Tier 1	Categorization_Tier_1	
Categorization Tier 2	Categorizaton_Tier_2	
Categorization Tier 3	Categorization_Tier_3	
Assigned Support Company	Problem_Manager_Support_ Company	
Assigned Support Organization	Problem_Manager_Support_ Organization	
Assigned Group	Problem_Manager_Assigned_Group	
z1D_WorklogDetails	Work_Info_Summary	Required for creating work information
z1D_Problem_Activity_Type	Work_Info_Type	Optional for creating work information, defaults to General Information if left null
z1D_Secure_Log	Work_Info_Locked	Optional for creating work information, defaults to No if left null
z1D_View_Access	Work_Info_View_Access	Optional for creating work information, defaults to Internal if left null
z1D_Details	Work_Info_Notes	Optional for creating work information
z1D_Activity_Date_tab	Work_Info_Date	Optional for creating work information
z1D_ CommunicationSource	Work_Info_Source	Optional for creating work information
Target Resolution Date	Target_Date	Target Date is required when Status is not at Draft stage
ServiceCI	ServiceCI	For more information about this element, see Associating entries with configuration items
ServiceCI_ReconID	ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items
PBM_CI_ReconID	PBM_CI_ReconID	

The following table lists the fields set by workflow:

Fields set by workflow

DB field on interface form	Notes
Sys-Problem Investigation ID	
Company	
Contact Company	
Requestor Company	
Support Organization Requester	
Support Group Name Requester	
Priority	
Priority Weight	
Requestor ID	
Problem Manager Login	
Site ID	
Site	
Region	
Site Group	
Phone Number Business	
Person ID	
Corporate ID	
Support Group ID Requester	
PBM Location Address	
PBM_CI	Set from PBM_CI_ReconID value
z1D_CI_FormName	Set from PBM_CI_ReconID value

Problem_Modify_Service

You search for, then modify, a specific problem using the problem investigation ID as the search criteria. Problem modifications are made through the **PBM:ProblemInterface** form.

> ⚠ **Note**
> When using web services, you must use the interface form to populate all fields mapped to the Problem Investigation form, otherwise a null value is sent, and the current values are overwritten.

Input field values

DB field on interface form	Displayed on web services	Field value	Notes

z1D_Action	Action	MODIFY	Keyword triggers workflow that initiates the modify operation
Problem Investigation ID	Problem_Investigation_ID		Used as the search criteria
Description	Summary		
Detailed_Description	Notes		Appears in Notes on the PBM: Problem Investigation form
Investigation Status	Investigation_Status		
Investigation Status Reason	Investigation_Status_ Reason		
Investigation Justification	Investigation_ Justification		
Investigation Driver	Investigation_Driver		
Impact	Impact		
Urgency	Urgency		
Product Categorization Tier 1	Product_ Categorization_Tier_1		
Product Categorization Tier 2	Product_ Categorization_Tier_2		
Product Categorization Tier 3	Product_ Categorization_Tier_3		
Product Name	Product_Name		
Product Model/Version	Product_Model_ Version		
Manufacturer	Manufacturer		
Categorization Tier 1	Categorization_Tier_1		
Categorization Tier 2	Categorization_Tier_2		
Categorization Tier 3	Categorization_Tier_3		
Generic Categorization Tier 1	Generic_ Categorization_Tier_1		
Temporary Workaround	Temporary_ Workaround		
z1D_WorklogDetails	Work_Info_Summary		Required for creating work information
z1D_Details	Work_Info_Notes		Optional for creating work information
z1D_Activity Type	Work_Info_Type		Optional for creating work information. Defaults to General Information if left null.
z1D_ActivityDate_ tab	Work_Info_Date		Optional for creating work information
z1D_ CommunicationSource	Work_Info_Source		Optional for creating work information

z1D_Secure_Log	Work_Info_Locked		Optional for creating work information. Defaults to No if left null.
Z1D_View_Access	Work_Info_View_ Access		Optional for creating work information. Defaults to Internal if left null.
ServiceCI	ServiceCI		For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	ServiceCI_ReconID		For more information about this element, see Associating entries with configuration items.
PBM_CI	PBM_CI		
PBM_CI_ReconID	PBM_CI_ReconID		
z1D_CI_FormName	z1D_CI_FormName		

Problem_Query_Service and Problem_QueryList_Service functions

Both of these functions are web service specific. To perform a search, do it directly from the **PBM:Problem Investigation** form.

