SERENA®

SERVICE MANAGER

On-Demand Installation and Configuration Guide

Serena Proprietary and Confidential Information

Trademarks

U.S. Government Rights

Table of Contents

Chapter 1: Welcome to Serena Service Manager

This chapter gives an overview of the pieces included with Serena Service Manager and Serena Request Center.

> **Note:** If you purchased Serena Request Center, you will receive a subset of the pieces that are included with Serena Service Manager. Serena Request Center includes Service Desk Process App, Starter Pack Forms, Knowledge Management, and SRC. The ITSM process apps such as Problem Management, Change Management, and Configuration Management System are only included if you purchased Serena Service Manager.

Serena Service Manager

Serena Service Manager is a process-driven approach to ITSM – one that allows business and IT to work together, in perfect harmony. Unlike traditional ITSM solutions that are difficult to use, expensive to maintain, and provide limited visibility across the service delivery lifecycle, Serena Service Manager draws on the power of a process management platform at its core to provide you with the following benefits:

- Lowers TCO

- Complete visibility

- Improved user satisfaction and agent productivity

- A contemporary interface for IT services

Serena Service Manager comes packaged with fully functional, easy-to-use applications including those for Request, Incident, Problem, Change and Configuration Management.

Service Manager also provides the IT operations team with visual dashboards and robust report generation capabilities so that they can maintain complete visibility across the end-to-end service delivery process. This includes the ability to view actionable metrics related to costs and resource utilization.

Serena Request Center

Serena Request Center provides a one-stop interface for corporate users to discover and request IT services, submit incidents, and review knowledge base articles. It comes with a rich, interactive, and intuitive web portal. The portal contains an enterprise service catalog allowing for services to be composed, organized and published into convenient categories for anytime, anywhere access.

The portal comes pre-populated with IT Services use the request fulfillment workflows in the Service Desk Process App, such as New Hire and Install OS. The services also make use of the Starter Pack Forms, which are customized external forms for submitting requests.

Purpose of This Guide

This guide explains how to perform administrative duties in Serena Service Manager 3.0.

This guide is meant for Service Manager administrators who are responsible for deploying the Service Manager solutions.

This guide does not give details on the specifics about the service management workflows and their features. For details on Service Manager and its workflows, refer to the *Serena Service Manager User's Guide*.

This guide also does not contain detailed information on modifying projects, users, workflows, or orchestrations. For details on configuring and modifying the solution after you have promoted it, refer to the following guides that are included with your Serena Business Manager installation:

- *SBM Composer Guide* for modifying workflows and process apps.

- *SBM Application Repository Guide* for deploying and promoting snapshots and process apps.

Chapter 2: Installing On-Demand

This chapter describes how to successfully install and set up Serena Service Manager in an on-demand SBM system.

To install Service Manager on-demand, perform the following steps:

1. Import the solution files as described in Importing the Solutions [page 7].

2. Promote the solution process apps as described in Promoting the Snapshots [page 8].

3. Deploy the process apps as described in Deploying the Process Apps [page 14].

4. Add auxiliary data, add users to appropriate roles, and define SLAs as described in Chapter 3: Setting up Serena Service Manager [page 17].

Importing the Solutions

This topic describes how you import the Serena Service Manager solution files into your environment.

Importing a solution adds all of the snapshots and process apps for the solution to your SBM Server. The process apps and snapshots are available for promotion after the import.

To import a solution:

1. Log in to SBM Application Repository.

2. Select the **Solutions** tab.

3. Click the **Import** button to begin importing the solution.

Upon successful completion of the import, the imported solution appears in the **Imported solutions** list.

On the **Process App Snapshots** tab, the snaphots contained in the imported solution will now be available for promotion.

On **Process Apps** tab, the new process apps are displayed and now available for import into SBM Composer.

> **Important:** Choose to promote the snapshots before deploying them. Promoting maintains data that is necessary for some operations such as maintaining internal IDs and priming Request Center with sample data. Deploying first may cause synchronization problems later.

Troubleshooting Import

If the import of a solution file fails with an error, you can view the error in the **Application Repository Log** from within SBM Application Repository.

During the import, if there are already existing applications in the destination environment, then Application Repository attempts to upgrade the existing application

with the data in the new application if the internal IDs (UUIDs) are identical. If the internal IDs are different but the Application Names are identical, then the import fails.

Note: Contact Serena support for information on finding an application's UUID.

If the import fails due to identical application names, the workaround is to delete the process app in the repository and then reimport the solution.

Promoting the Snapshots

Note: Promotion is performed after you have completed importing the solutions as described in Importing the Solutions [page 7].

After importing the solution, you must promote the associated snapshots into your environment. Promoting the snapshots places the contents of the solution, including all reports, notifications, process apps, and auxiliary table data, onto your SBM Server.

Important: Choose to promote the snapshots before deploying them. Promoting maintains data that is necessary for some operations such as maintaining internal IDs and priming Request Center with sample data. Deploying first may cause compatibility problems later on.

