



SERENA®

SERVICE MANAGER

User's Guide

Serena Proprietary and Confidential Information

Copyright © 2011 Serena Software, Inc. All rights reserved.

This document, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by such license, no part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Serena. Any reproduction of such software product user documentation, regardless of whether the documentation is reproduced in whole or in part, must be accompanied by this copyright statement in its entirety, without modification. This document contains proprietary and confidential information, and no reproduction or dissemination of any information contained herein is allowed without the express permission of Serena Software.

The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Serena. Serena assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Trademarks

Serena, TeamTrack, StarTool, PVCS, Collage, Comparex, Dimensions, Serena Dimensions, Mashup Composer, Mashup Exchange, Prototype Composer, Mariner, and ChangeMan are registered trademarks of Serena Software, Inc. The Serena logo, Version Manager, Meritage, and Mover are trademarks of Serena Software, Inc. All other products or company names are used for identification purposes only, and may be trademarks of their respective owners.

U.S. Government Rights

Any Software product acquired by Licensee under this Agreement for or on behalf of the U.S. Government, its agencies and instrumentalities is "commercial software" as defined by the FAR. Use, duplication, and disclosure by the U.S. Government is subject to the restrictions set forth in the license under which the Software was acquired. The manufacturer is Serena Software, Inc., 1900 Seaport Boulevard, 2nd Floor, Redwood City, CA 94063-5587.

Part number: Serena Service Manager Product version: 2.0

Publication date: 2011-07-27

Table of Contents

Chapter 1: What's New in Serena Service Manager 2.0.0?	7
Chapter 2: Overview	11
Process Apps Overview	11
General Features	12
State Forms	13
Transition Forms	14
Urgency, Impact, and Priority	15
Chapter 3: Request Center	19
Request Center Overview	19
Service Catalog	20
Requests View	20
Knowledge Center	22
Configuring Request Center	23
About the Image Picker	27
Chapter 4: Incident Management	29
Incident Management Overview	29
1. Incident Creation.....	30
2. Incident Classification and Initial Support	31
3. Incident Investigation and Diagnosis	33
4. Incident Resolution and Closure	34
5. Incident Monitoring and Communication	35
6. Incident Reporting	36
Incident Management Workflow	36
Incident Management Dashboard	37
Satisfaction Dashboard	39
Incident Management Roles	40
Chapter 5: Request Fulfillment	43
Request Fulfillment Overview	43
1. Request Creation.....	44

2. Request Classification and Initial Support	45
3. Request Approvals	45
4. Request Resolution and Closure	46
5. Request Monitoring and Communication	47
Request Fulfilment Roles	47
Request Fulfillment Workflow	48
Chapter 6: Problem Management	51
Problem Management Overview	51
1. Problem Creation.....	52
2. Problem Classification	53
3. Problem Investigation and Diagnosis	53
4. Problem Error Assessment	54
5. Known Errors	54
6. Problem Resolution.....	54
Problem Management Workflow	55
Problem Management Dashboard	56
Problem Management Roles.....	57
Chapter 7: Change Management	59
Change Management Overview	59
1. RFC Creation	59
2. RFC Classification	60
3. RFC Assessment	61
Risk Analysis Calculator	62
4. RFC Authorization	65
5. RFC Implementation	66
6. RFC Review and Closure	67
Change Management Workflow	67
Change Management Dashboard	68
Risk Dashboard	69
Change Management Roles	70

Chapter 8: Configuration Management System	73
Configuration Management Overview	73
1. Configuration Identification	73
About Relationships	75
Creating CIs from Events	76
2. Configuration Control	77
Understanding Baselines	78
3. Audit and Verification	79
4. Status Accounting	79
CMS Workflow	81
CMS Dashboard	81
CMS Roles	82
Chapter 9: Knowledge Management.....	85
Knowledge Management Roles	86
Working with Articles from the User Workspace	86
Creating Announcements and Articles	87
Reviewing Articles	91
Publishing Knowledge Center Articles	92
Working with Articles from Request Center	92
Viewing and Commenting on Articles	92
Updating Knowledge Center Articles	93
Deleting Knowledge Center Articles	94
Knowledge Management Workflow	94
Knowledge Management Dashboard	95
Chapter 10: Additional Information	97
Adding Auxiliary Data	97
Modifying Process Apps	98
Managing Users	98
Enabling Notifications	99
Integrations Between Applications	100
Additional ITIL References	101

Chapter 1: What's New in Serena Service Manager 2.0.0?

The following features and changes are new in Service Manager.

Request Center

Request Center is the new portal for Service Manager end users. Through Request Center, end users can access important and pertinent information quickly, without having to learn to navigate the User Workspace.

Request Center provides the ability to browse the service catalog, view submitted requests, and search for Knowledge Center articles. From the service catalog, users can submit requests into applications or access specific URLs as determined by the IT Administrator. The Requests view allows end users to view items that they have submitted, alerting them if any item requires action such as adding information. Request Center allows users access to articles within Knowledge Center.

For more information, see [Chapter 3: Request Center \[page 19\]](#).

Knowledge Center

Knowledge Center is a new knowledge base feature included with Service Manager. Users access Knowledge Center through the Request Center portal, including receiving IT announcements and searching Knowledge Center articles.

Knowledge Center announcements appear to all users in the announcements bar when they log in to Request Center. These announcements alert users to important IT events, such as possible outages. Announcements reduce the number of service requests since the alert may answer common questions that end users have.

End users can also become self-sufficient by accessing the articles within Knowledge Center. From the Knowledge Center view in Request Center, users can search the Knowledge Center for related articles. Users can then comment and rate the articles that they find, giving IT feedback on which articles are being consumed and which articles may need to be rewritten for clarity.

Both the Knowledge Center articles and announcements are managed with the Knowledge Management process app.

For more information, see [Knowledge Center \[page 22\]](#).

Knowledge Management

The new Knowledge Management process app manages your Knowledge Center articles and announcements.

The Knowledge Management workflow lets you track new knowledge base articles as they receive the necessary approvals before being published for public viewing. This process ensures that items receive the appropriate reviews before being seen by end users. If an existing article requires edits, these edits receive the same scrutiny as they progress through the same Knowledge Management workflow.

Knowledge Management also provides the ability for IT departments to create announcements that appear to end users in Request Center. The announcements are used for important notices that will only apply for a limited time, after which they are automatically removed from the display.

For more information, see [Chapter 9: Knowledge Management \[page 85\]](#).

Request Fulfillment

Request Fulfillment is a new Service Manager process app for managing service requests. Service requests are a request for a service to be provided, such as a request for a new laptop or a request for information. Service requests differ from incidents, because they are not accompanied by a service interruption.

Service requests may be entered by users directly or they may be spawned from an incident. For example, a user may open an incident because applications are not responding. Upon investigation, IT finds that a user's machine has run out of disk space, so IT opens a service request to add a new hard drive to the user's machine.

Requests that an end user submits can be accessed from the Requests view within Request Center. Users can add any additional information necessary to the request directly from Request Center.

For more information on the Request Fulfillment process app, see [Chapter 5: Request Fulfillment \[page 43\]](#).

Risk Calculator

The Change Management application now includes the Risk Analysis calculator. The Risk Analysis calculator includes a risk survey form, where information is gathered about the extent of the risk this change poses. Based on the responses to the survey, the inherent risk is calculated for the change. The Risk Calculator survey is easily modified to meet your company's risk model. The calculated risk appears on the **Risks** tab when viewing a change.

The Risk dashboard uses the results in the Risk Calculator to help change management staff monitor the risk of upcoming changes. The dashboard includes a report that shows the ratio of RFCs that have completed surveys compared to those that do not.

For more information, see [Risk Analysis Calculator \[page 62\]](#).

Solution Files

The Service Manager solution is now delivered as solution files that are imported and promoted using SBM Application Administrator. The new solution file delivery method allows all components of the solution, such as notifications and reports, to be included when you import and promote the solution.

Previous versions of Service Manager required that on-premise installations start with the sample database provided with Service Manager. The sample database was the only way to receive the reports and notifications included with Service Manager.

For more information, see *Serena Service Manager Installation and Configuration Guide*.

2009 R4.02 Enhanced Functionality

The following features which were made available in Serena Business Manager R4.02 are incorporated in this new release of Service Manager:

-
- The Application Names have been changed in SBM Composer. The names now have an **SSM** prefix. This prevents possible naming collisions with existing applications. This change will not affect upgrades to existing installations, because the internal ID remains the same.
 - The transition buttons that appear on transition and state forms have been updated to make use of the **transition control** feature. The transition buttons in Service Manager are no longer unique images. The button text is now automatically updated when you modify the transition name within SBM Composer.
 - The ability to add and edit relationships has been updated to use the **Editable Grid**, which allows users to submit or modify relationships in a grid layout directly from the **Relationships** tab.
 - The **Post Problem** and **Merge Incident** transitions in Incident Management have been implemented using an *Any to Any* transition with decision nodes.
 - Embedded reports and the Relationship Explorer have been changed to make use of the sub-relational IDs. These IDs eliminated the need for orchestrations which monitored changes to the auxiliary tables and then updated a field within the primary table with a new auxiliary item IDs when new auxiliary items were added. Both the orchestrations and fields have been removed from the solution.

Chapter 2: Overview

This chapter gives an overview of the Serena Service Manager and how the different pieces work together to meet ITIL standards.

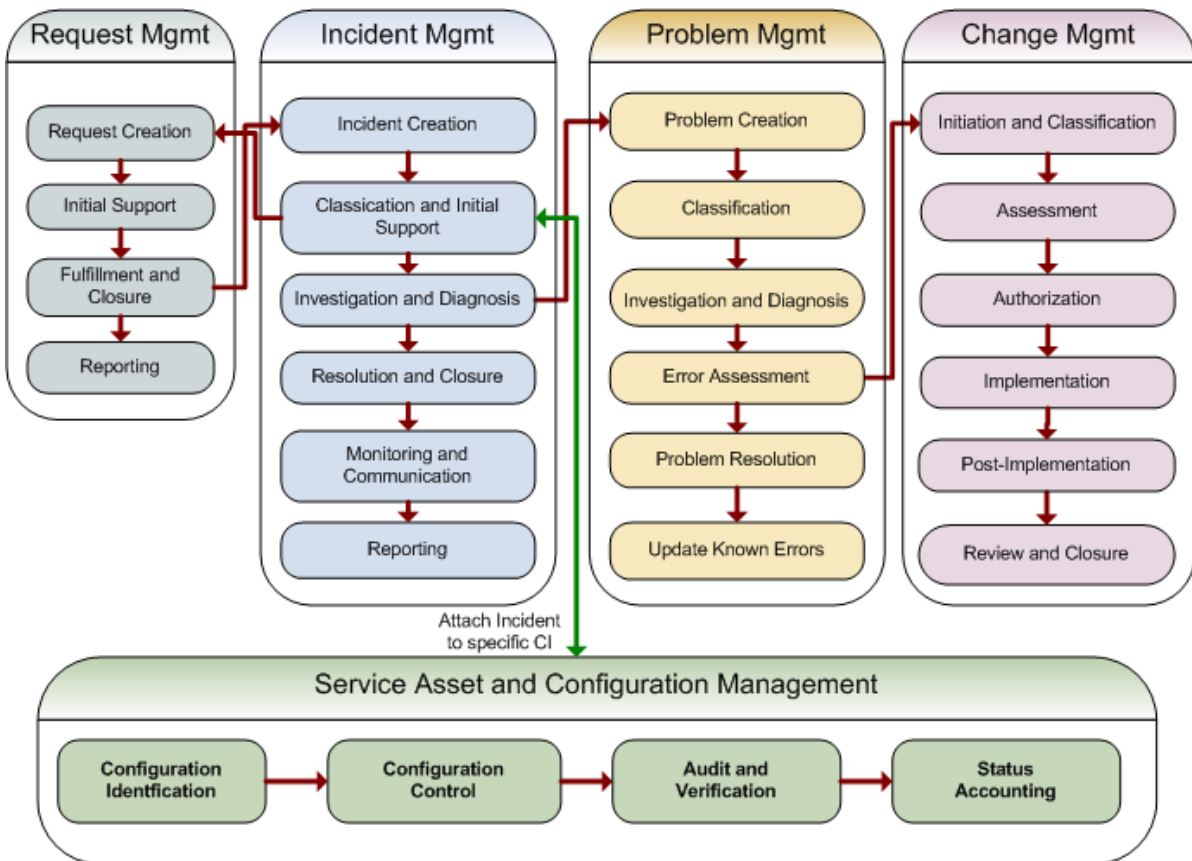
- [Process Apps Overview \[page 11\]](#)

Process Apps Overview

The Serena Service Manager is composed of the following process components:

- **Request Fulfillment**, which addresses service requests from users by providing a request channel, gathering or supplying information, and fulfilling the request.
- **Incident Management**, which focuses on restoring normal service operations as quickly as possible to minimize the impact of incidents on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.
- **Problem Management**, which analyzes the root cause of incidents, prevents their recurrence, and limits the impact of problems that cannot be prevented. Problem management includes the **Workarounds** auxiliary table, where information on workarounds is stored.
- **Change Management**, which helps ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure. This minimizes the number and impact of any related incidents upon service after changes are implemented.
- **Configuration Management System (CMS)**, which oversees the life of the Configuration Items (CIs) through enabling the fundamental elements of identification, change management, status accounting, and audits. The CMS is composed of three pieces, the **CMS** where all CIs are stored, the **CMS Baselines** workflow where all of the CI baselines are processed, and the **Relationships** auxiliary table where the relationships between CIs, RFCs, Problems, and Incidents are stored.

Here is a graphical representation of the different process components and how they work together:



A typical integration flow is as follows:

1. *Configuration Items (CI)* are entered in the Configuration Management System and stored in the CMS. Baselines of CIs are stored in the CMS Baselines project.
2. End users or Service Desk staff submit an *incident*, choosing the **Affected CI** for the incident, which creates a link between the incident and the CI.
3. If the incident needs to be escalated for root cause analysis, a *problem* is submitted based on the incident.
4. Problems can lead to entries in the *Known Errors* table, documenting workarounds for problems, and resolutions to Known Errors.
5. Problems can lead to the creation of a Request for Change (RFC), which is an investigation into possible changes to the IT infrastructure.
6. An RFC may require an update to a CI and a new CI baseline.

General Features

The following topics describe the general features and settings available in the Serena Service Manager.

These features apply to all of the processes: CMS, Incident Management, Problem Management, and Change Management. For information on specific process apps, refer to [Chapter 10: Additional Information \[page 97\]](#).

Role Based Access

For each management process, administrators can map functional and access privileges to users by assigning the appropriate roles.

Access to items and data are controlled by roles. Roles can grant read-only access to one group and update privileges to another. Data attributes can also be classified, and access to each data classification granted by role.

Functional privileges include access and ownership over the workflow. The ability to transition problems from one state to another is also controlled by the role privileges. Furthermore, owners are assigned to each active state in a workflow.

Roles are customizable, allowing you to tailor the roles to your installation.

Workflow Rules

Workflow rules determine how an item should progress through the workflow, and if certain criteria must be met before an action can be performed. These actions can be performed automatically.

For example, workflow rules can be established to ensure that a CI has valid data. If these conditions are not met, an automated action can be launched on the item, such as preventing the item from being transitioned to the next state.

Audit Trails

Serena Service Manager includes the complete tracking functionality of SBM, which enables you to track changes to every item. Each item is assigned a unique identifier after it is created in Serena Service Manager. Every activity is recorded, including field updates, transitions, and relationships, as the item moves through the workflow.

You can access this information through viewing the Change History of the item or from running reports to gather information about the item. This data provides an audit trail for the item throughout its lifecycle, and you can use this data to improve your processes.

Auxiliary Tables

Multiple auxiliary tables are included which contain values that are used by selection fields. The values for these fields can be easily modified from SBM User Workspace by modifying the auxiliary tables.

State Forms

State forms are displayed when an item is in a state. They are designed with the following features to give visual indicators of the status of the item and of the important information.

The screenshot displays a service manager interface for an incident. The title bar shows the incident ID and title: "FIX_001539: Network OS on most Router/switches failed after applying patch overnight". The interface is divided into several sections:

- Left Sidebar:** Contains a state icon (1), a list of transition buttons (2) including "Resolve", "Escalate - L3", "Post Problem", "Post RFC", "update", "copy incident", "post new incident", and "delete", and incident details (3) such as "Incident Number: FIX_001539", "Incident Type: Break Fix", "Urgency: Medium", "Impact: Single User", "Priority: 4", and "Incident Operator: Karl Malone".
- Right Sidebar:** Includes a "Back to Results" link, an "Actions" menu (5), and sections for "Categorization" (Configuration Item, Incident Category, Incident Sub-Category, Incident Sub-Category Type, Symptom Code) and "Contacts" (Reported By: Latrel Sprewell, Affected User, Additional Contact(s)).
- Bottom Section:** Shows "Incident Operator" details, with "Level 2 Technician" highlighted in yellow (4), listing "Karl Malone" and "Tim Hardaway".

1. The item's title appears along the top of the item. Item backgrounds are colored based on the process app that you are in.
2. The state icon gives users a visual cue of where the item is in the workflow. The icon is added using unique forms for each state and adding the icon image to the form.
3. Primary transition buttons are enlarged to display to users the usual path through the workflow. Secondary transitions, such as **Update** and **Delete**, are minimized to reduce the clutter on the page.
4. Current owner is highlighted to show which user is currently working on the task.
5. Item actions appear in the upper right corner allowing you to link other items, add attachments, and send e-mail messages in relation to the opened item.

Transition Forms

Transition forms are displayed when you click a transition button on the state form or submit a new item. Transition forms share a similar layout, which assists you when populating the form with the necessary information.

Resolve - FIX_001539: Network OS on most Router/switches failed after applying patch overnight

Incident Number: FIX_001539
 Incident Type: Break Fix
 Urgency: Medium
 Impact: Single User
 Priority: 4
 Incident Operator: Karl Malone

Incident Sub-Category: (None)
 Incident Sub-Category Type: (None)
 Symptom Code: (None)
 Resolution Code: (None)

Resolution Details

* Resolved: with Workaround

Known Error Used: PR_001765: SAP Purchasing Module is not updating the order system - CLASSIFICATION

Known Error Description: FusionCharts v3 helps you create animated and interactive Flash charts for web and desktop applications. It livens up your applications by converting monotonous data into exciting visuals. FusionCharts can be integrated with a myriad of web technologies like ASP, ASP.NET, PHP, JSP, ColdFusion, Ruby on Rails, Python or even simple HTML pages. It works with all databases including MS SQL, Oracle, MySQL, PostgreSQL, CSV or even legacy data storage.

* Workaround Used: (None)

Workaround Steps: (None)

cancel > OK

1. Required fields are highlighted in yellow calling attention to fields that must be populated. This is done by adding background coloring to the cells for the form in SBM Composer.
2. Relational fields enable a keyword search with a drop-down list of results.
3. **OK** and **Cancel** buttons are placed on the bottom of the form. In addition, transition options may be placed at the bottom of the form. These options make use of the conditional routing available in SBM. You select from one of the selections, which routes the item along a particular path in the workflow. The following is an example of a routing selection in the Incident process.

Serena Service Manager | © 2010-2011 Serena Software, Inc. | Documentation

cancel > Escalate to Level 2 Major Incident



Note: For form designers: the forms are designed so that fields that are set automatically are put into the System section of the form. Other fields are in the User section so that users will be able to view the fields that require information.

Urgency, Impact, and Priority

An item's *Priority* determines the sequence in which items will be addressed. High priority items should be addressed quickly and escalated up the organizational hierarchy, if

necessary. Lower priority items can be addressed in a less urgent manner, and they should not be re-prioritized to expedite their resolution.

The default Service Manager includes five levels of priority, with 1 being the highest priority and 5 being the lowest priority.

ITIL defines *Priority* as being based on the *Impact* to the business and the *Urgency* within which the resolution is required by the user or business. In other words, *Impact* is a measure of how business critical the incident is and *Urgency* is the speed required to resolve the incident. Service Manager automatically determines Priority after you have selected the Impact and Urgency for an item.



Tip: Since there are additional elements that could be included in determining the priority, like scope, complexity, who is requesting the change, and resources required for resolution, submitters can override the automatically determined priority by selecting a new one in the **Priority** drop-down list.



Note: Overall impact can be difficult to determine, and it is common to simplify impact by relating it directly to how many users are affected by the item. Serena Service Manager uses this approach and allows for three impact choices: **Enterprise**, **Department**, and **Single User**.

The following table explains how the priority is determined based on your selection for *Impact* and *Urgency*:

Table 1. Urgency, Impact, and Priority

		Impact		
		Enterprise	Department	Single User
Urgency	High	1	2	3
	Medium	2	3	4
	Low	3	4	5

Implementation Method

The automatic calculation is performed by JavaScript included on the **Submit** form.

You can make modifications to this process, for example by adding a new level of Impact, by performing the following changes in SBM Composer. Note that this change must be performed for each process app, such as Incident Management, Problem Management, and Change Management.

To update the JavaScript:

1. Open a process management app in SBM Composer, such as Incident Management.
2. Add the selection values to the Impact, Urgency, or Priority fields to the primary table. For example, for Incident Management, you would add the values to the **Incidents** table under Data Design.
3. Change the calculation of Priority by modifying the **calcPriority** script found on the Submit form. For example, suppose you added a new Impact value called `CEO`, in

case the incident impacts the CEO directly, you could change the following line to include checking for the CEO value when setting the priority:

```
if ((impact == "Enterprise" && urgency == "High") || (impact == "CEO")) \{  
    SetFieldValue("PRIORITY", 1);  
\}
```


Chapter 3: Request Center

Request Center is a user friendly IT Service Portal, designed for the non-IT user. Request Center both advertises IT functions and allows users to access these operations in a visually appealing way.

The simplified interface allows users access to the service catalog, their submitted requests, and the Knowledge Center.