Input values

Web service field	Field value	Notes
Problem_Investigation_ID		This is used only by the Problem_ Query_Service operation.
Qualification	AR System qualification	This is used only by the Problem_ QueryList_Service and Problem_ GetWorkInfoList operation.

The following table lists the output values:

Output values

Web service field	Notes
Problem_Investigation_ID	Returned only in the Problem_QueryList_Service operation
Investigation_Status	
Investigation_Status_Reason	
Investigation_Justification	
Investigation_Driver	
Summary	
Notes	
Impact	
Urgency	
Priority	
Priority_Weight	
First_Name	

Last_Name	
Company	
Contact_Company	
Region	
Site_Group	
Site	
Organization	
PBM_Location_Address	
Assigned_Support_Company	
Assigned_Support_Organization	
Assigned_Group	
Assignee	
Support_Group_Name_Requester	
Support_Organization_Requester	
Product_Categorization_Tier_1	
Product_Categorization_Tier_2	
Product_Categorization_Tier_3	
Product_Name	
Product_Model_Version	
Manufacturer	
Categorization_Tier_1	
Categorization_Tier_2	
Categorization_Tier_3	
Ceneric_Categorization_Tier_1	
Temporary_Workaround	
Target_Date	
ServiceCI	For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items.
PBM_CI	
PBM_CI_ReconID	
PBM_CI_FormName	
Problem_Coordinator_Support_Company	
Problem_Coordinator_Support_Organization	

Problem_Coordinator_Assigned_Group	
Problem_Coordinator	
Known_Error_Created_Date	
Estimated_Resolution_Date	
Last_Completed_Date	
Submit_Date	
Target_Resolution_Date	
Vendor_Responded_On	
Workaround_Determined_On	

GetListOfRelatedProblems function

The following table lists the values needed to retrieve a list of related problems:

Input values

Web service field	Field value	Notes
Problem_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values in addition to the output values mentioned in the **Output values** table in Problem_Query_Service and Problem_QueryList_Service functions:

Output values

Web service field	Notes
Association_Type01	The relationship type from the Problem to its related record
Request_ID01	The ID of the record related to the Problem
Request_Type01	The type of ticket related to the Problem

Problem _GetWorkInfoList function

The following table lists the values needed to retrieve a list of work info records for a list of problems:

Input values

Web service field	Field value	Notes
Problem_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values:

Output values

Web service field	Notes
ProblemInvestigationID	Problem ID that the work info belongs to
WorkInfoCommSource	
WorkInfoInstanceID	
WorkInfoNotes	
WorkInfoStatus	
WorkInfoSubmitDate	
WorkInfoSummary	
WorkInfoType	
WorkInfoAttachment1Data	Attachment Information
WorkInfoAttachment1Name	
WorkInfoAttachmetn1OrigSize	
WorkInfoAttachment2Data	
WorkInfoAttachment2Name	
WorkInfoAttachmetn2OrigSize	
WorkInfoAttachment3Data	
WorkInfoAttachment3Name	
WorkInfoAttachmetn3OrigSize	

Known Error records

This section describes how to make and modify known error records. It also describes how to create a work information entry when creating or modifying a Known Error record.

Successfully creating a Known Error entry through web services returns the newly created Known Error ID.

See the following topics for detailed information about the individual services and functions:

- KnownError_Submit_Service
- KnownError_Modify_Service
- KnownError_Query_Service and KnownError_QueryList_Service functions
- KnownError_GetWorkInfoList function
- GetListOfRelatedKnownErrors function

KnownError_Submit_Service

Known Error entries are submitted through the **PBM:ProblemInterface_Create** form.

> ⚠ **Note**
> This interface form uses shared fields between Problem Investigation, Known Error, and Solution Database.

The following tables describe the values needed to create a Known Error entry.