If you have an installed a previous version of Service Manager, the promotion will overlay the previous version. Note that the update only occurs when the process apps contain the same internal SBM ID. If you initially deployed a process app instead of promoting the snapshot, the process app may have been assigned a different ID. You will no longer be able to update the existing process app.

The **Activities** tab of Application Repository contains a log of the promotions. When viewing the logs, you may notice many warning messages, such as the following from the promotion log for SSM - Change Management:

```
WARN -- Unable to create field 'Linked CIs' in table
'Changes' because relational table 'Configuration Items' is not defined.
```

These warning messages are usually due to the related application having not yet been promoted to the target environment. In the previous example, SSM - Configuration Management System has not yet been deployed, which means that the relational field **Linked CIs** in SSM - Change Management cannot be defined successfully. This warning will be fixed once the referenced snapshot has been deployed.

Tip: If you do not plan to use a particular process app, it is recommend that you still promote it; however, you do not make it available to the end users. Each process app references other process apps, and this approach eliminates the reference errors that appear in SBM Composer when you attempt to modify the process apps.

Promoting the Serena Service Manager Snapshots

To promote the Serena Service Manager snapshots:

1. Log in to SBM Application Repository.

2. Select **Process App Snapshots** tab.

3. Click **All** and then select to filter on Serena Service Manager 3.0.

4. Promote the Serena Service Manager snapshots by performing the following steps:

   a. Select the snapshot and click the **Promote** button. The **Summary** screen of the **Promote Dialog Box** is displayed.

   b. Choose the **Destination Environment** by selecting the **Destination** box.

   c. On the **Entities** screen, you choose which entities to import. It is recommended to import all of them, but it is not mandatory. The following tables explain which options must be selected for each snapshot and which options are optional.

   Table 1. Promotion Options

Type	Notes
Projects	Mandatory.
Notifications	Optional, but suggested. Not importing notifications means that no notifications will be available until you create them.
Notification Rules	Optional, but suggested. Not importing notification rules means that notifications will not be sent within the workflow until you add new notification rules.
Reports	Mandatory.
Auxiliary Table Data	Depends on the process app. See the following table for more information.
Transition Group Restrictions	Mandatory.
User Field Selections	Mandatory.

   Table 2. Auxiliary Table Data

Process App	Notes on Importing Auxiliary Table Data
SSM - Change Management	No auxiliary tables or data.

Process App	Notes on Importing Auxiliary Table Data
SSM - Configuration Management System	• **CI Categories, CI Sub-Categories, CI Sub-Category Types**: Recommended, but not required. If you do not import the table data, you must populate the tables with data before using Service Manager. • **Model Numbers, Relationships, Software Platforms**: Not required. Note that these tables do not contain data and selecting them to import will have no effect. • **Relationship Types**: Strongly Recommended. If not, you must add relationship types before you can create relationships between CIs. • **Vendors**: Mandatory.
SSM - Problem Management	• **Workarounds**: Not required. Note that these tables do not contain data and selecting them to import will have no effect.
SSM - Service Desk	• **Client Software**: Not required. • **Computer Models**: Not required. • **Computer Types**: Not required. • **Departments**: Not required. • **Mobile Carriers**: Not required. • **Mobile Device Platforms**: Not required. • **Mobile Devices**: Not required. • **Operating Systems**: Not required. • **Resolution Codes**: Not required. • **Symptom Codes**: Not required.

> **Note:**
>
> Select the **Merge conflicts** option if you have already promoted the snapshot to the target environment and you want to preserve changes that were made to the existing application.
>
> For example, you have already promoted a previous version of the Incident Management snapshot, which you then modified to added new notifications and user roles. You want to preserve these changes when you promote the new Incident Management snapshot.
>
> The **Merge conflicts** option is only relevant when the items contained in the snapshot already exist in the target environment. Selecting the option will perform an automatic merge of the content in the snapshot with the existing content. The merge will change the existing data if it exists in the snapshot, and it will leave the other data alone.
>
> For example, by selecting **Merge conflicts**, if you have added new user roles, these will remain in the target environment after the promotion. If **Merge conflicts** is not selected, the existing entities will be deleted in the target environment.

   d. If no mappings are needed on the **Mapping** dialog box, click **Done**.

   e. Complete the Promotion dialog by clicking **Promote**.

   f. Repeat for each snapshot.

Promoting the Serena Request Center Snapshots

To promote the Serena Request Center snapshots:

1. Log in to SBM Application Repository. Select to filter on Serena Request Center.

2. Select **Process App Snapshots** tab.

3. Click **All** and then select to filter on Serena Request Center.

4. Promote the Serena Service Manager snapshots by performing the following steps:

   a. Select the snapshot and click the **Promote** button. The **Summary** screen of the **Promote Dialog Box** is displayed.

   b. Choose the **Destination Environment** by selecting the **Destination** box.

   c. On the **Entities** screen, you choose which entities to import. It is recommended to import all of them, but it is not mandatory. The following tables explain which options must be selected for each snapshot and which options are optional.