Users access the Request Center portal through the following URL:

`http://serverName/tmtrack/tmtrack.dll?shell=srp`

The following topics describe the functionality available in Request Center:

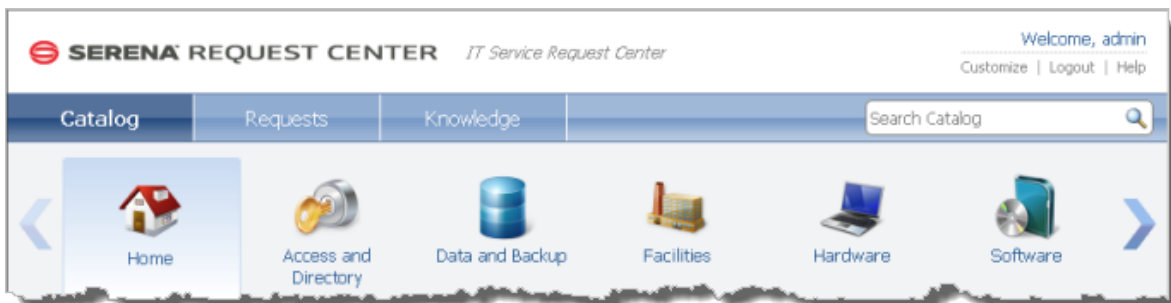
- [Request Center Overview \[page 19\]](#)
- [Service Catalog \[page 20\]](#)
- [Requests View \[page 20\]](#)
- [Knowledge Center \[page 22\]](#)
- [Configuring Request Center \[page 23\]](#)

Key Benefits

- User-friendly, visually appealing interface into the IT Service Operations.
- Instant access to important IT service announcements.
- Easy access to search articles in Knowledge Center.
- User sees a list of the items that they have submitted.

Request Center Overview

Request Center is a portal into the IT Services, where end users can access the important and pertinent information quickly. The Request Center is tailored for end users that require limited access to Service Manager and who do not need to be burdened by the additional functionality found in the User Workspace.



End users access Request Center through the following URL:

```
http://serverName/tmtrack/tmtrack.dll?shell=srp
```

Request Center consists of the following views:

- **Catalog** tab where users can submit requests into applications or access external URLs as determined by the IT Administrator.
- **Requests** tab where users can monitor the items that they have submitted, alerting them if any item requires action such as adding information.
- **Knowledge** tab where users access Knowledge Center articles.

Urgent announcements that were submitted into Knowledge Center are displayed in the announcement bar, which appears below the banner.

Users can click the **Help** button to display inline help for understanding how to use the portal.

Both the banner and the Contact Info are configurable by the IT Administrator. The IT Administrator can choose the logo and title to display in the banner. The IT Administrator can also choose which information to display in the Contact Info dialog.

Service Catalog

The service catalog view appears on the **Catalog** tab in Request Center. The service catalog is a collection of IT services defined by an IT administrator.

The end users choose from the available services by clicking on the appropriate icon. The services are organized by category, allowing the end users to filter the services based on categories. Users navigate between the categories by browsing the categories in the ribbon bar. Selecting a category will display only service actions assigned to that category.


Users access a service by clicking on the title. The user can display detailed information on a particular service by clicking the summary to show the details. Users can search for services by entering a keyword to search for in the search field. The search supports has limited wildcard support, such as `*`.



Certain services appear on the Home page for all users, and they are divided into **Favorite**, **Featured** and **What's New** services.

The IT Administrator defines what services appears in each section when customizing Request Center. For information on configuration, see [Configuring Request Center \[page 23\]](#).

Requests View

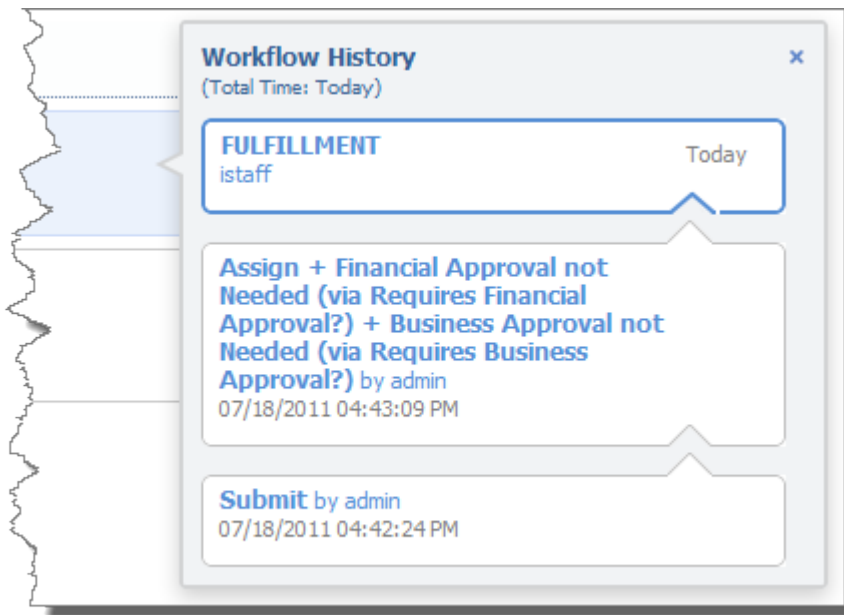
The Requests view displays items that the user submitted. By default, the items are grouped by request date. A symbol represents the status of each item:

-  signifies active items that are currently waiting for action by other users.

-
-  signifies items that the user must act on. These items may require that the user adds information or approve the item. Click on the item to display the form where you can update the item.
 -  signifies that the items are inactive.

The following actions can be performed on the **Requests** tab:

- Filtering items by selecting **Active**, **Follow Up**, or **Inactive**
- Searching for items using the search field
- Displaying the details of an item by clicking on its title
- Displaying the Change History of an item by clicking the magnifying glass adjacent to the title.



The Requests view depends on the **Request Center - My Request** report that is included with the Incident Management (IT Service) application. This report is a multi-table report that spans the Incident Management, Problem Management, Change Management, and Knowledge Management applications. The report displays all of the items that the user has submitted into these applications. You can modify the report to include additional process apps that you want to expose in Request Center.

The report requires that all of the process apps (Incident Management, Problem Management, Change Management, and Knowledge Management) have been promoted before it is available. If one or more of these process apps have not been promoted, the report will not exist, and the Requests view will be blank.



Tip: By default, the **Request Center - My Request** report only contains items that have been modified in the past 30 days, meaning that items that have not been modified for more than a month will not appear on the report. This setting eliminates the clutter of older items from the Requests view. Administrators can modify this setting by changing the filter in the report. The updated report must be saved with the same reference name of **SSMMYRequests**.

Knowledge Center

Knowledge Center is the online interface into the Knowledge Management system available with Service Manager. Users access Knowledge Center by logging into Request Center and selecting the **Knowledge** tab.

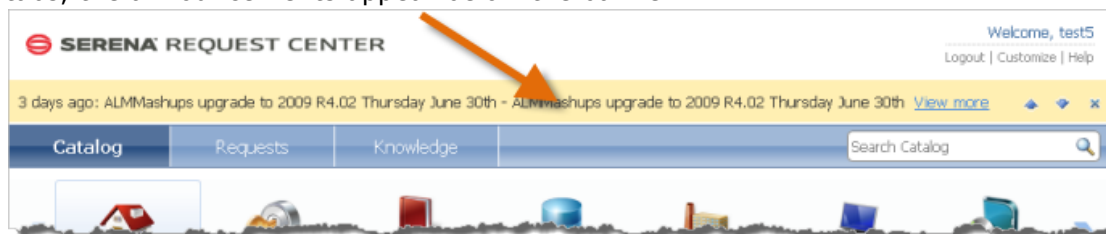
Knowledge Center lets you perform the following actions:

- Search for articles within Knowledge Center by entering keywords in the search field on the **Knowledge** tab.
- Sort the search results by latest added, top rating, most popular, or most commented. **Best** is based on cumulative ratings and **Popular** is the total number of views.
- Filter results based on category by selecting the category in the list.
- Group results by article type.
- Display detailed view by clicking on the article's title.
- Add comments and rate the article in the detail view by clicking **Add your own comment**. Choose the number of stars to give the article and enter any comments.



Note: You are only allowed one comment and rating per article. Subsequent comments will replace the original comment.

- View important IT announcements, such as possible outages. Similar to the other tabs, the announcements appear below the banner.



Note: If you have publish privileges, you will also be allowed to view expired articles and update articles. Select **Include Expired** to include expired articles in your search results. In the detail view, click **Update This Article** to begin the update process for the article.

Both the Knowledge Center articles and announcements are managed with Knowledge Management. For more information, see [Chapter 9: Knowledge Management \[page 85\]](#).

Configuring Request Center

Request Center is the simplified end user interface that allows end users to easily interact with the IT Services found in Service Manager. Request Center eliminates confusion for the user by removing the advanced functionality available in the User Workspace.



Important: Before accessing Request Center, promote all of the snapshots to your environment. This will allow the demo data to be available in Request Center when you log in.

Request Center is accessed at the following URL: `http://serverName/tmtrack/tmtrack.dll?shell=srp`.

If the SBM User Workspace is displayed instead of the Request Center when you access the URL, verify that:

- Request Center has been installed by running the Service Manager installer.
- IIS Web Server has been restarted after installing Service Manager.

Request Center requires customization before end users can access service operations.

The following topics explain how to customize Request Center:

- [Adding Categories \[page 23\]](#)
- [Adding Service Actions \[page 24\]](#)
- [Changing Logo, Announcements, and Contact Information \[page 26\]](#)
- [About the Image Picker \[page 27\]](#)



Important: Any customizations made to Request Center affect all users.

Adding Categories

Categories allow you to group service actions for easy navigation by users.

To add a new category:

1. Log in to Request Center (`http://serverName/tmtrack/tmtrack.dll?shell=srp`) with a user account that has administrator privileges.



Restriction: For on-premise installations, the administrator needs either a **Regular User** license and **Remote Administration** privilege or a **Managed Administrator** license and **Global Administration** privilege. For on-demand installations, the administrator needs to be part of the **Administrator** group.

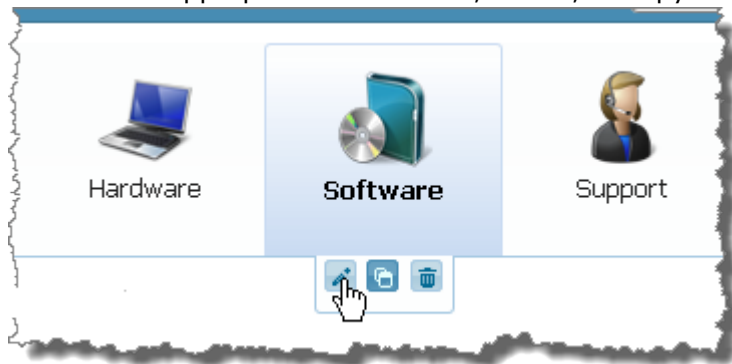
2. Select **Customize | Service Catalog**.
3. Click **+ Category** button.

4. Choose an image for the service by clicking **Change image**. You can choose from existing images or insert a URL. For best results, use an image that is 48 x 48 pixels. For information on the image picker, see [About the Image Picker \[page 27\]](#).
5. Enter a **Name** and **Description** for the category.
6. Click **Save** to save the new category.

The new category will appear in the selection list. The categories are arranged in alphabetical order.

To edit, clone, or delete a category:

1. Select **Customize | Service Catalog**.
2. Select the category to edit, clone, or delete.
3. Click on the appropriate icon to edit, delete, or copy the category.



Adding Service Actions

IT service actions are available to end users through Request Center. Service actions allow you either to submit a new item into a Service Manager process or to access a URL. Service actions are laid out in a user-friendly format within Request Center. Users can browse services by their category or by searching for them with the search filter.

To add a new service action:

1. Log in to Request Center (<http://serverName/tmtrack/tmtrack.dll?shell=srp>) with a user account with administrator privileges.
2. Select **Customize | Service Catalog**.
3. Click **+ Service** to add a new service operation.
4. Choose an image for the service by clicking **Change image**. You can choose from existing images or insert a URL. For best results, use an image that is 32 x 32 pixels. For information on the image picker, see [About the Image Picker \[page 27\]](#).
5. Enter a **Name** and **Summary** for the new service operation. The summary appears as a quick description in Request Center.

-
6. Change the **Category** by choosing the category from the drop-down menu.



Tip: Selecting a category before clicking add service will prepopulate the category field with the selected category.

7. Enter a longer description in the **Description** box. The long description appears when the end user expands the service action in Request Center.
8. Enter the **Service Level** expectation and **Charge Back** cost. Service level expectation is a description of the service level that the end user should expect. The Charge Back cost is the cost that end user or the end user's department will incur due to the successful completion of the service action. Note that these fields only display to the end user in Request Center when values are entered for the fields.
9. Choose to display the service operation under the **Favorite, What's New,** and **Featured** sections under the home view of the Catalog tab by checking all that apply.
10. Select the option either to submit into an SBM process app or to access an external URL:
 - For an SBM process app, select the process app and project to submit into. You can tailor the submit form to choose a particular **Item Type** or by prepopulating the **Title** field for the new item.



Note:

- If the user does not have permissions to submit into the application or project, the service will not appear in Request Center for that user.
- The **Query at Runtime** option in the project drop-down allows the user to select the project when submitting an item.
- The default Submit form for the project is used to submit new items into the project.
- The **Item Type** and **Title** are populated based on the selected process app and project.



Important: Choose a project that allows submissions. If the project does not allow submissions, then the user will receive an error when selecting the service. The following is a sample error:

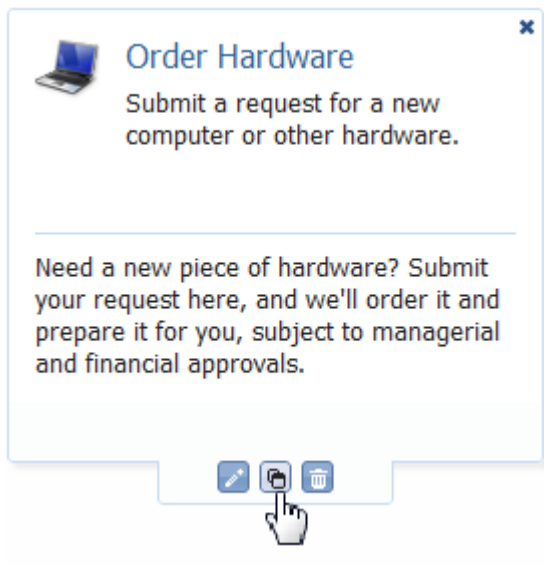
```
An error occurred while processing the last request.  
....  
Project doesn't allow submitted items:
```

- For external Web page, enter the URL in the field. Choose whether to display the link within the Request Center or in a new window.

To edit, clone, or delete a service action:

1. Select **Customize | Service Catalog**.
2. Select the service action to edit, clone, or delete.

- Click on the appropriate icon.



Changing Logo, Announcements, and Contact Information

The look and feel to Request Center is easily customizable, allowing you to tailor the portal. Possible changes that you can make include:

- Changing the graphic that is displayed in the title bar
- Modifying the information and hyperlink that appears alongside the graphic
- Turning off or on the announcements that are added to Knowledge Center
- Changing the contact information that appears in the **Contact Info** link



Important: Remember that Request Center customizations affect all users.

To customize the display properties of Request Center:

- Log in to Request Center (<http://serverName/tmtrack/tmtrack.dll?shell=srp>) with a user account with administrator privileges.
- Select **Customize | Request Center**.
- Change any of the following:

Customization	Notes
Title	The title appears alongside the logo. You can apply formatting to the text using the formatting toolbar.

Customization	Notes
Image (URL)	Enter a URL to your corporate logo. Remember this URL must be accessible by all users from Service Manager. For example, do not enter a logo that is located in a restricted domain that is inaccessible by all users.
Image Link	Enter a URL which a user will be directed to if they click on the logo.
News/ Announcements	Select Show in Request Center to display urgent announcements to users in the announcement bar, underneath the banner. You can set the Refresh Interval for the urgent announcements by selecting the minutes for a refresh. For more information on creating and publishing urgent announcements, refer to the chapter on Knowledge Management in the <i>Serena Service Manager Guide</i> .
Contact Info	Add a title and content for the contact info link. The title affects both the dialog title and the link name. HTML is not supported in the title field. The contents appear in the dialog. Use the formatting toolbar to apply styles and formatting to the content. You can hide the Contact Info link by deselecting Show in Request Center .

4. Click **Save**.

About the Image Picker

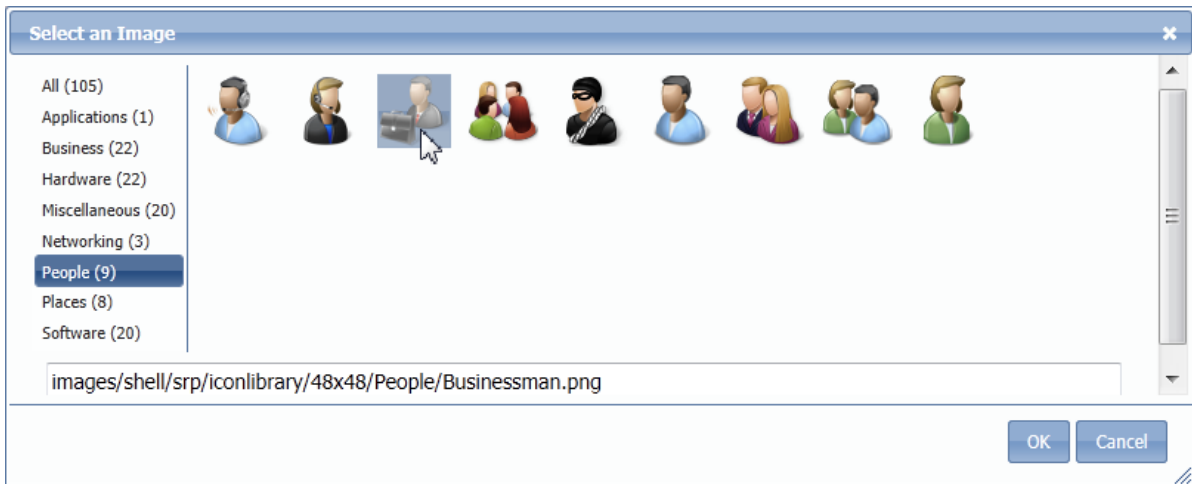
The image picker that is used to pick images for categories and services in Request Center, as well as for picking images when creating Knowledge Management categories.

The image picker comes with a collection of images that are arranged into multiple groups. You can choose to view all images or select a group to view only images in that group.

Choose the image by selecting the image and clicking **OK**.



Tip: Instead of picking the image, you can insert a URL to an image in the text field. Remember that the image location must be accessible by all Request Center users.



Adding New Images to Image Picker

On-premise installations can add new images to the image picker. The administrator must perform the following steps on the SBM Server:

1. Add the new PNG image files to the 32x32 or 48x48 folders in the following directory:

```
SBMinstallationDirectory\Serena\SBM\Application
Engine\bin\images\shell\SRP\iconlibrary
```

The image size should be 32 by 32 pixels in the 32x32 directory. This directory is used for the services. The image size should be 48 by 48 pixels in the 48x48 directory. This directory is used by both Request Center categories and **KM Categories**.

2. Update the **serviceimages.js** and **categoryimages.js** files to include the new images. These files are found in the following directory:

```
SBMinstallationDirectory\Serena\SBM\Application
Engine\bin\javascript\shell\SRP
```

Chapter 4: Incident Management

Incident Management focuses on restoring services to normal operation after service interruptions as quickly as possible and minimizing the impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

The following topics explain the features of Incident Management in the Serena Service Manager.

- [Incident Management Overview \[page 29\]](#)
- [Incident Management Workflow \[page 36\]](#)
- [Incident Management Dashboard \[page 37\]](#)
- [Satisfaction Dashboard \[page 39\]](#)
- [Incident Management Roles \[page 40\]](#)

Key Benefits

- Incident prioritization and classification based on ITIL standards.
- Graphical indicators for easier process visualization.
- Incident workflow according to ITSM best practices.
- Ability to relate existing Known Errors to new incidents.
- Ability to track first call resolution rates.
- Reporting dashboard to monitor possible problem areas and resolution rate.

Incident Management Overview

The incident management workflow addresses the following areas:

1. [Incident Creation \[page 30\]](#)
2. [Incident Classification and Initial Support \[page 31\]](#)
3. [Incident Investigation and Diagnosis \[page 33\]](#)
4. [Incident Resolution and Closure \[page 34\]](#)
5. [Incident Monitoring and Communication \[page 35\]](#)
6. [Incident Reporting \[page 36\]](#)

1. Incident Creation

Incident creation is known as submitting incidents in Serena Service Manager. Two primary actors responsible for submitting incidents are end users and IT Service Desk staff.

Users can submit their incidents using the Request Center, SBM User Workspace or by e-mail.



Note: Incidents can also be submitted automatically from another application using Web services. For example, if you have the Service Manager integration to Microsoft Operations Manager, incidents will be submitted automatically with Web services when certain issues arise.

To create a new incident using SBM User Workspace:

1. Select the **Incidents** application tab.
2. Select **Submit** from the navigation pane on the left.
3. Click **Submit to My Preferred Projects** and choose the project to submit into from the project tree.
4. On the Submit form:
 - Choose the **Urgency** and **Impact** from the drop-down lists. **Priority** is calculated automatically described in [Urgency, Impact, and Priority \[page 15\]](#), but the value can be overridden.
 - Enter a **Title** and **Description**.



Note:

A keyword search of Knowledge Center is performed after you have entered a **Title** and moved focus to another field. When articles exist in the Knowledge Center that match the title words, a message will appear informing you of the number of matches. Click **View** to look at matching articles.



If one of the articles addresses your issue, open the article by clicking on the title and choose **Yes, cancel submit** to cancel the submit process.

- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.
5. Click **OK** to create the new incident.

Submitting Incidents Using E-mail

You can configure SBM to accept new incidents through e-mail.

For on-premise installations, information on configuring SBM to handle e-mail submissions is available in the *SBM System Administrator Guide*.

For on-demand installations, contact Serena Support for configuring e-mail submissions.

Submitting Incidents from an Existing Incident

The incident management workflow has two methods for creating incidents from within the workflow.