Required input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	KNOWNERROR	Keyword triggers workflow that initiates the submit operation
Known Error Status	Status		
Impact	Impact		
Urgency	Urgency		
Description	Summary		
Detailed Description	Notes		
View Access	View_Access		
Assigned Group Pblm Mgr	Problem_Coordinator_ Assigned_Group		If Assignment engine is configured, you may not need to specify the Problem Coordinator values
Support Company Pblm Mgr	Problem_Coordinator_Support_ Company		
Support Organization Pblm Mgr	Problem_Coordinator_Support_ Organization		
Target Resolution Date	Target_Date		

The following table lists optional input field values:

Optional input field values

DB field on interface form	Displayed on web services	Notes
Company	Company	
Searchable		
Category	Category	
Product Categorization Tier 1	Product_ Categorization_ Tier_1	
Product Categorization Tier 2	Product_ Categorization_ Tier_2	
Product Categorization Tier 3	Product_ Categorization_ Tier_3	
Product Name	Product_Name	

Product Model/Version	Product_Model_ Version	
Manufacturer	Manufacturer	
Categorization Tier 1	Categorization_ Tier_1	
Categorization Tier 2	Categorization_ Tier_2	
Categorization Tier 3	Categorization_ Tier_3	
Generic Categorization Tier 1	Generic_ Categorization_ Tier_1	
Temporary Workaround	Temporary_ Workaround	
Resolution	Resolution	
Assigned Support Company	Assigned_Support_ Company	
Assigned Support Organization	Assigned_Support_ Organization	
Assigned Group	Assigned_Group	
Assignee	Assignee	
z1D_WorklogDetails	Work_Info_Summary	Required for creating work information
z1D_Activity Type	Work_Info_Type	Optional for creating work information. Defaults to General Information if left null.
z1D_Secure_Log	Work_Info_Locked	Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_View_ Access	Optional for creating work information. Defaults to Internal if left null.
z1D_Details	Work_Info_Notes	Optional for creating work information
Z1D_ActivityDate_ tab	Work_Info_Date	Optional for creating work information
z1D_ CommunicationSource	Work_Info_Source	Optional for creating work information
ServiceCI	ServiceCI	For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items.
PBM_CI_ReconID	PBM_CI_ReconID	

The following table lists fields set through workflow:

Fields set through workflow

DB field on interface form	Notes
Known Error ID	
Priority	
Priority Weight	

PBM_CI	Set from PBM_CI_ReconID value
z1D_CI_FormName	Set from PBM_CI_ReconID value

KnownError_Modify_Service

Known Error modifications are done through the **PBM:KnownErrorInterface** form. To search for and then modify a specific Known Error, use the Known Error ID as the search criteria.

When using web services, all fields mapped with values on the Known Error form must be populated by the interface form, otherwise a null value is sent and the current values are overwritten.

Input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	MODIFY	Keyword triggers workflow that initiates the modify operation
Known Error ID	Known_Error_ID		
Know Error Status	Known_Error_Status		
Status_Reason	Status_Reason		
Description	Summary		
Detailed Description	Notes		
Impact	Impact		
Urgency	Urgency		
View Access	View_Access		
Searchable	Searchable		
Category	Category		
Company	Company		
Product Categorization Tier 1	Product_ Categorization_Tier_1		
Product Categorization Tier 2	Product_ Categorization_Tier_2		
Product Categorization Tier 3	Product_ Categorization_Tier_3		
Product Name	Product_Name		
Product Model/Version	Product_Model_ Version		
Manufacturer	Manufacturer		
Categorization Tier 1	Categorization_Tier_1		
Categorization Tier 2	Categorization_Tier_2		
Categorization Tier 3	Categorization_Tier_3		

Generic Categorization Tier 1	Generic_ Categorization_ Tier_1		
Temporary Workaround	Temporary_ Workaround		
Resolution	Resolution		
Assigned Support Company	Assigned_ Support_Company		
Assigned Support Organization	Assigned_ Support_ Organization		
Assigned Group	Assigned_Group		
Assignee	Assignee		
z1D_ WorklogDetails	Work_Info_ Summary		Required for creating work information
z1D_Details	Work_Info_Notes		Optional for creating work information
z1D_Activity Type	Work_Info_Type		Optional for creating work information. Defaults to General Information if left null.
z1D_ActivityDate_tab	Work_Info_Date		Optional for creating work information
z1D_CommunicationSource	Work_Info_ Source		Optional for creating work information
z1D_Secure_Log	Work_Info_ Locked		Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_ View_Access		Optional for creating work information. Defaults to Internal if left null.
ServiceCI	ServiceCI		For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	ServiceCI_ReconID		For more information about this element, see Associating entries with configuration items.
PBM_CI	PBM_CI		
PBM_CI_ReconID	PBM_CI_ReconID		
z1D_CI_FormName	z1D_CI_FormName		

KnownError_Query_Service and KnownError_QueryList_Service functions

These two functions are web service specific. To perform a search outside of web services, use the **PBM:Known Error** form.