5. On the **Entities** screen, you choose which entities to import. The following tables explain which options must be selected for the process apps and which are optional.

Table 3. Promotion Options

Type	Notes
Projects	Mandatory.

Type	Notes
Notifications	Optional, but suggested. Not importing notifications means that no notifications will be available until you create them.
Notification Rules	Optional, but suggested. Not importing notification rules means that notifications will not be sent within the workflow until you add new notification rules.
Reports	Mandatory.
Auxiliary Table Data	Depends on the process app. See the following table for more information.
Transition Group Restrictions	Mandatory.
User Field Selections	Mandatory.

Table 4. Auxiliary Table Data

Process App	Notes on Importing Auxiliary Table Data
Starter Pack Forms - IT	No auxiliary data required.
Knowledge Management	• **KM Categories**: Optional, but suggested.
SSM - Service Desk	• **Client Software**: Not required. • **Computer Models**: Not required. • **Computer Types**: Not required. • **Departments**: Not required. • **Mobile Carriers**: Not required. • **Mobile Device Platforms**: Not required. • **Mobile Devices**: Not required. • **Operating Systems**: Not required. • **Resolution Codes**: Not required. • **Symptom Codes**: Not required.

Note:

Select the **Merge conflicts** option if you have already promoted the snapshot to the target environment and you want to preserve changes that were made to the existing application.

For example, you have already promoted a previous version of the Incident Management snapshot, which you then modified to added new notifications and user roles. You want to preserve these changes when you promote the new Incident Management snapshot.

The **Merge conflicts** option is only relevant when the items contained in the snapshot already exist in the target environment. Selecting the option will perform an automatic merge of the content in the snapshot with the existing content. The merge will change the existing data if it exists in the snapshot, and it will leave the other data alone.

For example, by selecting **Merge conflicts**, if you have added new user roles, these will remain in the target environment after the promotion. If **Merge conflicts** is not selected, the existing entities will be deleted in the target environment.

6. If no mappings are needed on the **Mapping** dialog box, click **Done**.

7. Click **Promote** to import the snapshot.

8. Repeat for each snapshot.

Deploying the Process Apps

> **Note:** Deployment is performed after you have completed promoting the process app snapshots as described in Promoting the Snapshots [page 8].

After you promote the process app snapshots from Application Repository, you must open certain process apps in SBM Composer that reference other process apps and deploy them in a specific order because the apps contain references to one another.

For example, after you import the Serena Request Center solution and promote the Service Desk and Starter Pack process apps, you must open SBM Composer and deploy the process apps again in the following order:

1. Starter Pack

2. Service Desk

3. Starter Pack

> **Important:** You must allow SBM Composer to resolve the references between these apps before you deploy them by opening each of them in SBM Composer first. To do this, launch SBM Composer, open Starter Pack from the repository, and then open Service Desk from the repository. Deploy your local Starter Pack copy (no check-in required), then deploy your local Service Desk copy (again, no check-in required), and then open Starter Pack from the repository and deploy it once again.

This deployment order ensures that the proper forms in the Starter Pack process app are available for use in each of the services that come with the Service Desk process app.

Setting Authentication for Orchestrations

As of SBM 10.1, security tokens are issued to all authenticated users whether you use SSO or not, so you are no longer required to provide auth materials for SBM Application Engine calls in orchestrations. However, you might want to hard-code specific auth credentials so that the orchestration runs under a specific user in either of the following scenarios:

- In case the calling user in the User Workspace does not have sufficient privileges.

- In the event you have upgraded from a previous SBM release in which SSO was disabled and you use external events in your orchestrations (as no token is issued for anonymous events).

The following steps explain how to import the process app into SBM Composer, modify the orchestration, and deploy the process app to your SBM Server.

> **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.

To modify the orchestrations:

1. Open the process app in SBM Composer by clicking **Composer Button | Open | Application Repository** and selecting the process app.

2. Configure the orchestrations in the process app to be authenticated under a user account that is authorized to run orchestrations:

   a. Select an orchestration workflow under **Orchestration Workflows**.

   b. Click the **Data Mapping** tab in the **Property Editor**.

   c. Under **Working Data**, add user account to the **userId** and **password** Default Values. These values will be used to authenticate the orchestration.

   d. Repeat for all orchestrations in the process app.

3. Publish and deploy the updated process app to your environment. You are prompted to save your changes, and then the process app is then deployed to your environment. A confirmation message will appear in the **Message List** when the deployment is complete.

4. Repeat these steps for each of the process apps with orchestrations.

Chapter 3: Setting up Serena Service Manager

This section explains how to set up Serena Service Manager after you have promoted the solution files. These tasks must be done before you can use Service Manager.

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.