- **Copy Incident** - Creates an identical copy of the existing incident.
- **Post New Incident** - Opens the submit form with the fields populated based on the existing incident. The values can be edited in the new incident before you submit the item.

2. Incident Classification and Initial Support

Incident classification includes setting priority, performing incident matching, and linking incidents to configuration items. Initial support includes finding an existing workaround or matching with other existing errors.

In the **Classification** state, the Service Desk staff review the issue and determines how the incident should be handled. The following actions may be available to you for updating and routing the incident. Your actual available actions depend on your role:

- **Route** the incident, which allows you to choose from the following options:
 - **Assign to Operator** which assigns the incident to an Incident Operator for additional review.



Note: The **Level 1 Technician** selection list includes users who are in the *Level 1 Tech*, *Level 2 Tech*, and *Level 3 Tech* roles. This allows a Level 2 Tech or Level 3 Tech to be assigned level 1 incidents if the tech is available.

- **Major Incident** which escalates the incident immediately to the *Incident Manager*.



Note: Major incidents require the immediate attention of the incident manager. The incident manager may pull in the appropriate resources to quickly restore normal service operations. It may also require the incident manager to coordinate with problem management to find the root cause of the major incident to prevent its recurrence.

- **Resolve** the incident, noting whether it was resolved on the first call.
- **Update** with additional information from the end user.
- **Delete** the incident, removing it from the system.

The following options are available to move the incident to another project, to merge the incident with other incidents, or to create duplicate incidents:

- **Recategorize** moves the incident to another project within Incident Management. Use this transition to change the Incident to a Service Request.
- **Merge Incident** ties together the current incident with an existing incident using Parent/Child relationships. See [Merging or Linking Incidents \[page 32\]](#).

- **Copy Incident** creates a duplicate of the incident in the same state as the current incident. You cannot modify the values when the item is created.
- **Post New Incident** creates another incident based on the current incident. You can modify the values in the new incident on the Submit form and the new incident begins at the start of the workflow.

In this state, users such as Service Desk staff can choose from the following:

- Attach a file to an incident on the **Attachments** tab.
- Choose an Item Action such as Send an E-mail for the **Actions** drop-down list.

When updating or transitioning the incident, you can modify data in the incident. The following describes the information to add in the fields, and how the information is used:

- Choose the **Incident Type**, **Urgency**, and **Impact** from the drop-down lists. **Priority** is calculated automatically as described in [Urgency, Impact, and Priority \[page 15\]](#), but the value can be overridden.
- Search for a **Configuration Item** to relate to the request. The configuration item categorizes the incident by automatically adding an incident category, incident sub-category, and incident sub-category type (if defined).



Note: Selecting a configuration item is important as the CI is used to show related CIs and to show links to existing problems.

- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.
- After selecting the Configuration Item, you can view other active incidents for that item by displaying the **Active Incidents** tab.

Merging or Linking Incidents

Merging or linking incidents creates a parent/child relationship between the incidents that you are merging. The parent becomes the main item, which continues to move through the workflow as updates are performed. The children move to the **Linked to Parent** state, indicating that they are no longer the main item. The parent issue is displayed within the child item, giving the status information of the parent.

When the parent is resolved, the children are automatically resolved as well. The resolution notes from the parent are added to the children.

To merge incidents, select the **Merge Incident** transition and then choose whether the incident should become the child or parent:

- If you chose the incident to become the **Parent**:
 1. Select the incidents to add as children and click **OK**.
 2. The children will be moved to the **Linked to Parent** state.
 3. The parent continues to move along the workflow.
 4. When the parent is resolved, all children are automatically moved to the **Resolved** state and the parent's resolution notes are added to each of them

-
- If you chose the incident to become the **Child**:
 1. Select the parent to merge into and click **OK**.
 2. The current incident will be moved to the **Linked to Parent** state while the parent moves along the workflow normally.
 3. When the parent is resolved, the incident is automatically moved to the **Resolved** state and the parent's resolution notes are added to the incident.

3. Incident Investigation and Diagnosis

If the initial support fails to resolve the incident, the IT Service desk staff can transfer the incident to a Subject Matter Expert (SME). The SME investigates the incident, adds details, and, if possible, resolves the incident. Other options include escalating the incident to another SME or posting an RFC to the change management group.

The default incident management workflow contains three levels of support. Each level is associated with a different role as described below:

- **Investigation and Diagnosis** state – Incident Operator role
- **Escalated to L2** state – Level 2 Technician role



Note: The **Level 2 Technician** selection list includes users who are in the *Level 2 Tech* and *Level 3 Tech* roles. This allows a Level 2 Tech to be selected to handle a lower level incident if the tech is available.

- **Escalated to L3** state – Level 3 Technician role

Each of these states allows the SME or technician to choose from the following actions:

- **Resolve** the incident, adding the necessary information in the *Resolution Details* section.
- **Escalate** the incident to the next level, for example, escalate the issue from level 2 to level 3.
- **Post RFC** to create a request for change from the incident. The incident moves to the **Pending Change** state. It will return to the **Investigation and Diagnosis** state after the related change is closed.
- **Post Problem** to either create a new problem or choose an existing problem. To create a new problem, choose **Create New Problem** from the **Problem Link** drop-down list. To link to an existing problem, choose **Link to an Existing Problem** and search for the existing problem under **Raised Problem**. The linked problem appears on the **Linked Problem** tab. The link can be removed by selecting **Remove Problem Link**.



Tip: You can configure SBM to automatically assign the correct owner for each state. This improves the user experience by eliminating the need for them to select the correct SME when escalating the incident.

Similar to the **Classification** state, the investigation states allow the following additional actions to merge or create incidents:

- **Merge Incident** ties together the current incident with an existing incident using Parent/Child relationships. See [Merging or Linking Incidents \[page 32\]](#).

- **Copy Incident** creates a duplicate of the incident. You cannot modify the values when the item is created.
- **Post New Incident** creates another incident based on the current incident. You can modify the values in the new incident on the Submit form.

4. Incident Resolution and Closure

Incidents are resolved when service has been restored to normal. Incidents can be resolved in a variety of ways including attaching a Workaround or a Known Error. A *Workaround* includes the steps on how to circumvent the problem. A *Known Error* is a problem where there is no known fix. There may be a workaround for the Known Error or maybe not.

When resolving the error, the **Resolution Details** section enables you to select a Known Error, a Workaround, or a Knowledge Center article as resolving the incident.

The screenshot shows a form with the following fields and values:

- First Call Resolved:** Yes (dropdown)
- Create How To Article:** No (dropdown)
- * Resolved:** with Known Error (dropdown)
- *Known Error Used:** A search box containing "KE_000012: Windows explorer is running slow - RESOLVED" with a dropdown arrow and a red arrow icon to the right.
- Known Error Description:** Windows explorer suddenly consumes 99% of the resources.
- Known Error Resolution:** Created a workaround describing what needs to be accomplished.



Note: When the incident is resolved from the **Classification** state, the incident may be marked as **First Call Resolved**. This data is used in reports, such as **Weekly First Call Resolution Rate**, to keep managers informed to which incidents are resolved with the first call.

The option to create a **How To** article in the Knowledge Center is available on the Resolve transition. Selecting **Yes** will launch the submit form into Knowledge Management after completing the **Resolve** transition.



Restriction: You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.



Note: The content fields in the knowledge base article are automatically populated with the content from the incident. Selecting **Load Article Template** will erase the populated information, replacing it with the content from the template.

In the Resolved drop-down list, you can select Without Known Error, With Known Error, With Workaround, and With Knowledge Center article:

- **Without Known Error** enables you to enter the resolution details in the **Resolution** field.

-
- **With Known Error** and **With Workaround** enable you to search for existing known errors and their associated workarounds.



Tip: When closing the item **With Known Error** or **With Workaround**, you must select a **Problem** or **Known Error** which is active. A problem cannot be selected if it is in the **Closed** state.

- **With Knowledge Center Article** enables you to search for and select a Knowledge Center article to associate with the incident. To search for the article, click **Search Knowledge Center** and choose the relevant article in the results.

Depending on whether the incident was resolved with a workaround:

- If the incident was resolved without a workaround, it moves to the **Resolved** state, where it can be closed.
- If the incident was resolved with a workaround, it moves to the **Resolved by Workaround** state. The incident remains in this state until the problem associated with the workaround is addressed. When the problem is closed, then the incident automatically moves to the **Resolved** state.

From the **Resolved** state, a user can close the incident by selecting the **Close** transition. The **Close** transition launches a Survey form, where users can rate their service desk experience. The survey form has four selection fields and a text entry field for additional comments.

The completed incident moves to the **Closed** state, indicating that it is no longer active. The final incident displays a total Survey Score, which is a summation of the weighted values of **Courtesy**, **Responsiveness**, **Technical Expertise**, and **Overall Satisfaction** values. The default weightings for **Courtesy**, **Responsiveness**, and **Technical Expertise** are the selected values. **Overall Satisfaction** is weighted at ten times the selection, for example, a selection of *1* would be weighted as *10* for the **Survey Score**. Change the weightings by editing the fields using SBM Composer.



Tip: The **Satisfaction** dashboard provides four reports to assist in monitoring the responses to the satisfaction survey.

A second method of closing an incident from the **Resolved** state is the **IT Close** transition. This transition is available only to users in the IM Operators, IM Manager, IM Level 2, IM Level 3, and IM Administrator roles. This transition does not include a survey form.



Note: If you are a member of IM User and a role with permissions to the **IT Close** transition, you will see two close transition buttons, **Close** and **IT Close**, on the **Resolved** state form. Choose the **Close** transition to complete the survey.

5. Incident Monitoring and Communication

Serena Service Manager has two main methods to monitor and communicate about the status of incidents: notifications and reporting.

The first method is through e-mail notifications, which inform users about the status of incidents. Automated e-mail notifications can be configured to notify users of incident creation, incident transfers, incident resolutions, and incident closures.

For example, you can create a notification that automatically informs incident submitters that they need to update their incident with more information. The submitters can either log in to the SBM User Workspace using the link in the notification or reply to the e-mail to update their incident.

The notifications are tailored using notification rules and notification templates. Administrators are responsible for editing the notifications and creating the workflow rules. (On-premise only)

Users can subscribe to the selected notifications under their **User Profile** in SBM User Workspace.

For information on reporting, see the following section, [6. Incident Reporting \[page 36\]](#).

6. Incident Reporting

In addition to the preconfigured reports that are included with the Service Manager, you can create a variety of reports in SBM to track your incidents.

The following are some example reports:

- First Call Resolution
- Mean Time to Incident Resolution
- Number of Incidents SLA Breaches per Week
- Number of Incidents by Category
- Number of Escalations

You can also combine reports to create a dashboard or multi-view report like the one created for the Incident Management launch page ([Incident Management Dashboard \[page 37\]](#)).



Tip: You can create reports to perform keyword searches on auxiliary tables, such as the Workarounds table. To create this type of report, select to report on the Workarounds auxiliary table and create a search filter with `Title contains Query-at-runtime`. When you run the report, you will be prompted to enter your keyword search criteria, and the results will return all workarounds which contain the search terms in the title.

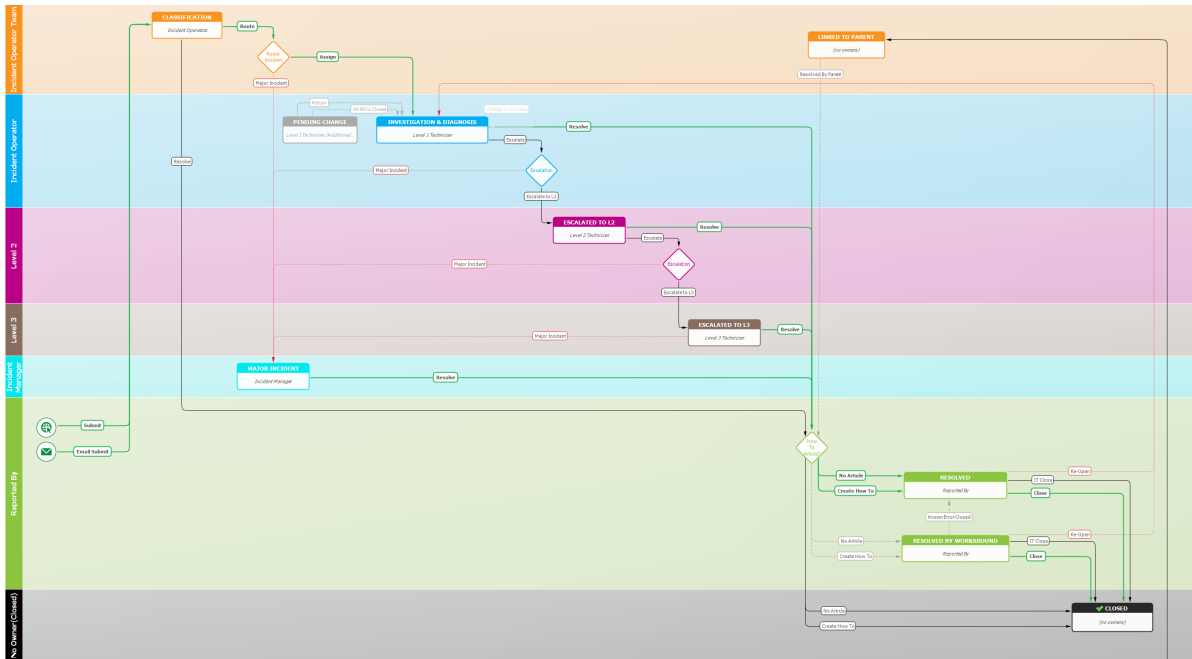
For details on creating and running reports, refer to the SBM User Workspace online help.

Incident Management Workflow

The Incident Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Classification* and *Major Incident*, and the transitions are marked with arrows, such as *Close* and *Assign*. The process starts with the **Submit** and can proceed along the different transition arrows.

The **Incident** workflow is one of two workflows in the Incident Management application. The other is the Service Request workflow which is used for request fulfillment.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.




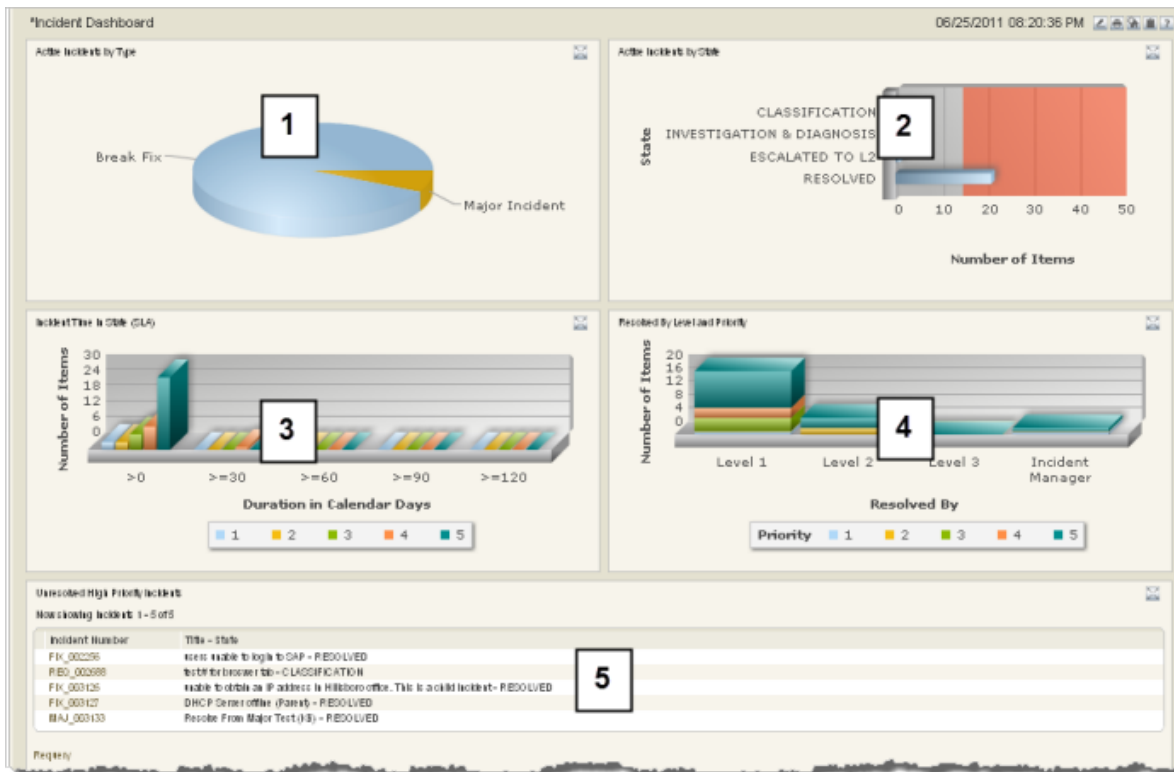
Incident Management Dashboard

The Incident Management dashboard is designed to give managers and staff an overview of existing incidents and possible problem areas. The following screenshot and descriptions explain the information that the reports convey.

The Incident Dashboard report is available in the reports that are shipped with the Incident Management snapshot.



Tip: Set the Incident Dashboard report as the home page report for the IT Services application by opening the **Incidents** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



- 1. Active Incidents by Type** gives an overall view of the distribution of incidents based on their type. Note that this report does not appear in the on-demand trial version of Serena Service Manager. Instead, there is a list of training videos to enable you to get up and running.
- 2. Active Incidents by State** shows incidents and whether the number of incidents has reached a threshold. This graph allows the team to be proactive in addressing issues and keeping them under the critical threshold.
- 3. Incident Time in State (SLA)** shows the duration of time that incidents remain in each state. Incidents are grouped by priority.
- 4. Resolve by Level and Priority** shows at which support level incoming incidents have been resolved.
- 5. Unresolved High Priority Incidents** lists existing high priority incidents. These incidents may be a cause for alarm because they are high priority yet have failed to be addressed.




Note: The dashboard report is a multi-view report titled **Incident Dashboard**. You can modify this report to add additional reports that help you to improve your Incident Management process. You can modify the report under the Report pane in the SBM User Workspace.

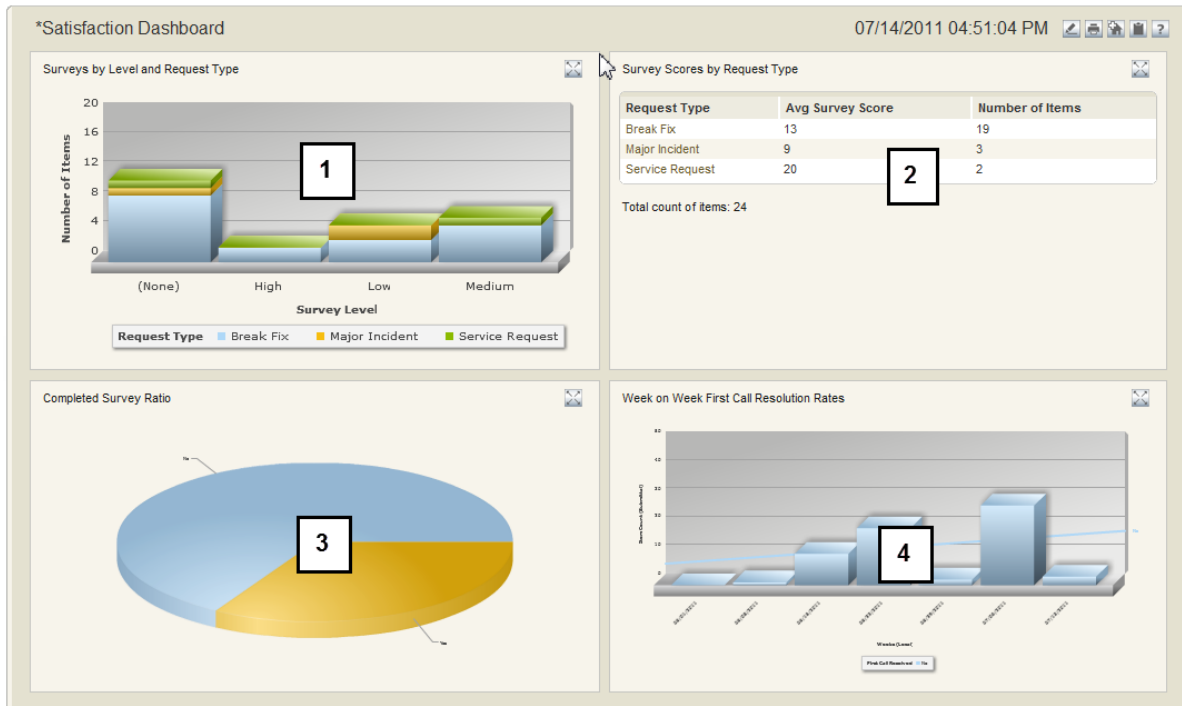
Satisfaction Dashboard

The Satisfaction dashboard is designed to give managers and staff an overview of how quickly incidents are being addressed and the responses to the satisfaction surveys for the incidents. The following screenshot and descriptions explain the information in the report.

The Incident Dashboard report is available in the reports that are shipped with the Incident Management snapshot.



Tip: Set the Satisfaction Dashboard report as the home page report for the IT Services application by opening the **Incidents** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



1. **Surveys by Level and Request Type** shows the incidents that have completed surveys based on level and type. You can drill-down to the incident to view the survey.
2. **Survey Scores by Request Type** shows the average score and the number of surveys that were received per incident type.
3. **Completed Survey Ratio** shows the number of incidents with completed surveys compared to the number of incidents where surveys were not completed.
4. **Week on Week first Call Resolution Rates** shows the number of incidents that were resolved on the first call, broken down by weeks.



Note: The dashboard report is a multi-view report titled **Satisfaction Dashboard**. You can modify this report to add additional reports that help you to improve your Incident Management process. You can modify the report under the Report pane in the SBM User Workspace.

Incident Management Roles

The following roles (or actors) are used in the Incidents workflow.



Note: The Incidents workflow and the Service Request workflow are in the Incident Management process app. These Level 1 Techs role is used in both of these workflows.

For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.