Input values

Web service field	Field value	Notes
Known_Error_ID		This is used only in the KnownError_Query_Service Operation.
Qualification	AR System qualification	This is only used in the KnownError_QueryList_Service and KnownError_GetWorkInfoList operation.

The following table lists the output values:

Output values

Web service field	Notes
Known_Error_ID	Returned only in the KnownError_QueryList_Service operation
Summary	
Notes	
Known_Error_Status	
Status_Reason	
Impact	
Urgency	
Priority	
Priority_Weight	
Searchable	
Category	
View_Access	
Company	
Product_Categorization_Tier_1	
Product_Categorization_Tier_2	
Product_Categorization_Tier_3	
Product_Name	
Product_Model_Version	
Manufacturer	
Categorization_Tier_1	
Categorization_Tier_2	
Categorization_Tier_3	
Generic_Categorization_Tier_1	
Temporary_Workaround	
Resolution	
Assigned_Support_Company	
Assigned_Support_Organization	
Assigned_Group	
Assignee	
Support_Company_Pblm_Mgr	
Support_Organization_Pblm_Mgr	

Target_Date	
ServiceCI	For more information about this element, see Associating entries with configuration items.
ServiceCI_ReconID	For more information about this element, see Associating entries with configuration items.
PBM_CI	
PBM_CI_ReconID	
PBM_CI_FormName	
Problem_Coordinator_Support_Company	
Problem_Coordinator_Support_Organization	
Problem_Coordinator_Assigned_Group	
Problem_Coordinator	
Corrective_Action_Determined	
Last_Corrected_Date	
Submit_Date	
Target_Resolution_Date	
Vendor_Responded_On	
Workaround_Determined_On	

KnownError_GetWorkInfoList function

The following table lists the values needed to retrieve a list of work info records for a list of Known Errors:

Input values

Web service field	Field value	Notes
Problem_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values:

Output values

Web service field	Notes
KnownErrorID	Known Error ID that the work info belongs to
WorkInfoCommSource	
WorkInfoInstanceID	
WorkInfoNotes	
WorkInfoStatus	
WorkInfoSubmitDate	

WorkInfoSummary	
WorkInfoType	
WorkInfoAttachment1Data	Attachment Information
WorkInfoAttachment1Name	
WorkInfoAttachmetn1OrigSize	
WorkInfoAttachment2Data	
WorkInfoAttachment2Name	
WorkInfoAttachmetn2OrigSize	
WorkInfoAttachment3Data	
WorkInfoAttachment3Name	
WorkInfoAttachmetn3OrigSize	

GetListOfRelatedKnownErrors function

The following table lists the values needed to retrieve a list of related Known Errors:

Input values

Web service field	Field value	Notes
Problem_Number		This is used only by the HelpDesk_Query_Service operation.
Qualification	AR System qualification	This is used only by the HelpDesk_QueryList_ Service operation.

The following table lists the output values in addition to the output values mentioned in "Output values" in KnownError_Query_Service and KnownError_QueryList_Service functions:

Output values

Web service field	Notes
Association_Type01	The relationship type from the Known Error to its related record
Request_ID01	The ID of the record related to the Known Error
Request_Type01	The type of ticket related to the Known Error

Solution Database records

This topic describes how to make and modify Solution Database records. It also describes how to query and add key words to a solution database.

Successfully creating a Solution Database entry through web services returns the newly created Solution Database ID.

See the following topics for detailed information about the individual services and functions:

- Solution_Submit_Service
- Solution_Modify_Service

- Solution_AddKeyword_Service
- Solution_Query_Service and Solution_QueryList_Service functions

Solution_Submit_Service

You submit Solution Database entries through the **PBM:ProblemInterface_Create** form.

> ⚠ **Note**
> This interface form uses shared fields between Problem Investigation, Known Error, and Solution Database.

The following tables describe the values needed to create a Solution Database entry.