Important: You must grant a user privileges to the tables below using SBM Application Administrator before you can populate them with auxiliary data in SBM Application Administrator.

CAUTION:

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

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. See Managing Auxiliary Data [page 19] for information on how to add information to these tables.

Serena Request Center Process Apps and Auxiliary Tables

The following auxiliary tables are packaged with the **Serena Starter Pack 3.0** process app:

- **KP Published**

- **KP UserRatings**

The following auxiliary tables are packaged with the **Knowledge Management** process app:

- KM Categories (Knowledge Management)

The following auxiliary tables are packaged with the **Service Desk** process app:

- Client Software

- Computer Models

- Computer Types

- Departments

- Mobile Carriers

- Mobile Device Platforms

- Mobile Devices

- Operating Systems

- Resolution Codes

- Symptom Codes

Serena Service Manager 3.0 Process Apps and Auxiliary Tables

The following auxiliary tables are packaged with the **Change Management** process app:

- None

The following auxiliary tables are packaged with the **Configuration Management System** process app:

- CI Categories

- CI Sub-Categories

- CI Sub-Category Types

- Model Numbers

- Relationship Types

- **Relationships**

- Software Platforms

- Vendors

The following auxiliary tables are packaged with the **Service Desk** process app:

- Client Software

- Computer Models

- Computer Types

- Departments

- Mobile Carriers

- Mobile Device Platforms

- Mobile Devices

- Operating Systems

- Resolution Codes

- Symptom Codes

The following auxiliary tables are packaged with the **Problem Management** process app:

- **Workarounds**

Managing Auxiliary Data

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

- Log in to SBM Application Administrator as a privileged user, select **Auxiliary Data**, choose the table from the drop-down list, and then click **New** or search for an existing item to edit. For details, refer to the *SBM Application Administrator Guide*.

- Log in to SBM User Workspace and 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's 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 used in Incident Management.

Managing users is a twofold process:

1. Create a user account.

2. Using SBM Application Administrator, add the user account directly to a role or add the user to a group that is granted the role.

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

- Incident Management Roles [page 20]

- Request Fulfillment Roles [page 21]

- Change Management Roles [page 22]

- Problem Management Roles [page 23]

Incident Management Roles

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

Note: The Incidents workflow and the request fulfillment workflows are in the Service Desk Process App. The Level 1 Techs role is used by all of these workflows.

Use the SBM Application 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.

Request Fulfillment Roles

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

> **Note:** The Incidents workflow and the request fulfillment workflows are in the Service Desk Process App. The Level 1 Techs, Level 2 Techs, and Level 3 Techs roles are used by all of these workflows.

Use the SBM Application 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.

Purchaser - This role is used in the **Requisition** workflow. The purchaser role is for users who will be responsible for the actually purchasing of the software or hardware.

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.

Change Management Roles

The following roles (or actors) are available in the Change Management process app. Use the SBM Application 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.

Problem Management Roles

The following roles (or actors) are available in the Problem Management process app. Use the SBM Application 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.

CMS Roles

The following roles (or actors) are available in the Configuration Management System process app. Use the SBM Application 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.

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. Use the SBM Application 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.

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 user or the administrator can subscribe the user to a notification. The administrator grants these privileges using the SBM Application 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.

Application	Notification Name	Change to Rule
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.

Configuring Request Center

Important: Before allowing users access to Request Center, promote all of the snapshots to your environment. This allows the data for Starter Pack Services to be available when you log in.

If you have remote administration privileges, you are able to customize Request Center. All customizations that you make to Request Center will affect all users.

- Adding Categories [page 27]

- Defining Services [page 28]

- Changing Logo, Announcements, and Contact Information [page 30]

- Troubleshooting [page 32]

- About the Image Picker [page 32]

Note:
When you log into Request Center as an administrator, you will see the following differences:

- In edit mode, invalid services will be marked with alert icons . Invalid services may point to a deleted project or to a project that is used by another service.

- In view mode, invalid or hidden services appear. This allows administrators to modify invalid services instead of having to create a new one. Invalid and hidden services are not seen by end users.

The following topics explain how to customize Request Center.

Adding Categories

Categories group service actions for easy navigation.

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-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 64 x 64 pixels. For information on the image picker, see About the Image Picker [page 32].

5. Enter a **Name** and **Description** for the category.

6. Select the **Display Order** for the category by dragging the slider. The lower the number, it will appear further to the left in the display.

7. Click **Save** to save the new category.

The new category will appear in the selection list. The categories are organized as follows:

1. Home category is always first.

2. Other categories are arranged by display order and then alphabetically if the display order is the same.

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, copy, or delete the category.
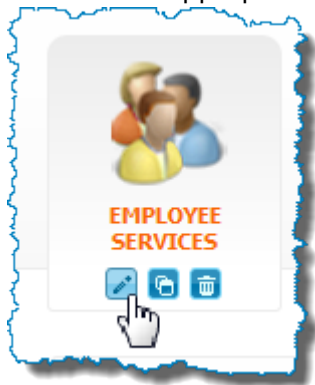
Defining Services

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 32].