Incident Manager - The Incident Manager is responsible for the Incident Management/Request Fulfillment process. Other duties include:

- Ensure efficiency and effectiveness of the Incident Management/Request Fulfillment process
- Manage Incident Management/Request Fulfillment staff
- Provide for continuous service improvement for Incident Management/Request Fulfillment
- Produce KPI reports for management review
- Maintain the Incident Management/Request Fulfillment system
- Collaborate with other Service Manager processes such as Request Fulfillment, Problem Management, Change Management, and Configuration Management

Level 1 Techs - This role is for service desk staff or first level support who are responsible for handling incoming calls and e-mails. The responsibilities of this role include:

- Own incidents/requests from recording to closure
- Record, classify, and resolve incidents/requests as quickly as possible
- Collaborate with end users and technical SMEs with the goal of quickly restoring normal service operation

-
- Escalate incidents/requests appropriately
 - Keep end users informed of incident/request status
 - Ensure Service Levels are met
 - Match similar incident/request records

Level 2 Techs and **Level 3 Techs** - This role is for Technical SMEs and advanced support staff responsible for further incident investigation and diagnosis. Their other tasks include:

- Resolve incidents that were not resolved at First level
- Escalate service level breaches to Incident Manager
- Inform Service Desk staff of incident status and resolution
- Identify matching workaround
- Record new workaround



Note: Incident Operators include all members in Level 1 Techs, Level 2 Techs, and Level 3 Techs.

Incident Users - This role is for the end users who will be submitting incidents, providing the necessary details to the Service Desk. IM User is the only role associated with the **Affected User** field.

Incident Contacts - This role is for the user accounts who should be available for selection in the **Additional Contacts** field.

IM Administrator - This role is responsible for administering Incident Management/Request Fulfillment, such as assigning users to roles or fixing SBM issues.

Chapter 5: Request Fulfillment



Note: Request fulfillment was added as a service operation in ITIL V3.

Request fulfillment is responsible for handling requests that are less than major changes and outside of items that require immediate resolution such as problems and incidents. These requests can come from employees or customers. Each request is logged and tracked as it progresses through the workflow. Request Fulfillment includes an approval process which must be completed before fulfilling the request.



Note: Service requests differ from incidents because they are not accompanied by a service interruption. In other words, there is nothing broken that needs fixing with a service request.

Typical service requests include:

- Configuration such as new employee setup or network access.
- Security requests such as allowing building access.
- Facilities requests such as moving offices or furniture.
- Communication requests such as adding a cellular phone.
- Information requests such as how to connect to the network.

The following topics describe the features found in Request Fulfillment:

- [Request Fulfillment Overview \[page 43\]](#)
- [Request Fulfillment Roles \[page 47\]](#)
- [Request Fulfillment Workflow \[page 48\]](#)

Key Benefits

- Process for tracking and monitoring requests.
- Reports for showing response time and customer satisfaction.
- Approval process to manage requests.
- Request fulfillment workflow according to ITSM best practices.

Request Fulfillment Overview

The request fulfillment workflow addresses the following areas:

1. [Request Creation \[page 44\]](#)
2. [Request Classification and Initial Support \[page 45\]](#)
3. [Request Approvals \[page 45\]](#)

4. Request Resolution and Closure [page 46]

5. Request Monitoring and Communication [page 47]

1. Request Creation

Request creation is known as submitting requests in Serena Service Manager. The primary actors responsible for submitting incidents are employees, customers, and IT Service Desk staff.

Employees and customers can submit their requests using the Request Center or SBM User Workspace. The following example describes submitting a request using Request Center.



Important: The following procedure assumes that there is a configured service action called **Order Hardware** under the **Hardware** category. This service action is included in the sample services. You must promote ALL of the snapshots before logging in to Request Center for the sample data to be available.

To create a new request using Request Center:

1. Log in to Request Center: `http://serverName/tmtrack/tmtrack.dll?shell=srp`.
2. Select the **Hardware** category on the **Catalog** tab.
3. Click the **Order Hardware** service action to open the submit request form. Note that you must click on the title.
4. On the Submit form:
 - Choose the **Type**, **Urgency** and **Impact** from the drop-down lists. **Priority** is calculated automatically described in [Urgency, Impact, and Priority \[page 15\]](#), but the value can be overridden.
 - Enter a **Title** and **Description**.



Note:

A keyword search of Knowledge Center is performed after you have entered a **Title** and moved focus to another field. When articles exist in the Knowledge Center that match the title words, a message will appear informing you of the number of matches. Click **View** to look at matching articles.

The screenshot shows a form titled 'Overview' with a 'Title' field containing 'How to change your password'. Below the title field is a green notification bar with a yellow exclamation mark icon and the text '2 similar articles have been found in the Knowledge Center. View'. Below the notification bar is a 'Description' field with a placeholder text: 'Tag keywords in the Description field by entering single words preceded by a hash: #tag, #tag_with_multiple_words or #tagWithMultipleWords'.

If one of the articles addresses your issue, open the article by clicking on the title and choose **Yes**, **cancel submit** to cancel the submit process.

-
- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.



Note: For users to be available for selection in the **Reported By** list, they must be added to one of the Incident Management roles such as **Incident Users**.

5. Click **OK** to create the new request.

2. Request Classification and Initial Support

Request classification includes setting priority, performing request matching, and determining which approvals are needed.

In the **Classification** state, the Service Desk staff reviews the request and determines how the request should be handled. The following actions may be available to you for updating and routing the request. Your actual available actions depend on your role:

- **Recategorize** moves the request to another project within Incident Management. Use this transition to change the Service Request to an Incident.
- **Assign** the request to a Level 1 Technician.
- **Update** the request with additional information.
- **Delete** the request, removing it from the system.
- Choose an item action from the **Actions** drop-down, such as Send an E-mail.

When assigning the request or transitioning the request, the fields can be modified. The following describes the information to add in the fields, and how the information is used:

- Choose the **Type**, **Urgency**, and **Impact** from the drop-down lists. **Priority** is calculated automatically as described in [Urgency, Impact, and Priority \[page 15\]](#), but the value can be overridden.
- Choose a **Level 1 Technician** who will be responsible for resolving the request once the request has been approved. Note that the Level 1 Technician selection includes *Level 1 Techs*, *Level 2 Techs*, and *Level 3 Techs*.
- Select whether the request requires **Financial Approval** or **Business Approval**. If financial approval is required, enter the **Cost Center** associated with the request.
- Select the **Financial Reviewer** and **Business Reviewer** if this request requires approval. The request will be routed to these users before being returned to the Level 1 Technician for implementation.
- Choose the **Reported By** user from the drop-down list. If necessary, you can also select the **Affected User** and any other **Additional Contacts**.

3. Request Approvals

The service request workflow has two levels of approval: financial approval and business approval. These two approvals help ensure that requests are adhering to the company's fiscal goals and business rules. The primary roles responsible for these actions are Financial Approvers and Business Approvers.

Requests are routed for approval when either the **Requires Business Approval** field or the **Requires Financial Approval** field is set to **Yes**.

The IT Service Request workflow sets these fields automatically when certain types of requests are created. For example, requesting access to a building or network usually does not have any financial cost, but there is usually a business approval process to ensure that this person should be granted access rights. When an **Access** type request is created, the **Requires Business Approval** field is automatically set to **Yes** and the **Requires Financial Approval** field is set to **No**.

In contrast, purchase requests require financial approval but probably not business approval. For **Purchase** type requests, the **Requires Business Approval** field is set to **No** and the **Requires Financial Approval** field is set to **Yes**.

The settings on these fields determine the route of the request through the Service workflow. Selecting **Yes** routes the request to the selected financial approver and business approver, where the approver can either approve or reject the request.

After approval, the request moves to the **Fulfillment** state, where the Level 1 Technician is assigned the item and becomes responsible for resolving the approved request.



Tip: To require that every request is approved, set the values for the **Requires Business Approval** and **Requires Financial Approval** field to **Yes** and mark it as read-only for the project. All requests with these settings will be routed for approvals.

4. Request Resolution and Closure

The actual fulfillment of a request depends on the nature of the request. The service desk staff may be able to fulfill a request, or the request may need to be sent to an outside group for completion.

After the request has been approved, it moves to the **Fulfillment** state, where the assigned Level 1 Technician is responsible for overseeing the closure of the request.

There are different options available to the technician to complete the request. The technician can choose to:

- **Resolve** the request, completing the request and closing the issue.
- **Post a Request for Change** to address the request. This opens an RFC in the Change Management workflow which will track the change. The request moves to the Pending Change state, where it remains until the RFC is completed. Once completed, the request returns to the **Fulfillment** state where the technician can close out the request. The related RFC can be seen on the **Linked RFCs** tab of the request.
- **Create a Task** to address the request. This opens a subtask in the Task workflow in Incident Management. The Task workflow is a simple workflow with two main states, **In Process** and **Closed**. The request stays in the **Fulfillment** state while the subtask is being completed. Examples of subtasks could include placing an order with a vendor or acquiring an access fob. Once the subtasks are completed, the request moves to the **Task Completed** state where the technician can close out the request. The subtasks related to the request can be seen on the **Subtasks** tab of the request.

Depending on the technician's privileges, the following transitions may also be available:

-
- **Recategorize** moves the request to another project within Incident Management. Use this transition to change the Service Request to an Incident.
 - **Delete** deletes the request.

The completed request moves to the **Resolved** state.

5. Request Monitoring and Communication

Serena Service Manager has two main methods to monitor and communicate about the status of requests: notifications and reporting.

The first method is through e-mail notifications, which inform users about the status of requests. Automated e-mail notifications can be configured to notify users of request creation, request transfers, and request resolutions.

For example, you can create a notification that automatically informs request submitters that they need to update their request with more information. The submitters can either log in to Request Center using the link in the notification or reply to the e-mail to update their request.

The notifications are tailored using notification rules and notification templates. Administrators are responsible for editing the notifications and creating the workflow rules. (On-premise only)

Users can subscribe to the selected notifications under their **User Profile** in SBM User Workspace.

In addition to the preconfigured reports that are included with the Service Manager, you can create a variety of reports in SBM to track your requests.

The following are some example reports:

- Active Service Requests by State
- Active Service Requests by Type
- Request Elapsed Time by Type

You can also combine reports to create a dashboard or multi-view report like the one created for the Incident Management launch page.

Request Fulfilment Roles

The following roles (or actors) are available for the Service Requests workflow.



Note: The Incidents workflow and the Service Request workflow are in the Incident Management process app. The Level 1 Techs, Level 2 Techs, and Level 3 Techs roles are used in both of these workflows.

For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.

Level 1 Techs - This role is for service desk staff or first level support who are responsible for handling incoming calls and e-mails. The responsibilities of this role include:

- Own incidents/requests from recording to closure

- Record, classify, and resolve incidents/requests as quickly as possible
- Collaborate with end users and technical SMEs with the goal of quickly restoring normal service operation
- Escalate incidents/requests appropriately
- Keep end users informed of incident/request status
- Ensure Service Levels are met
- Match similar incident/request records

Level 2 Techs and **IM Level 3 Techs** - In Request Fulfillment, these roles are included as Incident Operators, and members of the roles can be selected as owners for the initial classification of a request.



Note: Incident Operators include all members in Level 1 Techs, Level 2 Techs, and Level 3 Techs.

Business Approvers and **Financial Approvers** - These roles are for the business and financial approvers who are responsible for verifying that a request meets the business and financial requirements.

Incident User - This role is for the end users who will be submitting requests, providing the necessary details to the Service Desk. Request User is the only role associated with the **Affected User** field.

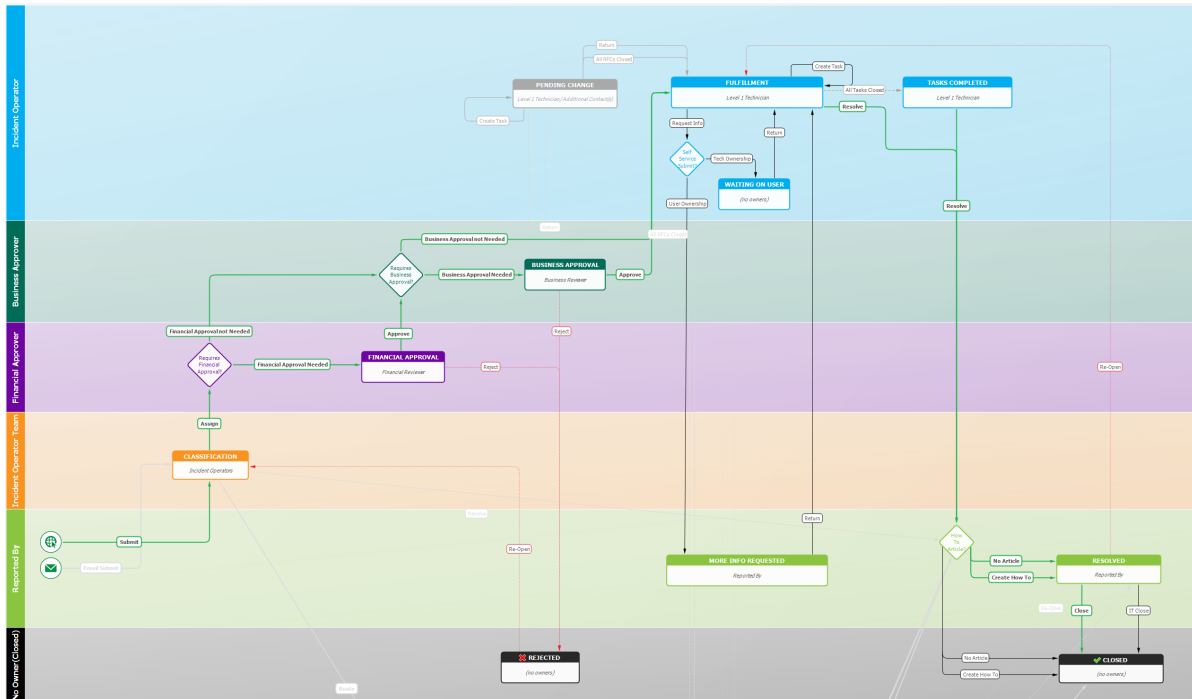
IM Administrator - This role is responsible for administering Incident Management/Request Fulfillment, such as assigning users to roles or fixing SBM issues.

Request Fulfillment Workflow

The Service Request workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Classification* and *Resolved*, and the transitions are marked with arrows, such as *Close* and *Assign*. The process starts with the **Submit** and can proceed along the different transition arrows.

The **Service Request** workflow is contained in the **Incident Management** application.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.



Chapter 6: Problem Management

Problem Management is a deeper dive into the cause of incidents. Problem Management seeks to find a resolution to the root cause of a problem so as to minimize or prevent the recurrence of incidents caused by the problem. It seeks to identify known errors and define a resolution. This information can prevent service disruption in the future. Proactive Problem Management helps your team to decrease the number of incidents as trends are analyzed and permanent fixes are implemented.

Problem Management works together with Incident Management and Change Management to ensure that IT service availability and quality are increased. As permanent resolutions are found to fix known errors, Requests for Change (RFCs) can be raised to make alterations to your IT process, applications or infrastructure. As these RFCs are implemented to resolve problems, related incidents are less likely to occur.

Problems can be related to incidents, changes, or solutions, giving your support desk the information that they need when they encounter similar issues. Known Errors and their resolutions are added to the Knowledge Base, where they can be accessed by the support staff to help identify permanent solutions and speed up the resolution time of similar incidents. This results in less downtime and less disruption to business critical systems.

The following sections describe the Problem Management application:

- [Problem Management Overview \[page 51\]](#)
- [Problem Management Workflow \[page 55\]](#)
- [Problem Management Dashboard \[page 56\]](#)
- [Problem Management Roles \[page 57\]](#)

Key Benefits

- Problem management for root cause analysis.
- Ability to relate existing Known Errors to new problems.
- Automatic recording of Known Errors.
- Auxiliary table to store Workarounds.

Problem Management Overview

The problem management application contains the following areas:

1. [Problem Creation \[page 52\]](#)
2. [Problem Classification \[page 53\]](#)
3. [Problem Investigation and Diagnosis \[page 53\]](#)
4. [Problem Error Assessment \[page 54\]](#)
5. [Known Errors \[page 54\]](#)

6. Problem Resolution [page 54]

1. Problem Creation

Creating a problem is known as submitting a problem in Service Manager. Problems may be submitted directly by the problem management staff or they may be spawned from an incident using the **Post Problem** transition in the Incident Management workflow.

The Submit form enables you to add the following information when creating a problem:

- **Problem Title** and **Problem Description** in the *Overview* section
- **Urgency**, **Impact**, and **Priority** in the *Problem Type* section. For details, see [Urgency, Impact, and Priority \[page 15\]](#).
- **Primary CI**, **Problem Category**, **Sub-Category**, and **Sub-Category Type** in the *Configuration Item* section. The *Problem Category* fields will populate based on the values in the *Primary CI*, but they can be modified. For details on CIs, see [Configuration Management Overview \[page 73\]](#).
- **Reported By**, **Affected User** and **Additional Contacts**. The *Reported By* field is used when the submitter of the item is not the one affected by the issue.
- Under Details, indicate whether a **Tech Note** should be created when the problem is resolved, and add **Work Notes** or **Attachments**.
- **Linked Incidents** tab allows you to link related incidents.



Note: When the problem is created from an incident using the **Post Problem** transition, details from the incident are pre-populated into the Submit form.

To create a problem directly:

1. Select the **Problem** Application tab.
2. On the **Submit** navigation pane, click **Submit to My Preferred Projects**.
3. Select the project to submit into.



Note: You will only be allowed to submit into a project if you have the appropriate permissions.

4. Complete the Submit form with the necessary information.
5. Click **OK** to create the new problem.



Tip: You can find the items that you submitted by using Search by Submitter functionality and searching for items submitted by *Current User*.

When the problem is created, it is assigned a unique item ID and moves to the **Classification** state where it can be classified by the project management staff.

If you selected a configuration item (CI) for the problem, the **Active Problems** tab will show all active problems related to the particular CI and the **CI Relationships** tab will list all of the relationships for the particular CI.

2. Problem Classification

Problem classification involves the triage and assignment of the problem for more investigation. After a problem is submitted, it moves to the **Classification** state, where the project management team can choose to do one of the following:

- Choose to **Investigate** the problem.
- Choose to **Update** the problem with new information.
- Choose to put the problem on **Hold**.
- Choose to **Delete** the problem (option appears if user has the delete item privilege).
- Attach a file to the problem by clicking **Add File** under *Details* or selecting **Add File** from Item Action drop-down.
- Choose an Item Action such as Send an E-mail for the Actions.
- Relate incidents to the problem.



Note: When you choose to relate incidents to the problem, the selected incidents are linked to the problem record, and the problem record is saved. On the **Related Incidents** tab, the related incidents records that were linked are shown.

3. Problem Investigation and Diagnosis

The **Investigation and Diagnosis** state is where the technical SME can investigate the root cause of the problem. The **Technical SME**, who is assigned the problem for investigation, is chosen when you select to **Investigate** the problem from the Classification state.

The Investigate transition lets you attach any necessary supporting documentation or add work notes to the file, supplying the additional information to the SME.

The SME will make use of Serena Service Manager to help diagnose and resolve the problem. **CMS** will be used to help determine the level of impact and to assist in pinpointing the point of failure. The **Known Errors** will be accessed and checked in order to discover whether the problem has occurred in the past, and if so, whether a resolution is already in place. Related problems should be checked to see whether similar problems have been raised previously. Information in these tables is available through the **Active Problems**, **CI Relationships**, and **Linked Incidents** tabs for the problem.

The result of an investigation for a problem will be a root cause diagnosis. The resolution should be the sum of the appropriate level of resources and skills used to find it.

Once the cause of the problem is discovered, it is forwarded to the **Error Control** phase. The information discovered about the cause is entered in the **Work Notes** field.

In addition to entering a root cause, the SME can perform one of the following actions in the *Investigation and Diagnosis* state:

- Choose to **Update** the problem with new information.
- Choose to put the problem on **Hold**.
- Attach a file to the problem by clicking **Add File**.

- Choose an Item Action such as Send an E-mail for the Actions.

4. Problem Error Assessment

Once the causes of a problem have been discovered, the problem goes into the Error Control phase, which is when a resolution to the known error is established. The Error Assessment state is when the SME logs the known error and describes a workaround.

The SME selects the **Error Identified** transition to log the Known Error and workaround. This transition allows the SME to add the details about the Known Error and what the workaround would be. The SME enters information for the Known Error under the **Known Error Notes** field.



Note: The **Error Identified** transition changes the problem prefix to KE, signifying that it is a Known Error. Known Errors are described in the following topic.

After completing the Error Identified transition form, a **Workaround** submit form is displayed, where the SME can enter information about the workaround for the problem. Workarounds are submitted into the **Workarounds** auxiliary table. The items are linked to the problem. This allows incidents that are linked to the problem to be able to refer to the workaround.



Note: You can avoid submitting the workaround at this point and add it in the next state. To avoid submitting a workaround at this time, click **Cancel** on the Workaround Submit Form.

In addition to transitioning the item and adding a workaround, the SME can choose from the following actions in the **Assessment** state:

- Choose to **Update** the problem with new information.
- Choose to put the problem on **Hold**.
- Attach a file to the problem by clicking **Add File**.
- Choose an Item Action such as Send an E-mail for the Actions.

5. Known Errors

In ITIL terminology, when the root cause of a problem is known and there is a workaround, it becomes a **Known Error**. Serena Service Manager changes the problem to a Known Error record automatically during the **Error Identified** transition.

The change from problem to Known Error is noted by the change of the Problem ID prefix from PR to KE. This change allows users to easily discern problems from known errors when looking at a Problems report, such as the report that is displayed on the **Problems** tab for a configuration item. You can also create a report that searches only for items that have a **Problem Type** of Known Error to help find possible solutions.

6. Problem Resolution

Problems can be resolved in a variety of ways. First, there may be a workaround to the problem, explaining how to address the problem when it is encountered. Second, the problem may be caused by an underlying problem in the system that needs to be changed. A change needs to be made in the system at large to fix the root cause of the problem. And third, the problem may have no solution and will have to be lived with. In

this case, you may want to create a tech note in Knowledge Center to alert people about the problem.

These three ways are not mutually exclusive; for example, there may be a workaround but there may still be a problem in the system that needs to be resolved.