Required input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	SOLUTION	Keyword triggers workflow that initiates the submit operation
Solution Status	Solution_Status		
Solution Description	Summary		
Description	Abstract		This appears as Abstract on the Solution form.
Solution	Solution		
View Access	View_Access		
Company	Company		
Contact Company	Contact_Company		

The following table lists the optional input field values:

Optional input field values

DB field on interface form	Displayed on web services	Notes
Status_Reason	Status_Reason	
Searchable	Searchable	
Solution_Type	Solution_Type	
Contact Company	Contact_Company	
Organization	Organization	
Department	Department	
Site Group	Site_Group	
Site	Site	
Region	Region	

Product Categorization Tier 1	Product_ Categorization_Tier_1	
Product Categorization Tier 2	Product_ Categorization_Tier_2	
Product Categorization Tier 3	Product_ Categorization_Tier_3	
Product Name	Product_Name	
Product Model/Version	Product_Model_Version	
Manufacturer	Manufacturer	
Categorization Tier 1	Categorization_Tier_1	
Categorization Tier 2	Categorization_Tier_2	
Categorization Tier 3	Categorization_Tier_3	
Assigned Support Company	Assigned_Support_ Company	
Assigned Support Organization	Assigned_Support_ Organization	
Assigned Group	Assigned_Group	
z1D Solution Keyword	Solution_Keyword	Starts workflow to create a keyword for the new solution record
z1D_ WorklogDetails	Work_Info_Summary	Required for creating work information
z1D_Details	Work_Info_Notes	Optional for creating work information
z1D_Solution_ Activity_Type	Work_Info_Type	Optional for creating work information. Defaults to General Information if left null.
z1D_ActivityDate_tab	Work_Info_Date	Optional for creating work information
z1D_ Communication_ Source	Work_Info_Source	Optional for creating work information
z1D_Secure_Log	Work_Info_Locked	Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_View_Access	Optional for creating work information. Defaults to Internal if left null.

Fields set by workflow

DB field on interface form	Notes
Solution Database ID	
Support Group ID	Only set if Assigned, Support Company, Organization, and Group are not null

Solution_Modify_Service

You make modifications through the **PBM:SolutionInterface** form. To find, then modify a specific solution, use the Solution Database ID as the search criteria.

⚠ **Note**
When using web services, you must use the interface form to populate all fields mapped to the Solution Database form, otherwise a null value is sent, and the current values are overwritten.

Input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	MODIFY	Keyword triggers workflow that initiates the modify operation
	Solution_Database_ID		This is a search qualification.
Solution Status	Solution_Status		
Status_Reason	Status_Reason		
Solution Description	Solution_Summary		
Abstract	Abstract		
Solution	Solution		
View Access	View_Access		
Searchable	Searchable		
Solution_Type	Solution_Type		
Company	Company		
Contact Company	Contact_Company		
Department	Department		
Organization	Organization		
Region	Region		
Site Group	Site_Group		
Site	Site		
Product Categorization Tier 1	Product_Categorization_Tier_1		
Product Categorization Tier 2	Product_Categorization_Tier_2		
Product Categorization Tier 3	Product_Categorization_Tier_3		
Product Name	Product_Name		
Product Model/Version	Product_Model_Version		
Manufacturer	Manufacturer		
Categorization Tier 1	Categorization_Tier_1		
Categorization Tier 2	Categorization_Tier_2		
Categorization Tier 3	Categorization_Tier_3		

Assigned Support Company	Assigned_Support_ Company		
Assigned Support Organization	Assigned_Support_ Organization		
Assigned Group	Assigned_Group		
Assignee	Assignee		
z1D Solution Keyword	Solution_Keyword		Used to create a keyword for the newly created solution record
z1D_Worklog_Details	Work_Info_Summary		Required for creating work information
z1D_Details	Work_Info_Notes		Optional for creating work information
z1D_Activity_Type	Work_Info_Type		Optional for creating work information. Defaults to General Information if left null.
z1D_ActicityDate_tab	Work_Info_Date		Optional for creating work information
z1D_CommunicationSource	Work_Info_Source		Optional for creating work information
z1D_Secure_Log	Work_Info_Locked		Optional for creating work information. Defaults to No if left null.
z1D_View_Access	Work_Info_View_Access		Optional for creating work information. Defaults to Internal if left null.

Solution_AddKeyword_Service

This function adds a keyword to the specified solution entry. Use a keyword when you want to search the database for a solution entry with a particular subject.