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 pre-populate 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 **Charge Back** cost. 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 this field is only displayed to the end user in Request Center when values are entered.

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 **Display Order** for the service by dragging the slider. The lower the number, the higher it will be in the display order.

11. Under **Visibility**, select **Show in Catalog** to display the service to the end user. Hidden services will not appear to end users but they will still appear to administrators.

12. Select the option either to submit into an SBM process app or to show an external URL.

    - For an SBM process app, you must define what project to submit into and which submit form to use. You can specify the **Type** and pre-populate the **Title** field for the new item as well. The following table explains the different fields available on this form.

Fields	Description
Process App	Choose the process app which contains the project to submit into.
Project	Select the project to submit into. There is a one-to-one relationship between projects and services. Projects used by another service are marked and cannot be selected.
	You can modify and create projects directly. Select **Open Project** to open the selected project in SBM Application Administrator. Select **Add Project** to open SBM Application Administrator to the top level view, where you can click on **Projects**, navigate to the desired parent project and add a new sub-project. After adding the project, click to refresh the project list.
Submit Form	Select a submit form to use for submitting the item. This form will override the submit form defined in the project. The form can either be in the process app with the primary table or in a process app that has forms which reference the primary table, such as the forms contained in the Starter Pack Forms process app.
	Note: Service Desk Process App includes additional forms which are designed for transitions other than submit. Do not choose these forms, since the JavaScript included on the forms may cause unexpected behavior like a disappearing form.
Type	Select an item type for the issue to be submitted. The item types are based on the project that you selected.
Title	Enter text which will be pre-populated in the title field of the item.
SLA Summary	The SLA Summary can either be a text entry or a list of SLAs for the selected project.
	The text field can be modified and it will appear to the end user when they view the details of the service. If the project has SLAs defined, instead of the text box, you will see a list of defined SLAs and their descriptions. See Defining SLAs [page 34] for more details on defining SLAs for a project.

Note:

- There is a one-to-one relationship between projects and services. Alert icons will appear in the portal if multiple services share the same project.

- 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.

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 an **external web page**, enter the URL in the field. Choose whether to display the link within the Request Center or in a new window.

  You can also enter an **SLA Summary**, which is a description of the service level that the end user should expect. The SLA Summary field is displayed to the end user in Request Center when values are entered.

To edit, clone, or delete a service action:

1. Select **Customize | Service Catalog**.

2. Select the service action to edit, clone, or delete.

3. Click on the appropriate icon.
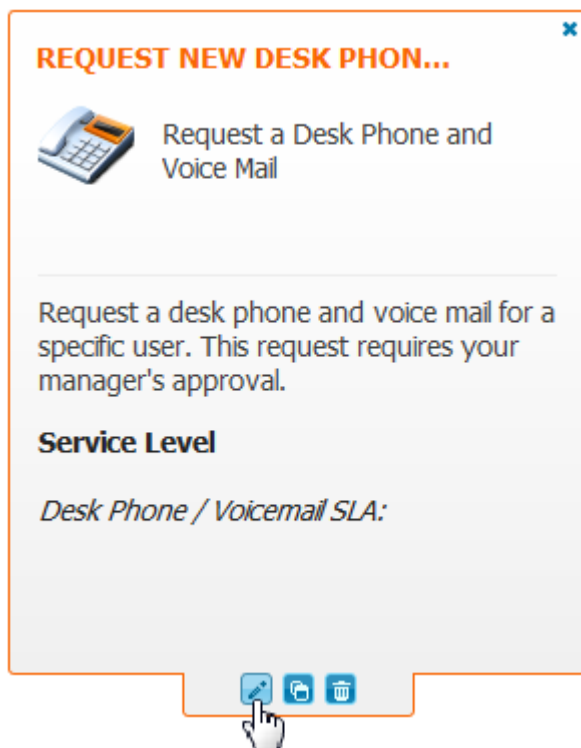
Changing Logo, Announcements, and Contact Information

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 on or off 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:

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

   > **Tip:** If you were already logged in to the Request Center, refresh your browser. This ensures that you have the latest updates to Request Center and that you will not overwrite someone else's updates. When you log in, the Request Center properties are cached locally. Failing to refresh will use the cached properties instead of the latest properties in the database.

2. Select **Customize | Request Center**.

3. 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.
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 not accessible by all users.
Image Link	Enter a URL which a user a 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 *Serena Service Manager User's Guide*.

Customization	Notes
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**.