Tip: A good practice is to occasionally review all major problems to ensure that the correct steps were followed, how to improve the process overall, and how to prevent recurrence of similar incidents. The reporting functionality in SBM helps to expedite this review process. You can create and share reports listing the major problems that were recently closed, and then share the list with your team.

All three of these approaches may be implemented from the **Error Identified** state in the problem workflow:

- **Add Workaround**, which opens a Submit form into the Workaround auxiliary table.
- **Post RFC**, which opens to the Submit form into the Changes workflow. This change is linked to the item. The problem moves into the Pending Change state. It will be automatically transitioned back to the **Error Identified** state when the change is completed.
- **Resolve**, which moves the known error to the **Resolved** state, where it can be reassessed at a future time.

To create a tech note from the problem, select **Yes** to **Create Tech Note** field. The tech note will be created when the problem is closed with the **Close** transition. The Close transition will open a submit form into Knowledge Management.



Restriction: You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.

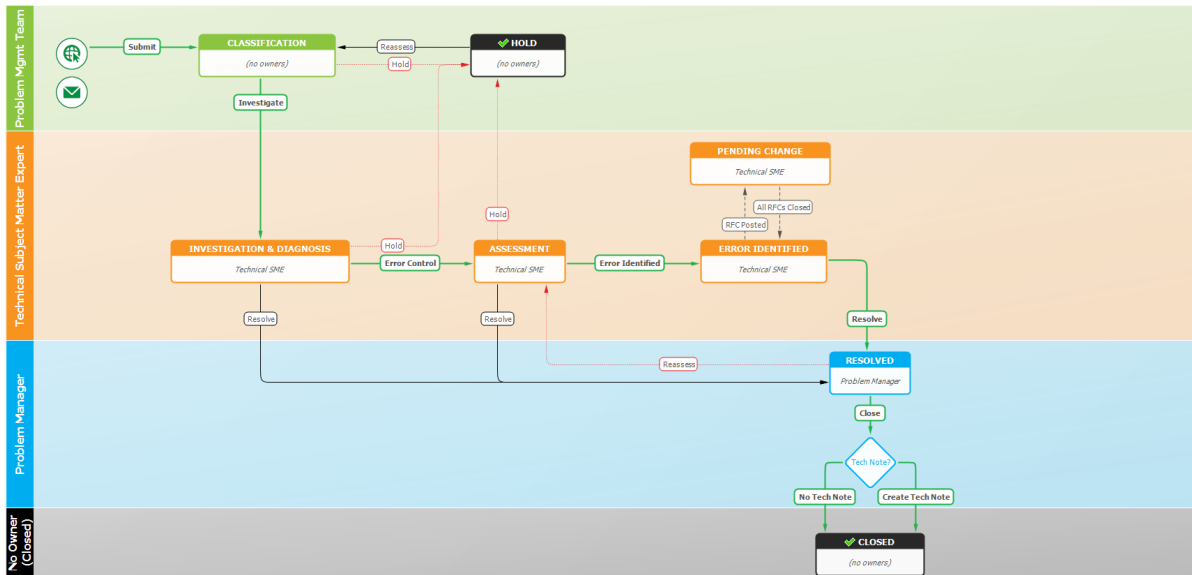


Note: The content fields in the knowledge base article are automatically populated with the content from the problem. Selecting **Load Article Template** will erase the populated information, replacing it with the content from the template.

Problem Management Workflow

The Problem Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Classification* and *Assessment*, and the transitions are marked with arrows, such as *Investigate* and *Hold*. The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.




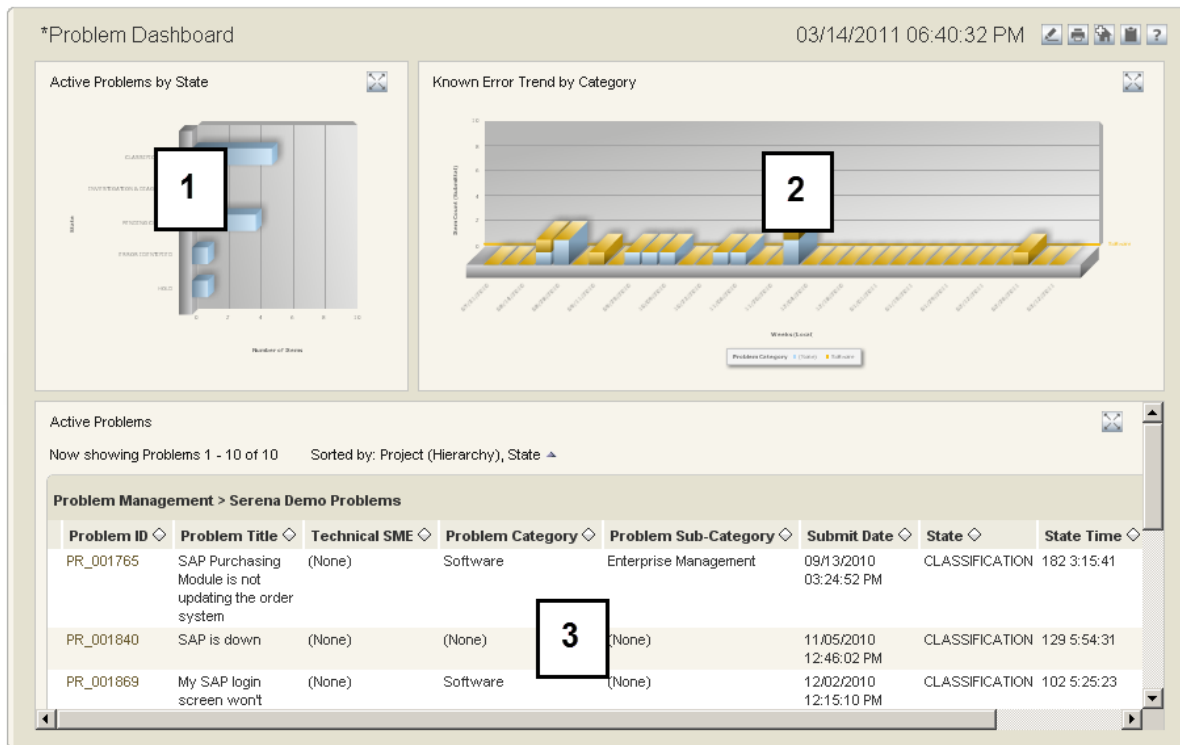
Problem Management Dashboard

The Problem Management dashboard is designed to give managers and staff an overview of existing problems, which states they reside in, what the backlog of problems is, and what the high priority problems are.

The **Problem Dashboard** report is available in the reports that are shipped with the Problem Management snapshot.



Tip: Set the Problem Dashboard report as the home page report for the Problem Management application by opening the **Problems** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



1. **Active Problems by State** shows problems that have not been resolved. The problems are broken down by state. This graph allows the team to see where in the problem management process most problems are.
2. **Known Error Trend by Category** is a graphical trend report, showing the submittal rate of problems over the recent time frame. The submittal rates are divided based on the category of the problem.
3. **Active Problems** lists all problems in active states, such as CLASSIFICATION, ASSESSMENT, INVESTIGATION & DIAGNOSIS, and PENDING CHANGE.



Note: The dashboard report is a multi-view report titled **Problem Dashboard**. You can modify this report to add additional reports that help you to improve your Problem Management process. You can modify the report under the Report pane in the SBM User Workspace.

Problem Management Roles

The following roles (or actors) are available in the Problem Management process app. For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.

Problem Manager - The Problem Manager is responsible for the Problem Management process. Other duties include:

- Ensure efficiency and effectiveness of the Problem Management process
- Initiate proactive Problem Management initiatives

- Provide for continuous service improvement for Problem Management
- Monitor the quality and usefulness of problem records and known error information
- Produce KPI reports for management review
- Maintain the Problem Management system
- Collaborate with other Service Manager processes such as Incident Management, Change Management, and Configuration Management

Problem Specialist - This role is for Technical SMEs and advanced support staff responsible for problem investigation and diagnosis. The responsibilities of this role include:

- Perform investigation and diagnosis to determine the root cause of problems
- Identify, record, and update known error record
- Identify incident trends that might be caused by a technical error

Problem Staff - This role provides information to problem management staff as needed, including technical and business related details.

Problem Submitters - This role is problem submitters who are responsible for providing incident details to Problem Management staff.

PM Administrator - This role is responsible for administering Problem Management, such as assigning users to roles or addressing SBM issues.

Chapter 7: Change Management

Change Management helps ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to controlled IT infrastructure. This minimizes the number and impact of any related incidents upon service operations after changes are implemented.

The Change Management process included with Serena Service Manager is designed to be flexible so that you can tailor the process to your environment. It includes only the basic states, expecting that you will add states and transitions to meet your needs. The default workflow includes basic states such as Classification, Assessment, CAB Review (Change Approval Board), Approved Changes, Implementation, Post Implementation Review, and Successful.

Key Benefits

- Flexibility in implementing tailored change management processes.
- Ability to spawn Requests for Change from problems.
- RFC path through workflow determined by Category Type.

Change Management Overview

The change management application addresses the following areas:

1. RFC Creation [page 59]
2. RFC Classification [page 60]
3. RFC Assessment [page 61]
4. RFC Authorization [page 65]
5. RFC Implementation [page 66]
6. RFC Review and Closure [page 67]

1. RFC Creation

Creating a request for change (RFC) is known as submitting in Serena Service Manager. Requests for change may be submitted directly into the change management process or from another management process using the **Create RFC** transition.



Tip: Automated raising of an RFC when a CI is updated can also be enforced.

When creating an RFC, you add information about the RFC by completing the Submit form. The form contains multiple fields and tabs to enter appropriate information, such as:

- Change Title and Description
- Change Type and Category

- Urgency, Impact, and Priority (For details, see [Urgency, Impact, and Priority \[page 15\].](#))
- Primary CI
- Contact Details
- Announce Change
- Risks
- Communication, Training, and Marketing Plans
- Implementation Plans
- Linked CIs, Problems, and Incidents



Note: If the RFC was created from an incident or problem, the details are pre-populated into the RFC.

To create an RFC directly:

1. Select the **Changes** Application tab.
2. On the **Submit** navigation pane, click **Submit to My Preferred Projects**.
3. Select the change management project to submit into.



Note: You will only be allowed to submit into a project if you have the appropriate permissions.

4. Complete the Submit form with the necessary information.



Note: You can modify the workflow to select which fields are mandatory at each step of the process. For example, the default workflow requires that the submitter selects Change Type and Priority. Your process may require that the Change Manager sets these values when assessing the RFC. You can modify the workflow accordingly.

5. Click **OK** to create the new RFC.

When the RFC is created, it is assigned a unique item ID and moves to the **Classification** state where the change manager will determine how the change will be addressed.



Tip: You can find the items that you submitted by using Search by Submitter functionality and searching for items submitted by *Current User*.

2. RFC Classification

Once the RFC has been created, a preliminary assessment needs to be made of its importance. This occurs when the item is in the **Classification** state.

All fields are available for editing when you are updating or transitioning an item from the **Classification** state. This allows the change manager to modify the proposed values for priority, urgency, and category type that were selected by the submitter.

The change manager must determine what type of change the RFC is. The **Change Type** value controls which paths are available for the change to take through the workflow. For "standard" changes, the change manager can choose to **Pre-Approve** the change. In ITIL, "standard" changes refers to those changes that are commonly performed, such as password resets or user account provisioning. These "standard" changes are pre-approved, and therefore there is no need to go through the normal approval process. The changes skip the CAB and move directly from the *Classification* state to the *Approved Changes* state. For regular changes, the change manager selects the **Normal** type. Normal changes move through the entire workflow. The **Emergency** change bypasses the *Assessment* state and moves directly to the ECAB (Emergency CAB), which is a subset of the CAB. ECAB is convened to handle emergency RFCs.



Tip: Emergency changes must be responded to immediately, and the procedure to be followed in such cases must be planned for. It is possible to create a notification in SBM to inform ECAB members about Emergency RFCs that must be responded to immediately.

From the **Classification** state, the change manager can choose from a variety of options, depending on the value of the Change Type:

- An RFC may be *accepted*, which does not mean that it will subsequently be approved by the CAB, only that it is sufficiently justified to be given further consideration.
- An RFC may simply be *rejected* if it is felt that the change is not justified.
- An RFC may be *deferred* back to the originator, who can modify the item and then *re-open* it after the change is defined more clearly.
- An RFC may need to be *assessed* further by the change manager before being sent to the CAB.
- A pre-approved RFC can be *implemented* immediately without moving to the CAB.



Note: If the RFC was not submitted with linked items, the **Linked Items** tab does not appear on the **Classification** state form. The change manager must select to **Update** to add linked items such as problems, incidents, or other CIs.

3. RFC Assessment

A preliminary assessment occurs in the **Classification** state when the change manager determines the change type and where to route the change; however, a deeper assessment may be required. When this is the case, the change is routed to the **Assessment** state where a change manager can further assess the change.

When assessing the RFC, the change manager needs to set the appropriate values for the priority and category. Priority and Change Category are important settings for the RFC process in ITIL. The *Priority* determines the relative importance of the RFC in relation to other outstanding RFCs and it should be the main basis of when pending changes are scheduled. The Change Category determines the difficulty and impact of the RFC and will be the main parameter used to determine the resources that need to be allocated. The default Change Category types are:

- Minor
- Significant
- Major

Assessment also involves calculating the possible risk in implementing the change. The Risk Calculator on the **Risk** tab automatically determines the risk based on the change category, estimated effort, and an array of survey questions. For more information, see [Risk Analysis Calculator \[page 62\]](#).

Following assessment, the change manager **accepts** the RFC, and the RFC transitions to the Change Approval Board (CAB) for approval.



Note: Financial and Effort estimates are required for items that go through the Assessment phase.

Risk Analysis Calculator

The Risk Analysis calculator determines how the change affects business critical services. The Risk Calculator uses the change category, the estimated effort, and a group of questions to determine the risk level of the change.

The Risk Analysis calculator appears on the **Risk** tab of an RFC. The risk level is determined to be either **Low**, **Medium**, or **High** based on the weighted answers to the survey questions, the change category, and the estimated effort. The default ranges are: **Low** is less than or equal to 20; **Medium** is 21 to 40; **High** is greater than 40.



Note: **Total Risk Score** contains the summation of the weighted answers to the survey.

On the **Risk** tab, the risk level only displays when the **Risk Analysis Completed** field is set to **Yes**. This ensures that users have answered the risk survey before calculating the risk level. If the risk survey has not been completed and **Risk Analysis Completed** remains set as **No**, the risk level displays **Questionnaire Not Completed**.



Tip: When creating a report to show high risk items, remember to include both items which have a high **Total Risk Score** and items which have a change category set as **Major** and their **Risk Analysis Completed** field set as **No**. Items without a completed risk survey will show a lower overall risk level since the risk level sums the survey responses and a null response is given a weight of zero.

The following are the default questions and weighted answers (default weights) in the Risk Analysis questionnaire:

- 1. Does the change affect business-critical services?**
 - High Impact: Service temporarily unavailable / major changes (10)
 - Low Impact: Small upgrade, some features temporarily unavailable (5)
 - No Impact (0)
- 2. Does the change affect major IT infrastructure components?**
 - High Impact: Components taken offline / major service impact (10)
 - Minor upgrade or temporary performance degradation (5)
 - No Impact (0)
- 3. Will the change be tested prior to implementation in a development or test environment?**

-
- Yes (3)
 - No (7)
4. **Is the implementation well understood and documented?**
- This process has been done in the past and is repeatable (0)
 - This process is similar to one done in the past (5)
 - This is a completely new process or implementation (10)
5. **What is the implementation time?** *This field is set automatically based on the value entered in the Estimated Effort field for the change request. It can also be manually modified by choosing a selection in the list. The Estimated Effort field appears on the Implementation tab for a change request. This tab appears when approving a change.*
- 4 hrs or less (0)
 - 4 hrs to less than 1 day (5)
 - More than 1 day (10)
6. **What is the change complexity?** *This field is set automatically based on the value of the Change Category.*
- Minor (0)
 - Significant (5)
 - Major (10)

Modifying the Risk Calculator and Survey

You can modify the risk calculator and survey so that it reflects your company's processes. This topic describes how you would modify the calculator and survey.

The Risk Calculator uses a summation field to add the values of the weighted selections. The summation value is then evaluated using a JavaScript which adds a risk level of either **Low** (0-20), **Medium** (21-40), or **High** (>40).

The Risk Level is configured to only display a result when the **Risk Analysis Completed** binary field is set to **Yes**. This field is automatically updated by a JavaScript to **Yes** if any of the four survey fields contain an answer. After being set to **Yes**, the weighted values are summed and the results displayed. If not, the Risk Level displays **Questionnaire Not Completed**.

You can modify the risk survey and calculator, such as the risk level thresholds, the questions, or the weightings of the answers. The modifications are performed within SBM Composer, and then the changes are deployed to your server.

The following are some changes that you could make to the survey:

- Make the survey mandatory by marking all of the fields as **Required**.
- Modify the weighted responses to questions by selecting to edit the field and setting the weighted values on the **Options** tab of the **Property Editor** for the field.

- Change existing questions and answers by modifying the field names and descriptions in the **Property Editor** for the field.
- Add new questions by adding single selection fields with weighted values. To add the new questions, you must:
 - Modify the summation field (**Total Risk Score**) to include the weighted value in the result.
 - Add the new field to **Risk** tab on every form in the Change Management process application.
 - Add the field name to the JavaScript contained in the **calcRisk_Transition** HTML/JavaScript widget. This script is responsible for checking if the question is answered. The following example of how you would add a new field is an excerpt of the JavaScript:

```
AddChangeCallback("ESTIMATED_EFFORT", funcLinkEstimatedEffort);
AddChangeCallback("RISK_ANALYSIS_Q1", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q2", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q3", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q4", funcAnalysisCompleted);
AddChangeCallback("RISK_ANALYSIS_Q5", funcAnalysisCompleted);
AddChangeCallback("NEW_FIELD_NAME", funcAnalysisCompleted);
```

- Change the range for how risk is calculated by editing the JavaScript on the state forms. The JavaScript is contained in the **calcRisk_State** HTML/JavaScript widget. For example, you would make the following change to add an additional risk category for Medium-High for risk scores between 31 and 40:

```
<script type="text/javascript">
AddLoadCallback(calcRisk);
function calcRisk() \{
var answered = GetFieldValue("RISK_ANALYSIS_COMPLETED");
if(answered == "Yes") \{
var score = parseInt(GetFieldValue("TOTAL_RISK_SCORE", 0));
if(score > 40) \{ SetFieldValue("RiskScoreLabel", "(High Risk)"); }
else if( score > 30) \{SetFieldValue("RiskScoreLabel", "(Medium-High Risk)"); }
else if( score > 20) \{SetFieldValue("RiskScoreLabel", "(Medium Risk)"); }
else \{ SetFieldValue("RiskScoreLabel", "(Low Risk)"); }
\}
else \{
SetFieldValue("RiskScoreLabel", "(Questionnaire Not Completed)");
\}
\}
</script>
```

- Change how the estimated effort is weighted by modifying the JavaScript on the transition forms. The JavaScript is contained in the **calcRisk_Transition** HTML/JavaScript widget. For example, to set everything under 1/2 day (12 hours) as low impact and everything else as high impact:

```
<script type="text/javascript">
var funcLinkEstimatedEffort = function()\{
```

```

var effort = GetFieldValue("ESTIMATED_EFFORT", "");
var implTimeFld = GetFieldByName("RISK_ANALYSIS_Q5");

if(effort != "") \{
  //Convert Estimated Effort field from milliseconds to hours
  var hours = effort / 3600000;

  if(hours > 12) \{ implTimeFld.selectedIndex = 3; \}
  else \{ implTimeFld.selectedIndex = 1; \}

  DisableField("ESTIMATED_EFFORT");
\}
\}

```

For more information on working with fields, refer to the *SBM Composer Guide*.

4. RFC Authorization

Information management systems are highly sensitive to configuration changes due to the complex relationships between all the CIs involved. An apparently minor change may trigger a chain reaction with catastrophic results. The **Change Advisory Board (CAB)** is responsible for evaluating the changes and discussing the possible side-effects of the change before giving their approval.

The CAB is usually chaired by the change manager, and its members include other service management managers. The CAB may also include other stakeholders such as customers or other third-party providers. In the case of high impact changes, upper management may need to be consulted as strategic issues and the organization's general policy may come into play.



Note: The default change management workflow assumes that the CAB would be conducted offline, and the change manager would then approve the RFC on behalf of the CAB. The default workflow can be modified to allow individual CAB approvals. One approach to allow individual approvals is to use the subtasking capabilities of SBM. Subtasks can be created and assigned to each selected CAB member, and then they can approve or reject the individual tasks, and the results can be displayed in the parent RFC.

The CAB must meet regularly to analyze and approve the pending RFCs. The members discuss the benefits of the RFC and verify that a back-out plan exists in case the change does not work as expected. They decide the date of when the RFC should be implemented, assess the effort, and assess the cost.

The CAB also discusses possible risks, services that are affected, impacts to business continuity, and disaster recovery. The results and decisions of the discussion should be collected and entered in the RFC. The details can be entered directly into the text fields or they can be attach supporting documentation using **Add File**.



Tip: Once the change has been approved, it can be assessed whether it should be implemented in isolation or as part of a package of changes that would be formally equivalent to a single change. This approach optimizes the use of resources, reduces the incompatibilities between different changes, and simplifies the back-out plan. Change managers can link RFCs by creating a principle RFC and then grouping the RFCs together using the subtasking capabilities of SBM.

Announcing a Change

The option to **Announce Change** enables you to post an Announcement to Knowledge Management after completing the **Approve** transition from **CAB Review**.

When **Announce Change** is set to **Yes**, the submit form into Knowledge Management will display after completing the **Approve** transition.

The content for the new Announcement will be populated with information from the article. The start date for the *Announcement* be set to the *Implementation Start Date* from the change.



Restriction: You must have permissions to submit an item into Knowledge Management to create an article. For example, you could be a member of the **Contributors** role in Knowledge Management.



Note: Selecting **Load Article Template** on the **Content** tab will erase the information that was imported from the change. The content will be replaced with the template.