Input field values

DB field on interface form	Displayed on web services	Field value	Notes
z1D_Action	Action	ADDKEYWORD	Keyword triggers workflow that initiates the add keyword operation
Solution Database ID	Solution_Database_ID		
z1D Solution Keyword	Solution_Keyword		

Solution_Query_Service and Solution_QueryList_Service functions

These two functions are web service specific. To perform a search outside of web services, use the **PBM:Solution Database** form.

Input values

Web service field	Field value	Notes
Solution_Database_ID		This field is used only in the Solution_Query_Service operation.

Qualification	AR System qualification	This field is used only in the Solution_QueryList_Service operation.

The following table lists the output values:

Output values

Web service field	Notes
Solution_Database_ID	Returned only in the Solution_QueryList_Service operation
Solution_Summary	
Solution_Status	
Solution_Type	
Searchable	
View_Access	
Abstract	
Solution	
Company	
Contact_Company	
Organization	
Department	
Region	
Site_Group	
Site	
Product_Categorization_Tier_1	
Product_Categorization_Tier_2	
Product_Categorization_Tier_3	
Product_Name	
Product_Model_Version	
Manufacturer	
Categorization_Tier_1	
Categorization_Tier_2	
Categorization_Tier_3	
Assigned_Support_ Company	
Assigned_Support_ Organization	
Assigned_Group	
Assignee	

Troubleshooting

This section provides the following troubleshooting information:

- Troubleshooting service requests with errors
- Troubleshooting email record creation and updates
- BMC Remedy AR System messages

Incident and Problem Processes community

Another valuable source of troubleshooting information is the BMC community for Incident and Problem Processes. Here, you can view discussions and other documents related to BMC Service Desk. Registered members of the community can take part in on-going discussions or start new discussions where they can ask questions, seek advice, or share information.

To register as a member

1. Go to https://communities.bmc.com/communities/community/bmcdn/bmc_it_service_support/incident_and_problem_
   .
   The Incident and Problem Processes community page opens.
2. At the top of the page, click **Register**.
3. Follow the on-screen instructions.

Troubleshooting service requests with errors

If the service request cannot be completed because of an error from BMC Change Management or Incident Management, you can view which service requests contain errors and review the event log to troubleshoot the service request.

> **Note**
> To see service requests with errors, you need Command Event Master permissions in addition to Requester console Master permissions.

To view requests with errors

1. From the Navigation pane of the Requester console, choose **Request Errors > View Requests with Errors**.
2. Click the **Change/Incident Data** tab.
3. Click **Reset Error** to restart the service request.
   Users can now continue to work on the service request.
4. Click **View Events** to review the event log and troubleshoot the service request.
5. View the event details:
   - Protocol
   - Access Mode
   - Error Code
   - Error Message

6. Take any of the following actions for events that are in error:
   - Retry
     It is best to retry each event in the order the events are generated. By default, the event table is sorted with the recent event on top, in reverse chronological order. Typically events should be retried when the problem indicated by the error message has been fixed.
   - Ignore

> **Warning**
> Delete service requests with caution. They cannot be recovered. You must have BMC Remedy AR System administrator permissions to delete service request records.

Troubleshooting email record creation and updates

This topic describes how to troubleshoot email record creation and updates and includes information about:

- Messages tab overview
- Before you begin
- To troubleshoot by using the Messages tab
- Related topics

The Messages tab on the Inbound Email Rule Configuration form provides you with a tool to help you troubleshoot incidents with the email service requests capability.

Messages tab overview

The table on the left of the Messages tab contains a list of the email messages that were received for processing. You can filter the email messages table to show only messages that were created today (the default setting) or to show all messages created in the last seven days. The **Show Messages** radio buttons at the top of the tab control this filter. From this table, you can see the message's status (New, Done, or Error).

The table on the right of the tab has additional information about the message selected in the table, including a summary of its To, From, and Subject fields. This table also tells you when the message was created, shows the system-generated, unique ID of the message, and indicates the name of the rule, or use case, that the Email Rule Engine ran.

To see more information about the selected message, click **Transaction**. If the use case triggered by the message ran successfully, you can also view the record that it created. Click **View Request** and use the links at the bottom of the tab.