Troubleshooting

About the Image Picker

The image picker 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.
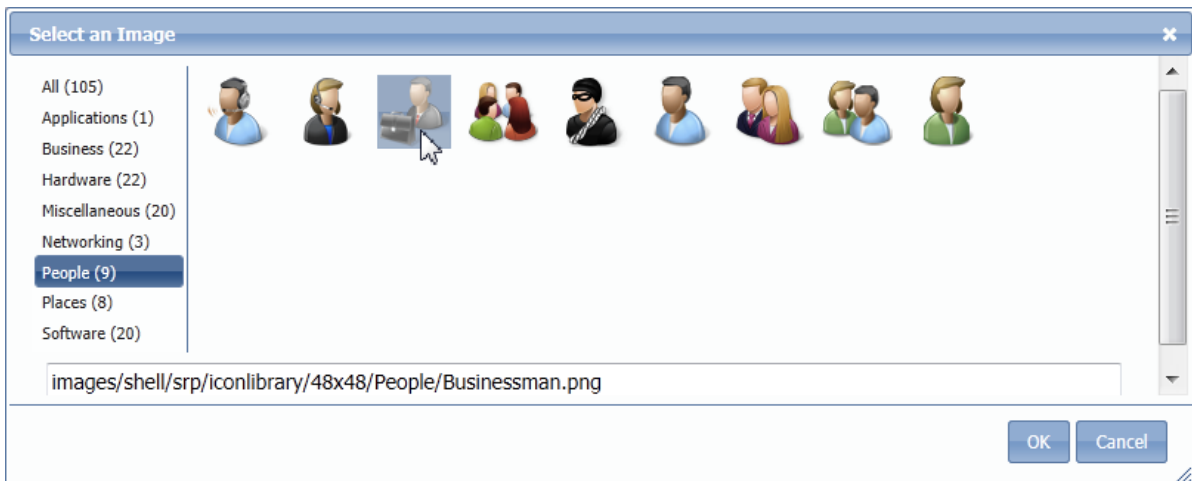
Modifying Process Apps

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.

> **Important:** The Link Release Train transition is only applicable if you have Serena® Release Manager (SRM). To eliminate confusion and possible issues, administrators should disable this transition if SRM is not installed.

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*.

General Modifications

The following sections address questions about some basic modifications that you can make to the process apps.

Can I use my existing Incident process app?

You can link your existing SBM Incident process app to the Change Management, Problem Management, and CMS process apps found in the Serena Service Manager. The procedure for doing this is beyond the scope of the book, and it is suggested that you contact Serena Professional Services for help.

Can I use my existing auxiliary tables?

You may have an existing auxiliary table that you want to link to one the process management apps. For example, you may have an existing table of Vendors and you do not want to copy all of the data to the Vendors table included with Serena Service Manager.

You can do this by editing the process apps in SBM Composer. For details, see *SBM Composer Guide*.

Can I edit the default reports?

You may edit the default reports that are included with Serena Service Manager. When saving edited reports, remember to save the reports under a new name. This will prevent

your changes from being overlayed when you upgrade to the next version of Serena Service Manager.

Can I personalize my Request Center?

You cannot personalize Request Center per individual user as changes affect all users.

Defining SLAs

Service Level Agreements (SLAs) define the level of service that an organization commits to its customers. You can use the SLA feature in SBM Application Administrator to define metrics for tracking these commitments. The topics in the SLA Settings [page 36] section describe how to do this.

Users have distinct reasons to monitor SLAs. For example, technicians need to know about SLAs that apply to their items so they can prioritize their work and understand if they are at risk of violating any SLAs. Managers need historical information to measure how well their organizations conformed to SLAs and forecast information to ensure that active items are not in danger of violating SLAs. SLA metrics can be tracked in the following ways:

- Users can customize and view SLA reports in the SBM User Workspace that include past performance and current risk information in various formats.

- Notifications can be sent to technicians and managers that alert them when violations occur or when items are at risk. This enables them to be proactive in meeting or exceeding customer expectations. You configure notifications in Application Administrator at the end of the SLA definition process, and can specify the users who should receive them. Alternatively, users can subscribe to the notifications in their user profiles in the SBM User Workspace.

- If the SLA widget control is included on state forms, users can view the status of SLAs that the current item is either in violation of or at risk of violating.

Examples

Because the SLA feature is flexible, SLAs can be tailored to specific customer requirements. The following list contains examples of SLAs that can be tracked using the SLA feature:

- High-priority items should be assigned to a technician within one business hour.

- High-priority items submitted by "Platinum" customers should be assigned to a technician within 30 minutes.

- High-priority items should be resolved within three business days.

- 99% of hardware requests should be completed within three business days of approval.

- No item can be in a "New" state for more than 3 business days.

Best Practices

SLAs need to be designed to ensure that performance measurements will be meaningful and accurate. If SLAs are defined too broadly, practical usage can cause measurements to

be distorted, or an item could remain in a certain state too long without being noticed. To prevent this, you can define more granular SLAs (or SLA clauses) that monitor specific phases of an item's lifetime.