5. RFC Implementation

The responsibility for implementing a change usually falls in the realm of the Release Management; however, the Change Management team remains responsible for overseeing and coordinating the implementation of the changes. The change management team usually helps to monitor that:

- Schedules are met and the appropriate resources are assigned.
- Software is developed and hardware is purchased according to specifications.
- The test environment is realistic and simulates the live environment.
- Back-out plans are created that will allow the last stable configuration to be recovered rapidly.

The default Change Management workflow is designed with the assumption that implementation steps vary between companies, and that the steps would be tailored according to the company's processes. The workflow contains only one state, **Implementation**, where the *Implementer* is assigned as the primary owner and the *Implementation Team* acts a secondary owner.

This process can easily be enhanced to meet your needs. Here are some examples:

- Add additional states to the change management process to track the implementation steps.
- Link the change management process to your existing release management process using Web services.
- Use subtasks to track the implementation tasks, automatically transitioning the RFC when the subtasks are complete.

After the implementation is complete, the RFC moves to the Post Implementation Review state, where the change manager conducts a review of the RFC before closing it.

6. RFC Review and Closure

After the implementation is complete, the RFC moves to the **Post Implementation Review** state, where the Change Manager can conduct a review of the change. This is known as a Post Implementation Review (PIR).



Note: By default, the Change Manager is notified when a change is transitioned to the Post Implementation Review state.

The review allows the real impact of the change on the organization's quality of service and productivity to be assessed. Some of the basic points to take into account are:

- Were the objectives met, and if necessary, were there any restrictions?
- Did the process deviate from the original plans?
- Were there any unexpected problems?

The PIR also verifies that all of the information related to the implementation is entered into the Change Record, such as the Objectives, Beginning and End dates, Time and Effort, Cost, and Lessons Learned.

If the final evaluation finds the process and results to have been satisfactory and the information entered in the RFC, the RFC can be closed using the **Complete** transition.

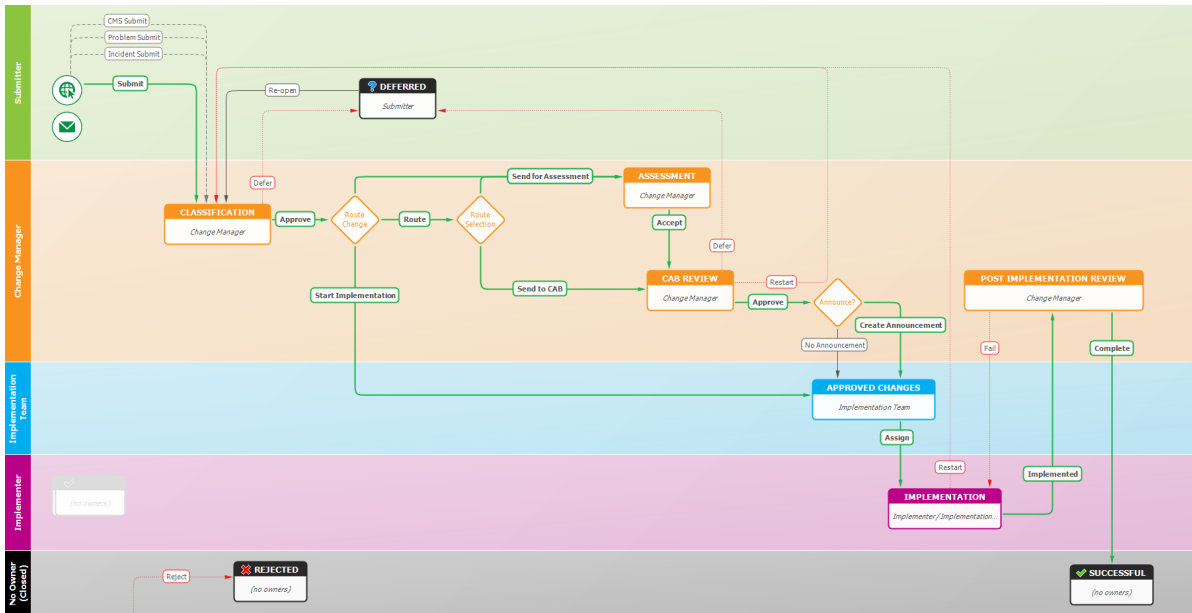
Items that raised the RFC are automatically transitioned to the next state when the RFC is closed. For example, if the RFC was raised from a problem, moving the problem to the Pending Change state. When all of the RFCs are closed, the **All RFCs Closed** transition is automatically performed, moving the problem back to the **Assessment** state.

Change Management Workflow

The Change Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Deferred* and *CAB Review*, and the transitions are marked with arrows, such as *Reject* and *Accept*.

The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.




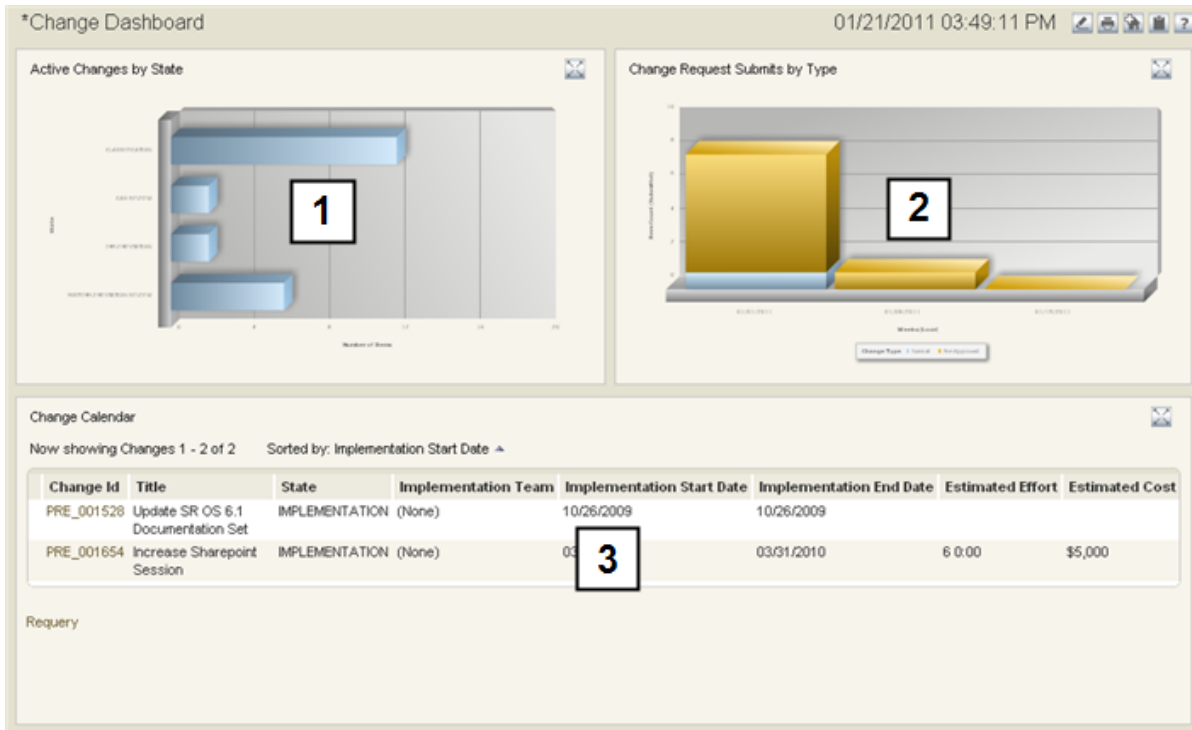
Change Management Dashboard

The Change Management dashboard is designed to alert change management staff to emergency RFCs and how long other RFCs have been active.

The **Change Dashboard** report is available in the reports that are shipped with the Change Management snapshot.



Tip: Set the Change Dashboard report as the home page report for the Change Management application by opening the **Changes** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



1. **Active Changes by State** displays the number of changes in each state.
2. **Change Request Submit by Types** breaks down by type how many changes are submitted over the past few weeks.
3. **Change Calendar** shows the scheduled changes and when the changes are scheduled for.




Note: The dashboard report is a multi-view report titled **Change Dashboard**. You can modify this report to add additional reports that help you to improve your Change Management process. You can modify the report under the Report pane in the SBM User Workspace.

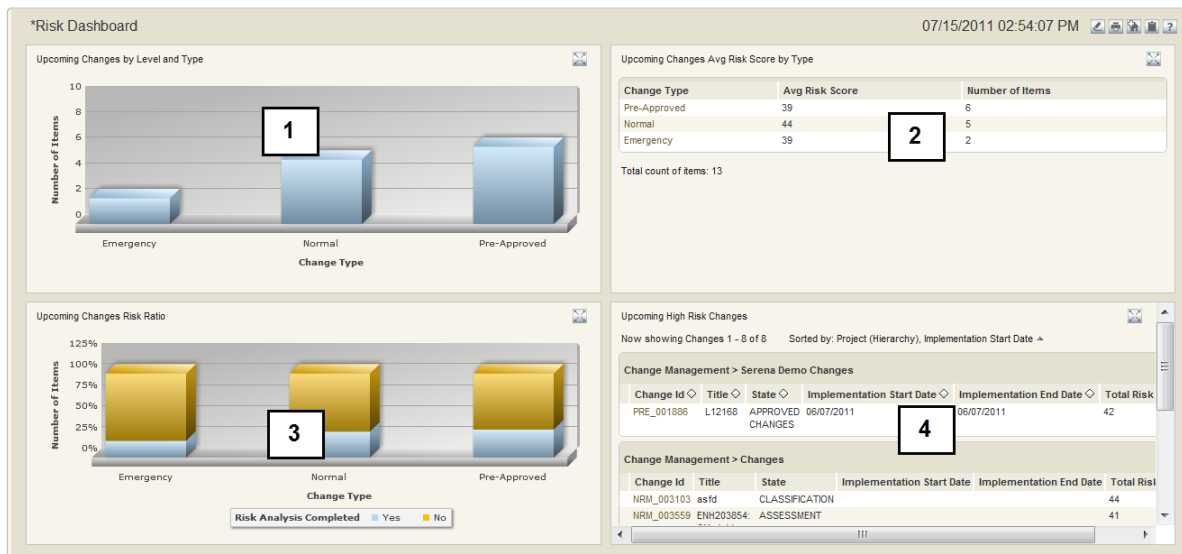
Risk Dashboard

The Risk dashboard is designed to alert change management staff to the risk of upcoming RFCs. The reports on the dashboard make use of the Risk Analysis survey and the Risk Calculator to determine the risk of the changes.

The **Risk Dashboard** report is available in the reports that are shipped with the Change Management snapshot.



Tip: Set the Risk Dashboard report as the home page report for the Change Management application by opening the **Changes** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



- Upcoming Changes** displays the number of upcoming changes broken down by change type. These changes have a completed Risk Analysis survey.
- Upcoming Changes Avg Risk Score by Type** breaks down the average risk score for the upcoming changes based on change type.
- Upcoming Changes Risk Ratio** shows the upcoming changes which have a completed Risk Analysis survey compared to the changes that do not have a completed survey.
- Upcoming High Risk Changes** has a list of upcoming changes with a risk score greater than 39. The items are sorted based on implementation start dates.



Note: The dashboard report is a multi-view report titled **Risk Dashboard**. You can modify this report to add additional reports that help you to improve your Change Management process. You can modify the report under the Report pane in the SBM User Workspace.

Change Management Roles

The following roles (or actors) are available in the Change Management process app. For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.

Change Manager - The Change Manager is responsible for the Change Management process, making sure that standard procedures for change are followed. Other duties include:

- Ensure efficiency and effectiveness of the Change Management process
- Manage Change Management staff
- Provide for continuous service improvement for Change Management
- Schedule regular configuration item verification and audits

-
- Produce KPI reports for management review
 - Manage Forward Schedule of Change conflicts
 - Conduct the Change Approval Board meetings on a regular basis
 - Maintain the Change Management system
 - Collaborate with other ITSM processes such as Problem Management, Issue Management, and Configuration Management

Change Implementer - This role is for change management staff who are responsible for implementing the change. The responsibilities of this role include:

- Own requests from implementation to closure
- Ensure that prior approval has been granted before executing the change
- Collaborate with requesters with the goal of implementing the requested change
- Inform change management staff of request status and resolution
- Coordinate with release management to ensure that processes are followed
- Provide Post Implementation feedback during PIR (Post Implementation Review)

Change Requester - This role is for the end users who will be submitting RFCs, providing the necessary details to the change implementers.

Change Administrator - This role is responsible for administering Change Management, such as assigning users to roles or fixing SBM issues.

Chapter 8: Configuration Management System

The Configuration Management System (CMS) process oversees the lifecycle of the Configuration Items (CIs) through the fundamental elements of identification, status accounting, and audits. From initial activation to final deactivation, the CMS process enables you to track your IT Assets.

This CMS solution contains the **CI Relationships** application, which is used to store relationship information between your CIs. This information allows you to see how items relate to each other, and how dependencies among items affect your IT services.

- [Configuration Management Overview \[page 73\]](#)
- [CMS Workflow \[page 81\]](#)
- [CMS Dashboard \[page 81\]](#)
- [CMS Roles \[page 82\]](#)

Key Benefits

- Configuration Management Database with CI categorization according to ITIL.
- Management of complete Configuration Item lifecycle.
- Ability to create relationships between CIs and view relationships in a graphical format.
- Links between CIs and other items (such as Incidents, Problems, or Changes) enable quick problem diagnosis and change control of assets.

Configuration Management Overview

The configuration management application contains the following areas:

1. [Configuration Identification \[page 73\]](#)
2. [Configuration Control \[page 77\]](#)
3. [Audit and Verification \[page 79\]](#)
4. [Status Accounting \[page 79\]](#)

1. Configuration Identification

Creating and identifying Configuration Items (CIs) is the process in which new items are defined and added to the Configuration Management Database. Once an item has been added, it can be tracked and managed through its workflow. This enables you to perform the necessary audits using the reporting capability found in SBM.

New items can be created either automatically based on an event raised from another tool or manually from within SBM. Other tools that can be configured to raise events include

other Asset Management Systems or Asset Discovery Systems. New items may need to be created from within SBM based on a Request for Change (RFC), Service Request for new hardware, or the results of an Audit where items were discovered not to exist in the system.




Note: Raising and receiving events within SBM requires knowledge of Web services and SBM orchestrations. If you do not have in-house expertise, contact Serena Professional Services, who can help you modify your Service Manager implementation to communicate with third party tools.

When you create or classify a CI, some fields have predefined values, such as the Category and CI Type fields. The predefined values enable you to select the appropriate entry for the item. The defined values create consistency among your configuration items, which in turn helps when searching for existing configuration items to relate to an incident or problem. In addition, the defined information improves the audit and report results for managing your configuration items.

The defined values are available from the drop-down lists on the Submit form. In the default Service Manager, values can be defined for CI types, Status, Categories, Sub-Category, Sub-Category Type, and Manufacturers. Note that the Sub-Category and Sub-Category Type include relational fields, which means that you must select a value in the related field before they will populate with values. For example, you must select a Category before values will appear in the Sub-Category field. And when you select a sub-category, the Sub-Category Type drop-down list will be populated.



Tip: Some selection lists are populated from auxiliary tables, such as Category, Sub-Category, and Manufacturers. If you have permission to edit the table, you can add or modify selections by selecting , navigating to the auxiliary table (**Search | Manage Data**), or using an Editable Grid report run against the auxiliary table.

Other lists are defined in the process app using SBM Composer. Updating these values requires that you redeploy the process app.

Some of the fields in CI items are free-form text fields, which allows flexibility when defining items. Examples of these fields are CI Name, Description, Maintenance Window, and Serial Number.

Your configuration management solution is customizable so that you can add fields to specify additional data, such as a date field of when the warranty expires. Custom fields can be added to the process app within SBM Composer and then deployed to your server.

After you complete the submit process by clicking **OK** on the submit form, the CI is created. It is assigned a unique identification number and it moves to the Classification state, where it is assigned to a Configuration Analyst. The analyst can choose how to proceed with the item. The analyst could choose to modify the CI by selecting to **Update** the item, and then choosing appropriate values for the item. If the analyst feels the CI is ready to activate or publish, the analyst clicks **Activate**. The configuration item is now live in the system, and it resides in the **Active** state in SBM until it is audited, inactivated, or disposed.



Note: Functional and access privileges to configuration items are role-based and your role is defined by your administrator. Depending on your privileges, you may not be able to create new items, update items, or add relationships to items. Field attributes may also be classified, and access to each data classification can be granted according to your role. The right to transition changes from one state to another can also be controlled by the role privileges.

About Relationships

Service Manager stores not only your configuration items, but the relationships between the configuration items as well. Knowing these relationships helps you understand what may happen when an asset is modified. For example, your company's internal Wiki may be *hosted on* server A. If a change occurs to Server A, it can affect the internal Wiki.

In addition, relationships can be used to group CIs together under one main CI. For example, an IT service such as the ERP application can be defined as a CI, which is made up of an application, database, server, and network components to provide that IT service.

Relationships between active Configuration Items are displayed using the Relationship Explorer. The Relationship Explorer graphically depicts the relationships between the currently displayed item and other items. You can view the related items by selecting them from the graph. The Relationship Explorer displays on the **Relationships** tab for an active configuration item, and on the **CI Relationships** tab for the Incident, Problem, and Change processes.



Note: The arrow in the Relationship Explorer points from the Primary CI to the Related CI, that is the Primary CI is the item that was specified as the Primary CI when creating a relationship. By default, the item which you are creating the relationship from is populated as the Primary CI.



Important: When a new version of CI replaces an existing CI, the relationships are automatically transferred to the new version of the item.

Adding a Relationship

To add a relationship to a CI:

1. Open the active CI.
2. Select the **Relationships** tab and click **Add New Relationship**.
3. A Submit form displays to the Relationships auxiliary table. The current CI is automatically chosen as the Primary CI.
4. Select the **Relationship Type** and the **Related CI**.
5. Click **OK** to submit the form.
6. After the relationship is added, it will appear on the **Relationships** tab of the item. The **Relationships** tab shows all CI relationships to or from the active CI.



Note: Configuration item relationships are stored in the **Relationships** auxiliary table of the CMS process app.

Removing or Modifying Relationship

To remove or modify a relationship from a CI:

1. Open the active CI.
2. Select the **Relationships** tab.
3. Expand the **Relationship Maintenance** section. This section displays the primary relationships associated with the item.

4. On the report results, select the relationship to modify or delete. The relationship appears in a new tab.
5. Select from the available options to **Update** or **Delete** the relationship.

Navigating Relationships

The Relationship Explorer displays the relationships to the CI in a tree format. The main CI appears with a red border and is *centered* in the Relationship Explorer. By default, one level of relationship upward from the centered item is displayed, and up to five relationships downward.

Choose from the following actions on the graph:

- Display the details of an item in the graph by clicking on the title of the item.
- Focus the graph on another item by clicking the title bar of that item. This centers the graph on that item. You can recenter to the original CI by clicking **Restore**.
- Change the layout of the graph by choosing either **left to right** or **top to bottom** from the drop-down list.
- Zoom in by clicking **Full Size**. See the entire set of connections by clicking **Full View**.



Tip: Vary the zoom level using your mouse wheel.



Note: The Relationship Explorer uses an AppScript to create and populate the graph. The **ServiceManagerGraphFromNode** AppScript is in the CMS process app and contains configuration criteria, such as the number of connection levels to display in the Relationship Explorer. See the AppScript for more details.

Adding a New Relationship Type

You can add, modify, and delete relationship types. The available relationship types are contained in the **Relationship Types** auxiliary table of the CMS process app.

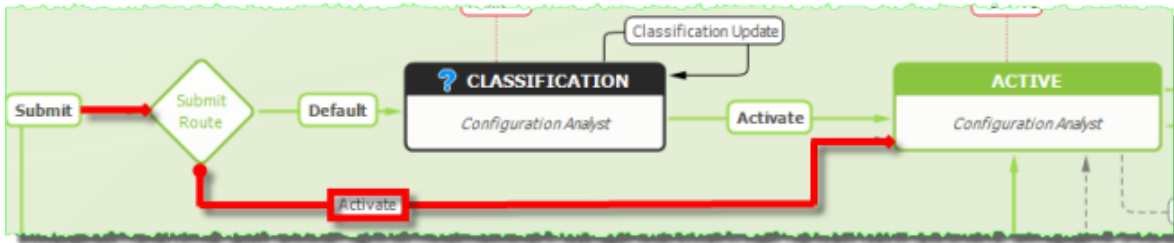
To access the relationships:

1. Open the **Relationship Types** auxiliary table by running a report against it or by selecting **Search | Manage Data**.
2. Choose to modify, delete, or add a relationship type.

Creating CIs from Events

When the Service Manager adapter issues an event, the event triggers the creation of a configuration item.

The submission from the connector is populated with specific information that allows the new CI to be automatically routed to the **Active** state, by passing the **Classification** state.



Note: Any submission that has these keys populated is auto-routed to the active state. Items manually submitted go to the **Classification** state.

2. Configuration Control

Service Manager configuration management has a set of processes and approvals that are required to change a configuration item's attributes. ITIL best-practice recommends that changes to CIs require an RFC. The default Service Manager configuration enforces the need of an RFC for certain changes to the CI. The RFC captures the details of the change, and it is managed by the Changes workflow, which enforces the collection of appropriate approvals and tracks the implementation steps.

The management of configuration items (CIs) may span across other process teams in addition to the configuration management team. For example, before a request for change is implemented, the attributes of the associated CI may need to be validated against the RFC by the change management team. And then after the change is implemented, the validation may be done again by the configuration management team to ensure consistency.

After the RFC has been approved and the changes made, SBM automatically baselines the existing CI and records the changed information. See [Understanding Baselines \[page 78\]](#) for more information on how baselines work in Service Manager.



Note: Updating from an RFC is different from using the **Update** transition on the item directly. The **Update** transition prevents modification of some fields such as version number. These fields can only be modified using an RFC.