Before you begin

To perform the following procedure, you must have system administrator and Email Rule Config permissions (Email Rule Config is a Foundation related permission).

You must also have permissions to view incident requests, problem investigations, known errors, work orders, and tasks so that you can use the troubleshooting tools. For information about specific BMC Service Desk permissions, see Incident Management permissions and Problem Management permissions. For information about BMC Service Request Management permissions, see User permissions.

To troubleshoot by using the Messages tab

1. From the **Application** list on the left side of the IT Home page, select **Administrator Console > Application**

Administration Console > Custom Configuration > Foundation > Email Engine Rules > Configure Rules.

2. In **Company** at the top of the form, select the company for which you are troubleshooting messages.
3. Click the **Messages** tab.

> ⚠ **Note**
> When the Messages tab opens, it is filtered by **Created Today** by default. To see messages that were created before today but no more than seven days ago, click **Last 7 Days** at the top of the tab.

4. In the table on the left of the tab, select the message that you are troubleshooting.
5. Click one of the following buttons:
    - **Transaction** — To see details of the email transaction if the transaction failed and you need to investigate the reason
    - **View Request** — To see the record created by the transaction

Related topics

- Record creation and updates by email
- Configuring the Email Rule Engine

BMC Remedy AR System messages

For information about BMC Remedy AR System error and warning messages and notes, see Working with error messages in the BMC Remedy AR System documentation.

Known issues and workarounds

This section describes the known issues that are associated with the BMC Service Desk application.

The following known issues relate to the BMC Service Desk documentation:

Tracking number	Description
None	The product documentation has been updated since the online help for BMC Service Desk was created. For the latest version of the documentation, refer to this BMC Service Desk online technical documentation.

Known issues for browsers

> ℹ **Recommendation**
> Use Mozilla Firefox instead of Microsoft Internet Explorer to access the documentation.

This following table describes known issues that are associated with browsers.

Issue	Workaround

When viewing the documentation portal in Internet Explorer 8, you cannot expand a graphic thumbnail by clicking it.	1. Go to **Tools > Compatibility View Settings**. 2. Clear the **Display intranet sites in Compatibility View** check box and then click **Close**. 3. In the topic, click the graphic thumbnail.
When viewing the documentation portal in Internet Explorer 8, you have trouble posting comments on a page.	1. On the page, click **Add Comment**. 2. Although you cannot type in your comment, click **Post**. You receive an error message that you cannot post an empty comment, but you now have a comment box. 3. Enter your comment and click **Post**.

Support information

This topic contains information about how to contact Customer Support and the support status for this and other releases.

Contacting Customer Support

If you have problems with or questions about a BMC product, or for the latest support policies, see the Customer Support website at http://www.bmc.com/support. You can access product documents, search the Knowledge Base for help with an issue, and download products and maintenance. If you do not have access to the web and you are in the United States or Canada, contact Customer Support at 800 537 1813. Outside the United States or Canada, contact your local BMC office or agent.

Support status

Based on the support policy adopted September 1, 2011, for releases from that date forward, BMC provides technical support for a product based on time rather than number of releases. The previous release-based policy applies to releases before September 1, 2011. To view the support status for this release, see the BMC Service Desk Application support page.

Additional resources

The following BMC sites provide information outside of the BMC Service Desk documentation that you might find helpful:

- BMC Service Desk, BMC Communities
- BMC Customer Support, BMC Communities
- BMC Support Knowledge Base, filter your searches using Incident Management or Problem Management in your search term
- BMC Service Desk learning path, BMC Educational Services

- BMC Service Desk offerings, high level product information
- BMC Remedy IT Service Management suite, high level product information
- Documentation for related products:
    - BMC Asset Management
    - BMC Atrium Core
    - BMC Change Management
    - BMC IT Service Management Suite
    - BMC Knowledge Management
    - BMC Remedy AR System Server
    - BMC Service Level Management
    - BMC Service Request Management

Legal notices

The information included in this documentation is the proprietary and confidential information of BMC Software, Inc., its affiliates, or licensors. Your use of this information is subject to the terms and conditions of the applicable End User License agreement for the product and to the proprietary and restricted rights notices included in the product documentation.

BMC Software Inc.
2101 CityWest Blvd, Houston TX 77042-2827, USA
713 918 8800
Customer Support: 800 537 1813 (United States and Canada) or contact your local support center