The following illustration shows a workflow that tracks the progress of an item.
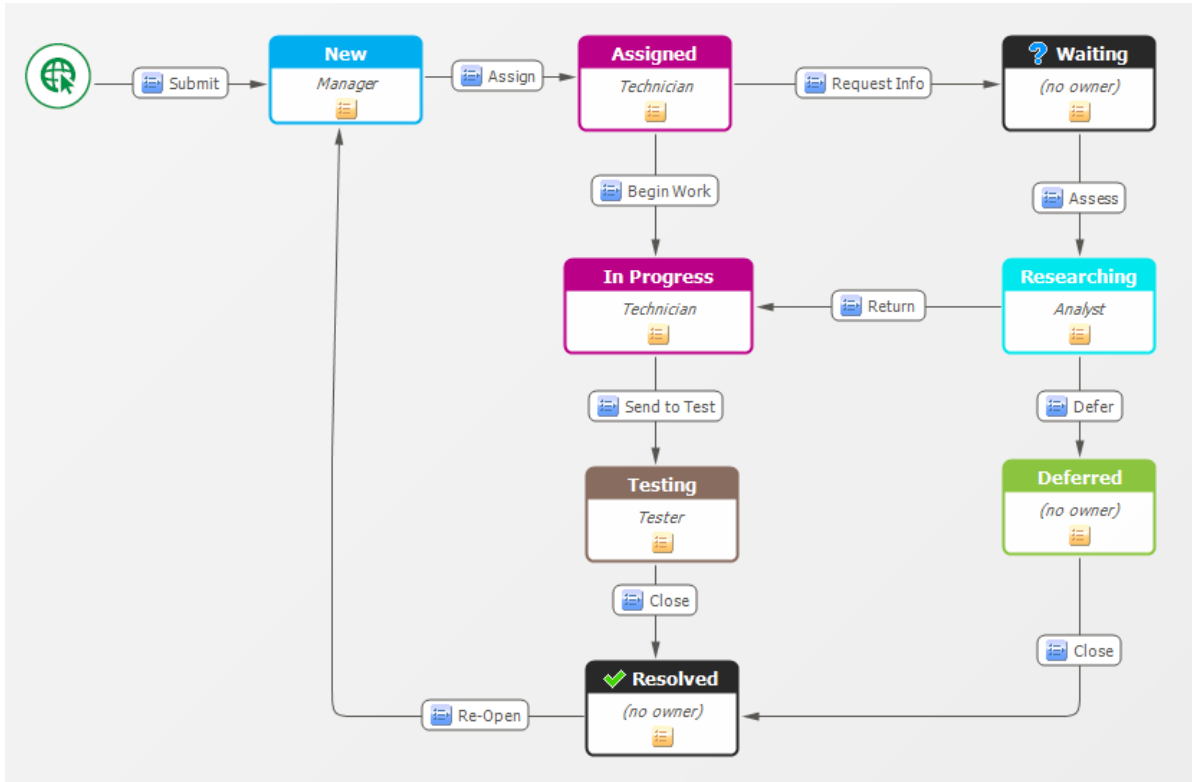
The following table describes two paths that an item could take in the workflow. (See SLA Clause General Options [page 38] for complete descriptions of the terminology used in the table.)

Scenario	Start State	End State	Paused State(s)
Entire process (SLA 1)	Assign	Resolved	Waiting, Researching, Deferred
Technician needs information before proceeding (SLA 2)	Waiting	Resolved	In Progress, Testing

When an item is in a "paused" state, time is not counted against the time remaining before the item is in violation of or at risk of violating the SLA. If only SLA 1 monitored the item, the item could remain in the "Waiting," "Researching," or "Deferred," states indefinitely. Reports would not indicate a problem, and warning notifications would not be sent. Customer service would be poor, even though it would appear that commitments are being met.

To ensure that an item is not neglected, an SLA should also be defined for the path that starts with the "Waiting" state. For example, suppose a new item must be completed

within three days, according to the high-level SLA (SLA 1). The technician needs critical information before work can start, and moves the item to the "Waiting" state.

At this point, the item is under SLA 2, which stipulates that an analyst must provide the information within four hours. Because the "Waiting" state is not a "paused" state in SLA 2, the item will have visibility in reports and notifications if the item stays in this state (or the "Researching" or "Deferred" states) too long.

SLA Settings

Restriction: To define or modify SLAs, you must have the following:

- "Managed Administrator" or "Regular User" product access type

- "Remote Administration" system privilege

- Privileges to edit projects for which SLAs are defined

Service Level Agreements (SLAs) are used to measure how well an organization responds to service requests compared to its published metrics. You define SLAs at the project level of an application.

The **SLAs** page lists the SLAs that have been defined for the project. It includes the name, description, status, and effective date of each SLA.

To access this page, in SBM Application Administrator, click the **SLAs** tab on the project page.

Note: If you change settings for an active SLA, both the old and new version of the SLA are stored. New items will use the new settings, but existing items will continue to use the original settings.

Toolbar Options

- **Add**

  Click to add a new SLA.

- **Details**

  Click to view or modify a selected SLA.

- **Delete**

  Click to delete a selected SLA.