The ability to create, manage, and update CIs and their attributes depends on how administrators assign roles within configuration management. Access privileges may grant read-only access for some roles, but update privileges for other groups. Data attributes can also be classified, and access to each data classification can be granted via the role. The right to transition changes from one state to another can also be controlled by the role privileges. Details of the roles in Configuration Management are described in [CMS Roles \[page 82\]](#).

Administrators can manage the workflow of CIs by determining owners for each state. Administrators can set rules that determine who the owner will be based on the CI attributes, which automates the workflow by automatically assigning items to the correct owner.

The fields that contain the CI attributes can be configured to be required or optional. You can fine-tune the requirements by marking the field as mandatory throughout the life-cycle of a configuration item (CI) or only for certain transitions from one state to another. Field settings are customized using SBM Composer.

Understanding Baselines

Baselines identify the significant states within the revision history of a configuration item. They capture the changes that were approved and implemented for a particular version of an item. By comparing the active item with its previous baselines, you can view the modifications that occurred between CI versions.

Service Manager uses separate items in the CMS workflow to track active CIs and baselines. The state of the item in CMS workflow determines whether the item is an active CI, an active baseline, or an inactive baseline. Links exist between baselines and active CIs, which allows Service Manager to track the baselines associated with each active CI.

The complete process for creating a new active CI and baseline using an RFC is as follows:

1. RFCs are required for a change to a CI. When you submit an RFC against an active CI, a new CI is also submitted. The new CI is placed in the **Pending Change** state, where it remains until the change is completed. The new item is linked to the active or original CI, and it is prepopulated with information from the existing CI. You can find a link to active CI from the new CI on the **Config Item** tab. You will see the version number has been incremented automatically on the new CI.
2. The original CI moves to the **Baseline Pending** state, informing you that a new CI is in process of being implemented.
3. After the RFC is closed, the new CI moves to the **Verification Required** state, where the change is verified by the Configuration Analyst to ensure that it matches what was expected.
4. After being verified, the new CI becomes the active CI. The original CI transitions from the **Pending Change** state to the **Active Baselines** state, marking it as a baseline.
5. You can see related active baselines for a CI by displaying the report on the **Baselines** tab.
6. A baseline can replace the active CI by selecting to **Restore** it. This creates an RFC and a duplicate of the baseline item. After the RFC is completed, the duplicate item will become the new Active CI.

In summary, an item in the CMS workflow can have the following possible designations as it moves through the workflow:

- An **Active CI** CI is the current version of the CI.
- A **Pending Change** is an item that is waiting for an RFC to be complete before it becomes the active CI.
- An **Active Baseline** is a non-current version of the CI. It resides in the **Active Baselines** state. You can see the active CI on the **Config Item** tab. An Active baseline does not display the other baselines on the **Baselines** tab. The report will be empty.
- An **Inactive Baseline** is a version of the CI that has been deactivated. Deactivated baselines do not appear in the Baselines report that appears on the **Baselines** tab. You can find inactive baselines by running a report against the CMS project which contains the baseline items. Remember to include inactive items in your report.

Keep in mind the following when working with baselines:

- All opened RFCs must be closed before the CI will transition to the next state. That is, if you have multiple RFCs opened up for one CI, all of these issues must be closed before the CI becomes the new active CI.

3. Audit and Verification

Audit and verification checks for the existence and accuracy of information contained in the CMDB against the actual asset. If any exceptions are realized, then the CMDB has to be updated appropriately.

In Service Manager, a configuration analyst can choose to audit an item by selecting the **Audit** transition and adding any applicable Work Notes. The CI moves to the Audit state, where the CI is verified. If a discrepancy is found or a change is required, the configuration analyst can choose from a variety of transitions to determine what happens to the CI:

- **Verify** – To mark the CI as verified against the actual asset, returning the CI to the Active state.
- **Not Found** – To mark an item as not found.
- **RFC Posted** – To raise a Request for Change to fix an issue or exception found during the audit.
- **Dispose** – To mark an item as disposed.
- **Inactivate** – To mark an item as inactive.



Note: Service Manager supports the process of auditing and verification, but the actual act of auditing or verifying a configuration item has to be performed by a member of the configuration management team.

Configuration items, their versions, and their changes form the basis of any configuration audit, and SBM enables you to create and run reports on these items. Service Manager comes with some default reports, and users can create additional reports by selecting **Create Reports** in the **Reports** pane of the SBM User Workspace.

Some of the out-of-the-box reports include:

- CIs by State
- CIs by Type
- Disposed CIs
- Missing CIs
- Active Incidents, Problems, and Changes linked to CIs

4. Status Accounting

Status accounting for configuration items (CIs) refers to the ability to record and report on the status of all CIs that are under control of the Configuration Management System (CMS).

Any activity performed on the CI from creation to disposal is recorded, providing an audit trail throughout the CI lifecycle. Records are marked with the activity date and ID of the individual who performed the action. This means that you can see when and who updated items, performed transitions, or added relationships to a particular item.

Status information is used for successful configuration audits, where the configuration management team wants to see the current status of the CIs. For reporting by the service management team, Service Manager comes with many out-of-the-box reports that are used to find the status of your CIs. In addition, you can easily create custom reports to display information that you require.

Status information may also be needed by other service management processes, such as Change Management and Problem Management, to relate new RFCs, problems, and workarounds to particular configuration items. Other Service Manager processes link directly to the configuration management application, enabling you to find CI information from within the context of the other process. For example, the incident management, problem management, and change management processes require that you choose a CI to relate to the new issue, and this can be performed directly from the form using the relational field search box.

SBM reports are important for keeping up-to-date on your configuration status. Status reports should be produced on a regular basis and include:

- Lists of all CIs under control, their current version, and change history
- Status accounting reports on the current, previous, and planned states
- Unique identifiers of constituent CIs and their current status
- Configuration baselines, releases, and their status
- Latest software item versions and their status for a system baseline
- Persons responsible for making status changes
- Change history and audit trail
- Open Problems and RFCs.

Status accounting reports can be used to establish system baselines and enable Changes between baselines and Releases to be traceable. Status reports may include:

- Baseline and release identifiers
- Latest software item versions for a system builds
- The number of changes for a system
- The number of baselines and releases
- The usage and volatility of CIs
- Comparisons of baselines and releases.

In addition to reports, notifications can be used to keep informed about CIs. SBM enables users to subscribe to notifications for changes to CI, such as a state transition or an update. Service Manager comes with default notifications. Additional notifications can be created and configured using SBM System Administrator. For example, you may be

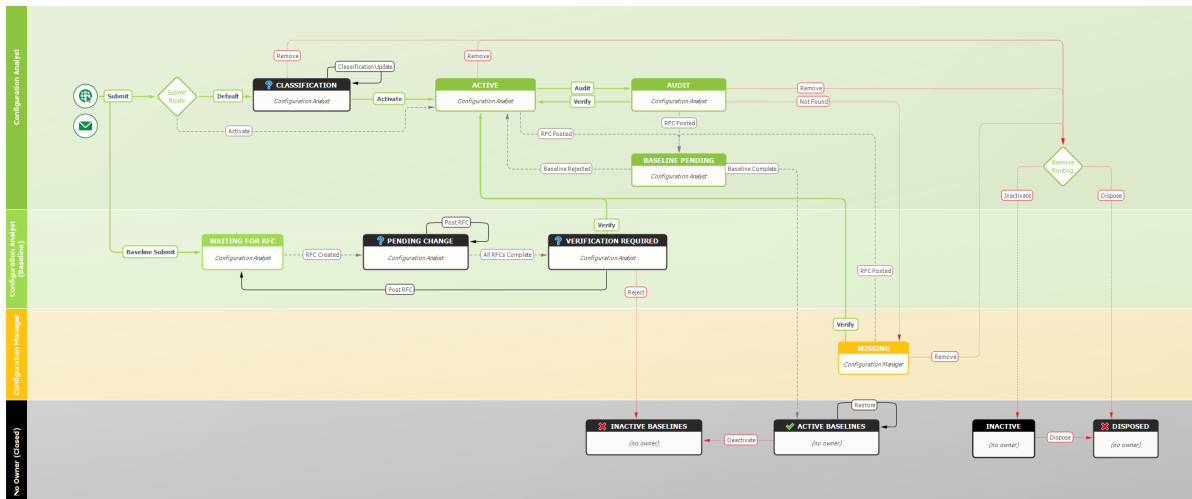
responsible for your production servers, and you want to be notified whenever a CI item related to servers is updated. Your administrator can create a notification that looks for certain conditions, such as updates on items related to production servers, and then sends an e-mail notification when the event occurs. An end user can subscribe to any notification to which they have access by configuring the notifications under their **User Profile** in the SBM User Workspace.

CMS Workflow

The Configuration Management System workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Active* and *Audit*, and the transitions are marked with arrows, such as *Close* and *Activate*.

The process starts with the **Submit** and can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.




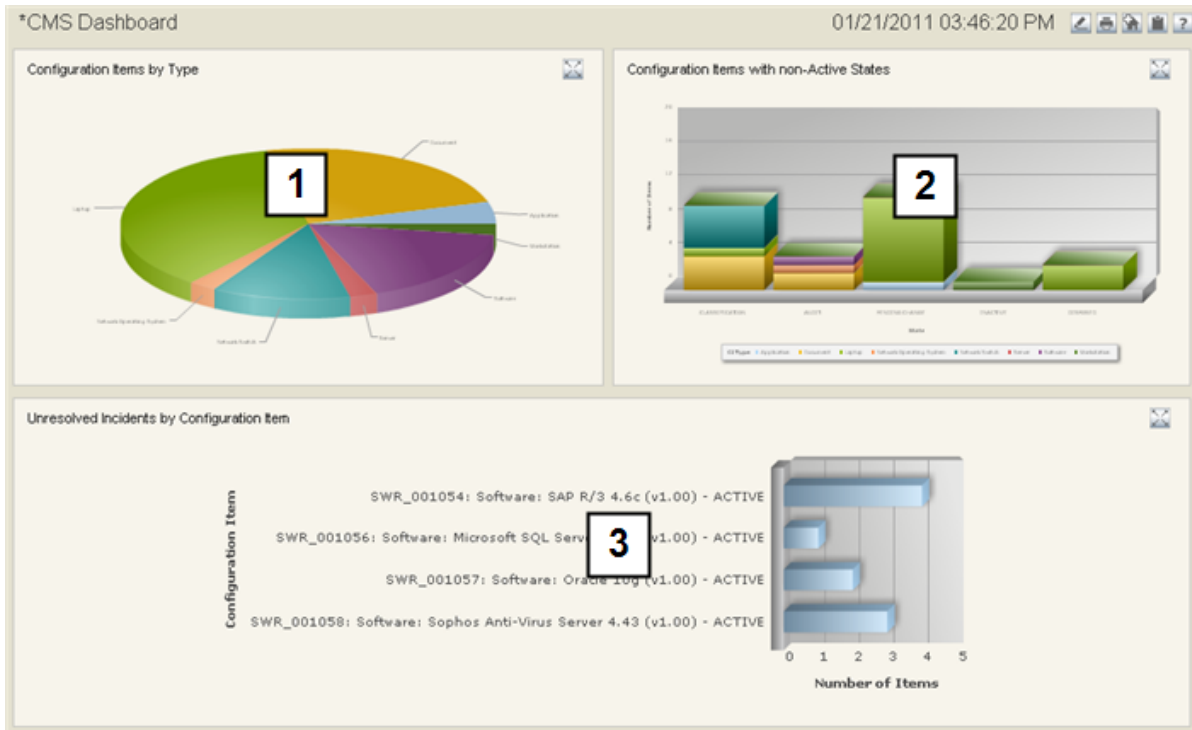
CMS Dashboard

The CMS dashboard gives an overview of your existing assets, incidents associated with those assets, and ongoing requests for change.

The **CMS Dashboard** report is available in the reports that are shipped with the Knowledge Management snapshot.



Tip: Set the CMS Dashboard report as the home page report for the CMS application by opening the **CMS** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.



1. **CI by Type** gives an overview of the distribution of assets that you have across your company.
2. **Configuration Items with Non-Active States** shows a breakdown of where CIs reside when they are not active.
3. **Unresolved Incidents by Configuration Item** shows the open active incidents broken down by CI asset. This gives you a high-level perspective of how many incidents are being raised against each CI item, enabling you to see problem areas which should be investigated or changed.

CMS Roles

The following roles (or actors) are available in the Configuration Management System process app. For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.

Configuration Manager - The Configuration Manager is responsible for the Configuration Management System and the CI Relationships. Other duties include:

- Ensure efficiency and effectiveness of the Configuration Management process
- Define Configuration management policy including scope
- Promote continuous service improvement for Configuration Management
- Produce KPI reports for management review
- Schedule regular Configuration Item verification and audits

-
- Maintain the Configuration Management system
 - Monitor the quality of the CI records and their usefulness to the other Service Manager processes, especially identity management, problem management, change management, and release management
 - Monitor the quality of CI information including CI-to-CI relationships
 - Develop methods and procedures for populating the CMDB

Configuration Analyst - This role is for configuration staff who are responsible for monitoring the CI records. The responsibilities of this role include:

- Coordinate Configuration management activities including CI identification, control, audit, and verification
- Collaborate with Change management on updating CI records
- Produce KPI reports

Configuration User - This role is for the end users who will be submitting new CIs or searching for CIs to relate to incidents, problems, or requests.

Demo Data Viewer and **Demo Report Viewer** - These roles are for users who are demoing Serena Service Manager. These roles have view-only privileges to either the CMS data or the CMS reports.

Chapter 9: Knowledge Management

Serena Service Manager has a new and improved Knowledge Center, for managing knowledge base articles and announcements. The Knowledge Management application allows you to manage the submission of new articles and to monitor changes to existing articles.

The Knowledge Management application has two main types of users:

- *Contributors* are responsible for submitting articles and adding content. They edit the content of the articles, adding formatting to text, such as italics and bulleted lists, using the embedded HTML widget. The contributors are able to save the articles as drafts, which stores the data in the database until the article is ready to be sent to the publisher for final approval.
- *Publishers* review articles before they are made available to end users. The publisher can send the article to additional team members for approval. When the article is ready, the publisher is responsible for posting or publishing the articles to Knowledge Center.

Once it is published, the Knowledge Management item is closed and the content is copied to the Knowledge Center where the material becomes available to end users. **Urgent** announcements are displayed to the user in the banner bar of Request Center.

The article now resides in Knowledge Center. Users can comment and rate the article, and these comments and ratings are stored in Knowledge Center.

The content of the published articles cannot be edited directly in Knowledge Center. Instead, a new item is submitted into Knowledge Management using the **Update this item** link on the published article. The new item must proceed through the same Knowledge Management workflow. When the change is published, the updated content replaces the existing content in Knowledge Center, while the comments and ratings will remain unchanged.

The following topics describe the features found in Knowledge Management:

- [Knowledge Management Roles \[page 86\]](#)
- [Working with Articles from the User Workspace \[page 86\]](#)
- [Working with Articles from Request Center \[page 92\]](#)
- [Knowledge Management Workflow \[page 94\]](#)
- [Knowledge Management Dashboard \[page 95\]](#)

Key Benefits

- HTML Editor for easy formatting of article content.
- Four distinct types of articles to distinguish types of information within Knowledge Center.

- Distinct user roles for publishers and contributors to ensure quality of Knowledge Center content.
- Tracking of approvals to ensure knowledge base article quality.

Knowledge Management Roles



Tip: After adding users to the roles described below, set default values for the Publisher and Contributor fields at the project level. The default values prevent possible permission errors which can result when Knowledge Management articles are submitted from other process apps.

The following roles are available in the Knowledge Management process app. For on-premise installations, use the SBM System Administrator to assign users or groups to roles. For on-demand environments, use the Web Administrator to assign users to roles.



Note: Members in all of these roles are available for selection when an item is sent for approval.

Editor/Publisher - The Publisher is responsible for editing, approving, and publishing Knowledge Center articles.

- Submit new articles to add to Knowledge Center
- Start the update process by submitting items for existing Knowledge Center articles
- Approve articles before they are published, ensuring that Knowledge Center articles meet the accepted standards

Contributors - The Article Writer is responsible for adding content to Knowledge Center articles. Other duties include:

- Add content to articles that are in the **Edit** state.
- Edit existing knowledge base articles that have been re-opened
- Review and approve content of an article written by another contributor

Announcement Contributors - The Announcement Contributor has the same privileges as the Contributor. In addition, the Announcement Contributor has the ability to publish announcements without requiring Publisher approval.

KM Administrator - This role is responsible for administering Knowledge Management, such as assigning users to roles, fixing SBM issues, or restoring deleted items.

Working with Articles from the User Workspace

The following topics explain the Knowledge Management activities performed in the User Workspace:

- [Creating Announcements and Articles \[page 87\]](#)
- [Reviewing Articles \[page 91\]](#)
- [Publishing Knowledge Center Articles \[page 92\]](#)

Creating Announcements and Articles

Knowledge Center articles and announcements can either be created directly by submitting a new item into Knowledge Management or by spawning an article from an incident, request, problem, or RFC. Both of these actions occur from within the User Workspace.

Articles are submitted into the Knowledge Management workflow. The articles are originally assigned to contributors, who add content to the article. Contributors may save the articles as drafts, allowing them to work on the items at a later time.

Contributors can make two types of modifications to the articles: changes to the metadata and changes to the content. The metadata includes expiration dates, summary, and keywords, and this data appears on the **Overview** tab of an article. The **Content** tab is where you modify the actual contents of the article.

Overview Tab

The following sections describe settings that you can make on the **Overview** tab.

Article Types

Knowledge Management articles are divided into four types, with some of the types being associated with a particular items. The four types with their respective items in parentheses are:

- **Announcement** (Changes)
- **FAQ**
- **How To**
- **Tech Note** (Incidents, Requests, Tech Notes)

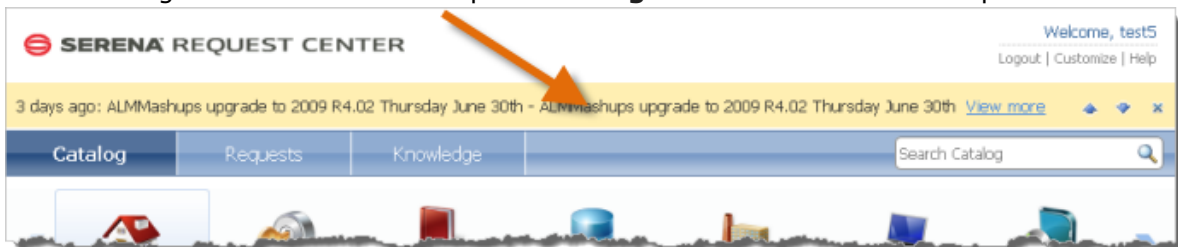
Announcements that are marked as **Urgent** appear both in Knowledge Center and in the announcement bar below the banner of Request Center.

Urgent Announcements

Check the **Urgent** option to mark an announcement as urgent, meaning that the announcement will be displayed prominently below the banner of the Request Center. Urgent announcements will still appear in search results on the Knowledge tab.

Users can navigate through the urgent announcements in the announcement bar by using the up and down arrows.

The following arrow shows an example of an **Urgent** announcement in Request Center.



Note: The IT administrator may disable the announcement bar in the Request Center.

Categories

Knowledge Center users can filter articles based on categories, allowing them an easier way to find knowledge base articles. A Knowledge Management article can be assigned to a particular category when it is created or modified.

To add, modify, or delete categories, access the **KM Categories** auxiliary table by selecting **Search | Manage Data | KM Categories** in the User Workspace.

You can choose an image to represent each category by clicking **Change image**. For information on the image picker, see [About the Image Picker \[page 27\]](#).



Restriction: Modifying items in the **KM Categories** auxiliary table requires the appropriate permissions.

Article Duration

Define how long the article will be available to end users in Knowledge Center by selecting the **Article Duration**. **Does not expire** means that you select when the article becomes active in Knowledge Center and the article will not be removed automatically at a specific date. **Expires** allows you define both the **Start Date** and **Expiration Date** for when the article will be available in Knowledge Center.

For example, you may be performing maintenance on your e-mail server this weekend, and you want to inform your users that the services will be off-line from noon to midnight on Saturday. You would set expiration date and time at the end of the Saturday. The announcement will no longer appear in Knowledge Center after the expiration date.

Users who have the privilege to **Submit** articles can view expired articles by selecting **Include Expired** articles in Request Center.

Keywords

When a user performs a Knowledge search in Request Center, the search is performed against the keywords defined for each article. The **Keywords** are automatically generated when an article's content is updated. The keywords for the article are displayed in the read-only **Keywords** field.

The keywords are also used for the item match search that is performed when a user submits an item.



Tip: The **Summary** field is not included when generating the keywords. Remember to include searchable terms from the **Summary** in the **Content**.

See the following section for information on how the keywords are generated.

About Keyword Generator

The keywords are generated using a script called wordStats. It generates the 35 top keywords for the document. The top keywords are found by stripping out the stop words (see following list) and then applying a weight to the words based on their frequency and on the style in which the words reside.

See the following sections for information on the weight for each style and the list of stop words.

For more information on wordStats, see: <http://hovinne.com/articles/jquery-wordstats-plugin>

Weighting

When a word is found in a particular style, it is assigned the following weight. If the word is found multiple times, the weights of the various instances are summed.

Style	Weight
Title	20
Heading 1	15
Heading 2	10
Heading 3, Heading 4, Heading 5, Heading 6	5
B, I	3
Paragraph, Lists, Links	2
Image Title	1

Stop Words

The keyword generator skips all one letter words. In addition, the following words are ignored:

about, after, ago, all, also, an, and, any, are, as, at, be, been, before, both, but, by, can, did, do, does, done, edit, even, every, for, from, had, has, have, he, here, him, his, however, if, in, into, is, it, its, less, many, may, more, most, much, my, no, not, often, quote, of, on, one, only, or, other, our, out, re, says, she, should, so, some, soon, such, than, that, the, their, them, then, there, these, they, this, those, though, through, to, under, use, using, ve, was, we, were, what, where, when, whether, which, while, who, whom, with, within, you, your



Note: An apostrophe is considered a word break, which means that abbreviations are treated as two words. For example, *you've* is considered to be *you* and *ve*.

Content Tab

The content of the article is shown on the **Content** tab. The text is divided up based on sections.



Note:

When submitting a new article, the **Content** tab includes the ability to select an Article Type and to choose to **Load Article Template** associated with that article type. The article template includes sample data and headings to assist in completing the different sections according to company standards.

After an article is submitted, the ability to load an article template is no longer available and the **Article Type** drop-down moves to the **Overview** tab.

For more information on the article types, see [Article Types \[page 87\]](#).

Add content to the different sections by placing your cursor in the section and adding the text. When editing text in non-title fields, the HTML editor appears, which allows you to

apply formatting to the text and insert links or images. The following topic describes how to use the HTML editor.



Note: You cannot add images to the article on the submit form. You must complete the submit form by selecting **Save as Draft** and clicking **OK**. This completes the submit process and creates the item. Then, you select **Edit** and add the image to the content.

Using the HTML Editor


The HTML Editor allows you to format the text that appears within your articles and announcements. The editor allows you to apply heading formats, add bulleted lists, format text, and insert images or links.

The HTML Editor appears on the **Content** tab of the Submit and Edit transition forms in Knowledge Management.

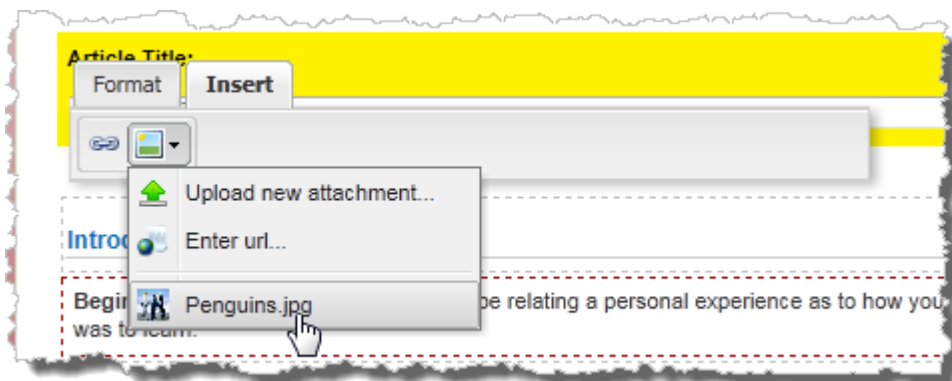
To use the HTML editor:

1. Select the text to modify or place your cursor in the section to add the text. The HTML Editor displays the following menu:




2. Format a section by selecting it and then selecting the formatting, such as **Bold** or **Heading 1**.
3. Insert an image by selecting the **Insert** tab and clicking . Select whether to reference a URL for the image or to upload the image as an attachment.


Uploading the image as an attachment is a two-part process. First, you select the insert image button to upload the image. This launches the Attachment dialog, where you can browse to the image to upload. After the upload completes successfully, then select the insert button again, and choose the image in the drop-down menu.



The image will now appear inline. In summary, the image file will be stored as an attachment in the item, and it appears inline in the content.

-
4. Make text a hyperlink by selecting text and clicking . The **Link** tab opens. Enter the URL for the hyperlink. The hyperlink will become active after the page is saved.

Note that if text is not selected, the text **New Link** will be added. This text can be modified to change the name of the link.

You can modify an existing link by clicking on the link in Edit mode. This will open the **Link** dialog to edit the hyperlink. Click  to remove the link.

Displaying Labels

On the **Content** tab, labels appear on the right side which help to define what type of content each section should contain.

You can show or hide the labels by clicking **Show Labels** or **Hide Labels** link on the top of the tab

Reviewing Articles

Reviewing articles before they are published for public viewing in the Knowledge Center ensures that your articles meet the standards set by your company.

The main actors for reviewing articles are the editor/publisher and reviewer. The editor/publisher is responsible for sending the article for review, adding suggested edits to the article, and publishing the article. The reviewers who are responsible for reviewing the article and suggesting edits.

The complete steps for review process in Knowledge Management are as follows:

1. Contributor finishes an article and sends the article to the editor/publisher using the **Send to Publisher** transition. The article moves to the **Content Preparation** state.
2. The publisher chooses to send the article for review by selecting the **Send for Review** transition.
3. On the transition form, the publisher chooses the reviewers by moving them into the **Reviewers** list.
4. After adding the **Work Notes** to the article, the publisher completes the transition by clicking **OK**.
5. The article moves to the **Content Review** state, where the selected reviewers become the owners.
6. The reviewer can **Approve** the article or **Suggest Edits**. The suggested edits are noted in the **Suggested Edit** field.
7. When a reviewer suggests edits to the article, the article moves to the **Edits Suggested** state after the reviews are completed.
8. The publisher can choose to **Edit** the item and add the suggested edits.
9. After the edits have been incorporated, the publisher chooses to either publish the article or send the article for another round of review.

In addition to the usual review path, publishers can choose from the following options:

- **Return** the article to the contributor, which moves the article back the **Draft** state. The contributor can add to the article and then send it back to the publisher.
- **Reject** the article, which moves the article to the **Rejected** state. The contributor to the article can choose to **Re-Submit** it.
- **Cancel review** of the article, which returns the article to the publisher. If suggested edits have been added, the article moves to the **Suggest Edit** state. If not, the article returns to the **Content Preparation** state.
- **Delete** the article, removing it from the system.

Publishing Knowledge Center Articles

Publishing an article moves the article into Knowledge Center, where it become active, available for searching, rating, and commenting by users. Publishing articles copies the content from the article in the Knowledge Management application into the Knowledge Center.

Publishing occurs with the **Publish** transition. The Publish transition is available from multiple states within the Knowledge Management workflow.



Important:

Do not use Mass Update or the Editable Grid to perform the **Publish** transition.

The article will not be published to Knowledge Center, and the item will move to the **Published** state in Knowledge Management preventing you from publishing the article again. You will have to recreate the article.

After the article is published, modifications require that a new item is submitted into Knowledge Management by clicking **Update this item**.

Working with Articles from Request Center

The following topics explain the Knowledge Management activities performed in Request Center:

- [Viewing and Commenting on Articles \[page 92\]](#)
- [Updating Knowledge Center Articles \[page 93\]](#)
- [Deleting Knowledge Center Articles \[page 94\]](#)

Viewing and Commenting on Articles

Knowledge Center articles can be viewed from the Knowledge tab in Request Center, the Knowledge Management dashboard report, and from Incident submission forms.

The detailed article view allows users to read the content of the article, comment on the article, and give the article a rating. The average rating of the article and the number of views the article has received is tracked for users to sort on highest rated and most popular articles.

The following sections include information on tasks to perform from the detailed view.


Adding Comments or Ratings

Each user is allowed one comment or rating, and can change the comment or rating at any time.

To add or update comments, the user must display the article, and then click **Add your own comment**.

Sending a Link to the Article

Send the article to another person by copying the URL and pasting it in an e-mail or IM.

To copy the URL to your clipboard, click . You can then paste (CTRL+V) the URL into an email or IM. This URL allows users direct access to the article.

Updating Knowledge Center Articles

You may need to modify the published articles in Knowledge Center to add information or to fix errors.

Modifying a published article requires that a new item is submitted into Knowledge Management in order to track the changes. The new item contains a copy of all the information contained in the published article. The published article remains in Knowledge Center.

This duplicate item proceeds through the same Knowledge Management workflow, requiring the approvals, if needed. When the item is published, the new content replaces the content of the existing article in Knowledge Center. The comments that were made against the original article remain in Knowledge Center.



Restriction: To modify an existing article, you must have publish permissions.



Important: Administrators must set a default value for the Contributor and Publisher fields at the project level to avoid errors when submitting or transitioning articles in Knowledge Management. One option is to set the default value of the Contributor field to the **Current User**, which will assign the item immediately to the submitter for editing.

To modify an existing article:

1. Select the Knowledge tab in Request Center.
2. Find the article to edit by performing a search.



Note: Access expired articles by selecting **Include Expired**.

3. Open the article then click **Update This Article**. A new item is submitted into Knowledge Management with the **Content** is populated with the data from the original.
4. Edit the article using the Edit transition and the HTML editor.
5. After finishing the modifications, publish the article to replace the existing content in Knowledge Center.

Deleting Knowledge Center Articles

You may need to delete or remove articles that are in the Knowledge Center.

To remove items, you will perform an update of the item from Knowledge Center as described in [Updating Knowledge Center Articles \[page 93\]](#), and then you set the expiration date in the past. Remember that the start date must be prior to the end date or the article will be considered a non-expiring article.

This will remove the article from the Knowledge Center, while keeping an audit trail of the item, informing others about who was the one responsible for removing the article.

Other publishers will be able to view the deleted article and its contents by selecting to view expired articles in Knowledge Center.

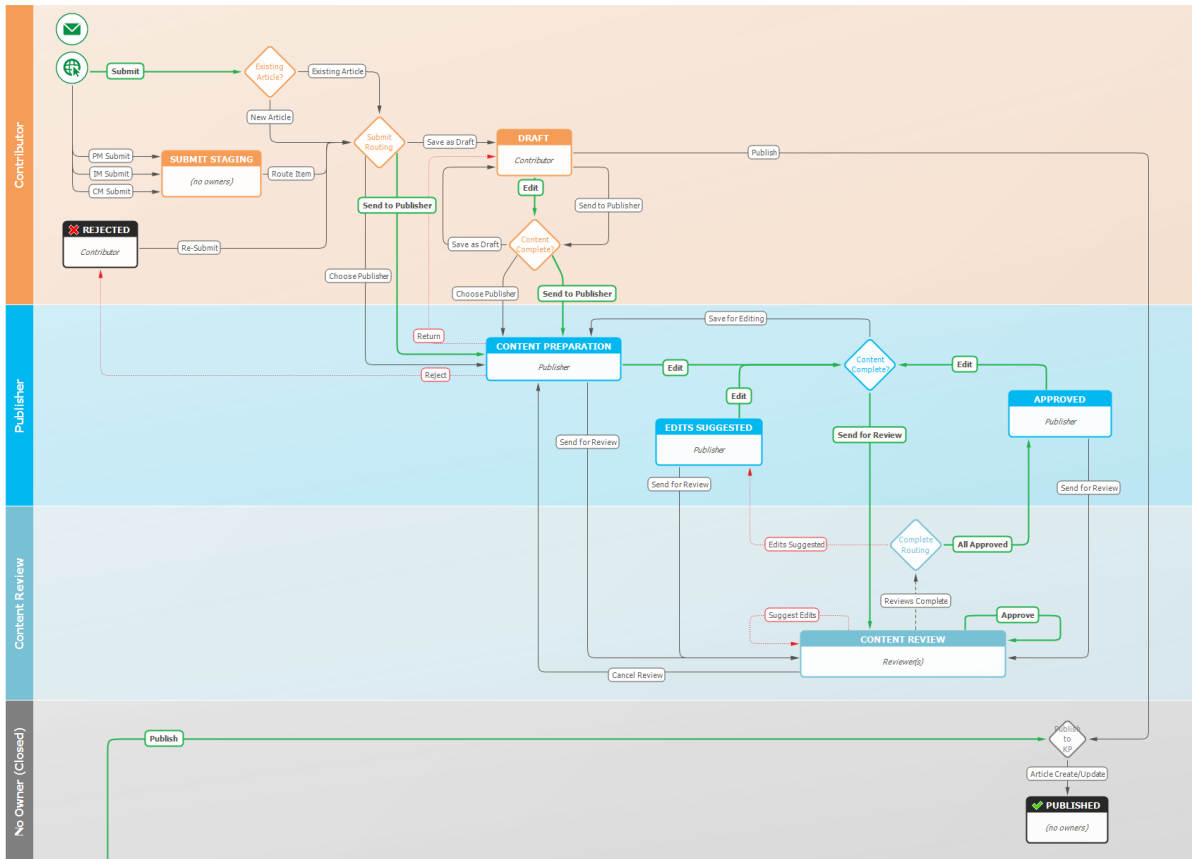
Knowledge Management Workflow

The Knowledge Management workflow in Serena Service Manager appears as follows. The states are represented by rectangles, such as *Deferred* and *CAB Review*, and the transitions are marked with arrows, such as *Reject* and *Accept*. The process starts with one of the different submit paths, and then it can proceed along the different transition arrows.

You can access this diagram through SBM Composer or SBM User Workspace. Use SBM Composer to modify the workflow.



Note: When an article is submitted from another application, the option to **Send to Publisher** is disabled. The user must save as a draft before sending the article to be published. This eliminates problems that may occur if default values have not been set for the publisher or if the submitter does not have appropriate permissions.




Knowledge Management Dashboard

The Knowledge Management dashboard gives an overview of the existing knowledge base articles, trend lines of published articles, and articles currently in the process of being published.

The **Knowledge Management Dashboard** report is available in the reports that are shipped with the Knowledge Management snapshot.



Tip: Set the Knowledge Management Dashboard report as the home page report for the Knowledge Management application by opening the **Knowledge Management** application in the User Workspace, clicking the **Application Settings** icon (), and choosing the report under **Home Page Report**.

*Knowledge Management Dashboard 06/25/2011 07:29:12 PM

Published Articles

All Types in All Categories Group by none

Recent articles Include Expired

Announcement fasdfs | 1 comments | 12 views | updated 5 days ago

How To Article Title - Keyword test | 1 comments | 27 views | updated last week

Published Article Trend by Type

Articles in Progress

Now showing Knowledge Management 1 - 17 of 17 Sorted by: Project (Hierarchy)

RM Request Id	Article Type	Article Title	Contributor	Publisher	State	Submit Date
HOW_002555	How To	How To Article Title	Administrator	Administrator	CONTENT PREPARATION	05/31/2011 01:59:32 PM
FAQ_002567	FAQ	asdfs	Administrator	Administrator	CONTENT REVIEW	06/01/2011 04:57:50 PM
HOW_002568	How To	How To Article Title	Ryan Cook	Administrator	CONTENT PREPARATION	06/01/2011 05:41:58 PM
FAQ_002768	FAQ	ZXCZ	Administrator	Administrator	CONTENT REVIEW	06/08/2011 03:57:52 PM
HOW_002978	How To	How To Article Title	Ryan Cook	Administrator	CONTENT PREPARATION	06/10/2011 03:53:58 PM
HOW_002985	How To	How To Article	Ryan Cook	Administrator	CONTENT PREPARATION	06/10/2011 04:55:55 PM
HOW_003002	How To	How To Article Title	Ryan Cook	Administrator	CONTENT PREPARATION	06/13/2011 12:07:04 PM
HOW_003004	How To	Test Article - Z1 	Ryan Cook	Administrator	CONTENT PREPARATION	06/13/2011 12:22:40 PM

1. The **Published Articles** widget displays the recently published articles in the same format that appears in Request Center. Choose from different display options such as filtering to display articles in one category.
2. **Published Article Trend by Type** shows the trend of how many articles are being published each week, based on the article types.
3. **Articles in Progress** shows the open active articles that have not been published and that are not in the draft state. Once articles are published, they are marked as inactive.

Chapter 10: Additional Information

This chapter has some additional information to understanding Serena Service Manager.

- [Adding Auxiliary Data \[page 97\]](#)
- [Modifying Process Apps \[page 98\]](#)
- [Managing Users \[page 98\]](#)
- [Enabling Notifications \[page 99\]](#)
- [Integrations Between Applications \[page 100\]](#)
- [Additional ITIL References \[page 101\]](#)

Adding Auxiliary Data

The Serena Service Manager makes use of data that is stored in auxiliary tables. These tables must be populated with some information in order to use the solution; however, the tables are meant to be added to as you add more information into your systems.

The auxiliary tables included with this solution include:



CAUTION: The bold tables in the list are populated by the solution. Use extreme caution when manually altering these tables.

- Categories (Knowledge Management)
- CI Categories (CMS, referenced by Incidents, Changes, and Problems)
- CI Sub-Categories (CMS, referenced by Incidents, Changes, and Problems)
- CI Sub-Category Types (CMS, referenced by Incidents, Changes, and Problems)
- Knowledge Base (Knowledge Management)
- **KP Published (Knowledge Center)**
- **KP UserRatings(Knowledge Center)**
- Model Numbers (CMS)
- **Relationships (CMS)**
- Relationship Types (CMS)
- Resolution Codes (Incident)
- Software Platforms (CMS)
- Symptom Codes (Incident)

- Vendors (CMS)
- **Workarounds (Problems)**

The non-bold tables have default values but can also be tailored for your needs. The values determine which selections are available when working with incidents, problems, changes, and CIs. The following topic explains how to add information to these tables.

Managing Auxiliary Data

To add or edit data records to your auxiliary tables, choose one of the following:

- In the User Workspace, select **Search | Manage Data**, choose the table from the drop-down list, and then click **Create Item** or search for an existing item to edit.
- Create an Editable Grid listing report based on the auxiliary table, and then either create or edit items in the table.

For details, refer to the *SBM User Workspace Online Help*.

Modifying Process Apps

SBM Composer is used to modify process apps, applications, and orchestrations. This includes designing states, transitions, forms, actions, and other elements. You also use SBM Composer to create new roles and tie the roles to particular states or transitions.

To modify the process apps using SBM Composer:

1. Open the process app in SBM Composer by clicking **Composer Button | Open | Application Repository** and selecting the process app.
2. Repeat for all Service Manager process apps. This allows reference information to be loaded into SBM Composer local cache.



Important: Open all process apps in SBM Composer before attempting to edit. The apps reference each other, and if one is not imported into SBM Composer, you may get validation errors.

3. Open the process app to modify.
4. Modify the process app.
5. Deploy the changes to your server.

For more information on using SBM Composer, refer to *SBM Composer Guide*.

Managing Users

To simplify the management of your users, roles have been created for the different applications. Administrators assign users to the appropriate roles, which gives the users the appropriate permissions and access to the applications.



Note: User and Multi-User field types refer to the roles for populating the lists. For example, the **Additional Contacts** field refers to all of the roles contained in the Incident Management application.

Managing users is a twofold process:

-
1. Create a user account in SBM.
 2. Add the user account directly to a role or add the user to a group that is granted the role.



Note: The client which you use to add user accounts depends on your SBM installation. If you are using an on-premise version of SBM, add the users using the Web Administrator or the SBM System Administrator. For on-demand customers, use the Web Administrator.

See the topics associated with each application for more information on the roles available in the application:

- [Incident Management Roles \[page 40\]](#)
- [Request Fulfilment Roles \[page 47\]](#)
- [Change Management Roles \[page 70\]](#)
- [Problem Management Roles \[page 57\]](#)
- [CMS Roles \[page 82\]](#)
- [Knowledge Management Roles \[page 86\]](#)

Enabling Notifications

Notifications keep users and staff aware of changes to items. These notifications are contained in the application snapshots that were promoted during installation.

After the snapshots have been promoted, the administrator must grant **allow subscription** privileges to the users who will subscribe to the notifications. Once a user has been allowed subscription to a notification, the administrator can subscribe the user to a notification. For on-premise installations, the administrator grants these privileges using the SBM System Administrator. For on-demand systems, the administrator must contact Serena IT to grant these privileges to a particular group and then assign users to that group using Web Administrator.

Users manage subscriptions on the **Notifications** tab of their User Profile. The users can subscribe or unsubscribe to notifications.

Service Manager contains specialized notifications and notification templates in addition to the default notifications usually available with SBM applications. The following notifications are the default ones available for a deployed process app.

- Any [item] changes owner
- Any [item] changes state
- Any [item] changes to inactive
- Any [item] I submitted changed state
- Any [item] I submitted changed to inactive
- Any [item] is submitted
- I become the owner of any [item]

The following table explains the additional or modified notifications available with each process app:

Application	Notification Name	Change to Rule
Incident Management	IM - Any Incident is Submitted	Notifies Reported By and Affected By user when incident is submitted.
Incident Management	IM - Automatic Escalation to L2	Notifies when change moved to Investigation & Diagnosis state.
Incident Management	IM - Resolved	Notifies Reported By , Affected By , and Additional Contacts users when incident is moved to Resolved state.
Incident Management	IM - Resolved Repeat Cancel	Notifies user when incident moves from Resolved state.
Incident Management	IM - Resolved with Workaround	Notifies Reported By , Affected By , and Additional Contacts users when incident is moved to Resolved by Workaround state.
Change Management	CM - Change Submitted	Notifies the submitter when a change has been submitted.
Change Management	CM - Change Closed	Notifies the submitter and the user selected as the contact when the change is closed.

Service Manager also contains specialized templates. For on-premise customers, these templates are prefixed by ITSM and are installed into the notification templates directory:

```
SBMinstallationDirectory\Serena\SBM\Application
Engine\emailtemplate\notificationtemplates
```

Integrations Between Applications

The following sections explain the different links between items.

Related CIs

Once a CI is related to an item in another process, the information from that CI can be found within the other management process. For example, once an item is assigned to a CI, any CIs related to that CI appear on the Relationships tab for the item. This allows other management teams to gather necessary CI status information, and to create reports to determine if any particular CI is related to multiple problems.

CI status is also used for workarounds, which are related to a particular CI. This allows users to find possible solutions to a problem based on the item which is causing the problems. They can also search for solutions based on the CIs that are related to the item giving them problems.

Relational Fields

All of the process apps have relational fields that point to other applications. For example, the Problem Management application has relational fields that point to the CMS and CI items. This allows you to relate Configuration Items with problems and select from the same CI Categories.

Post-Transitions

Many of the process applications use post-transitions to submit items into other applications.

For example, the Problem Management application contains the **Post RFC** transition, which creates a request in the Change Management application.

Storing File Attachments

Attachments to items may be stored in SBM or in Microsoft Office SharePoint, depending on what options you have enabled with SBM. Serena offers SBM Connect for SharePoint[®], a connector to SBM which allows you leverage the file management capabilities of SharePoint with SBM. For more information about SBM Connect for SharePoint[®], refer to *Integration Guide for SharePoint* or contact Serena support.

Additional ITIL References

The following sites contain additional information about ITIL standards.

- **OGC Official ITIL[®] Website:** <http://www.itil-officialsite.com>
- **Wikipedia Article on IT Service Management:** http://en.wikipedia.org/wiki/IT_Service_Management
- **itSMF International - The IT Service Management Forum:** <http://www.itsmfi.org/>