- **Refresh**

  Click to refresh the page to its last saved state.

- *Search for SLA*

  Type a text string to find matching SLAs. After a moment, all SLAs that contain the string are displayed. To clear your text to search for something else, click ⊗.

  Tip: Click the icon next to the SLA name to see a summary of the SLA.

SLA General Options

The following options are available when you add or edit an SLA:

Toolbar Options

- **Save**

  Click to save changes made on the page.

  > **Note:** If you make changes and do not click **Save**, you are prompted to save your changes when you navigate away from the page.

- **Discard**

  Click to discard changes made on the page.

Basic SLA Options

The following options enable you to define basic SLA settings.

- **Type**

  Select **SLA** (Service Level Agreement) or **OLA** (Operational Level Agreement).

  SLAs and OLAs are defined and processed the same way, but typically an SLA addresses customer commitments, while an OLA addresses internal commitments that ensure that an SLA is met. For example, an SLA could stipulate that a PC is delivered to a customer within five business days; one OLA could stipulate that the purchasing department processes the purchase order within four hours, and another OLA could stipulate that the IT department sets up the PC within one business day.

- **Name**

  Enter a name. Names must be unique within a project.

- **Description**

  Enter an optional description.

- **Starts On**

  (Optional) Click the calendar icon and select a start date and time for when the SLA should take effect. For the time, click the hour, minute, or second, and scroll up or down. Click **Accept** to keep the values, or click **Clear** to start over or specify no start date.

- **Ends On**

  (Optional) Click the calendar icon and select an end date and time (optional) for when the SLA should stop being in effect. For the time, click the hour, minute, or second, and scroll up or down. Click **Accept** to keep the values, or click **Clear** to start over or specify no end date.

- **Threshold**

  Type a number that represents the percentage of items that must meet the SLA before it is considered in violation. If you want the threshold to be measured against a period of time, select **per month**, **per quarter**, or **per year**. This value is used in the "Performance Breakdown" SLA report in the SBM User Workspace.

- **Status**

  After you click **Save**, this field shows **Active** (if the current date and time are within the specified range), **Inactive** (if the start date and time have not been reached), or **Expired** (if the end date and time have elapsed).

  > **Note:** If you do not specify **Starts On** and **Ends On** values, the SLA is considered active.

SLA Clause Options

A clause defines when items should be monitored, and can define what should happen when items violate or are at risk of violating the criteria defined for it. An SLA can contain multiple clauses. The following are examples of clauses:

- Items in the "New" state must reach the "Assigned" state within two hours if the value of the *Priority* field is "High." If the item is still in the "New" state and is 30 minutes away from being at high risk, an e-mail notification will be sent to the manager.

- Items in the "Assigned" state must reach the "Resolved" state within three business days if the value of the *Request Type* field is "Hardware," and time should not be counted against the SLA when the item is in the "Waiting for Customer" state.

- Items in the "Work Started" state must reach the "Tested" state within one business day if the value of the *Impact* field is "All work stopped."

When you click the **Clauses** tab, a list of existing clauses is displayed. The list includes the name, description, and duration of each clause.

The following toolbar options are available:

- **Add**

  Click to add a new clause.

- **Details**

  Select a clause and then click this button to view or edit the clause.

- **Delete**

  Select a clause and then click this button to delete the clause.

- **Refresh**

  Click to refresh the page to its last saved state.

By default, the **Group by path** check box is selected, and defined clauses are organized on this page according to the path specified in the SLA Clause General Options [page 38]. Clear this check box if you want to view defined clauses alphabetically by name.

SLA Clause General Options

The following options are available when you add or edit a clause:

Toolbar Options

- **Save**

Click to save changes made on the page.

> **Note:** If you make changes and do not click **Save**, you are prompted to save your changes when you navigate away from the page.

- **Discard**

  Click to discard changes made on the page.

- **Show Workflow**

  Click to show the visual workflow assigned to the project.

Basic Clause Options

- **Name**

  Type a name. Names must be unique within an SLA.

- **Description**

  Type an optional description.

Time & Risk Options

- **Duration**

  Type a number and then select **Minute(s)**, **Hour(s)**, **Day(s)**, or **Week(s)**. This option specifies how long the clause will stay in effect, beginning with the start date and time for the SLA. The default value is **2 Day(s)**.

- **Calendar**

  By default, **24-hour Calendar** is selected. If other calendars have been defined for the project, you can select them from the drop-down list.

- **Risk**

  This option enables you to define risk levels in terms of time remaining before items are in violation of this SLA. When 100% of the time remains, the risk is considered **Low**. When 0% of the time remains, items are in **Violation**. You can define the percentage of time remaining that puts items in **Medium** or **High** risk of violation. The default value for medium risk is 50%; the default value for high risk is 25%.

Path Options

Path options enable you to define the range of states in the workflow that needs to be monitored. For example, if the SLA states that 99% of hardware requests must be completed within 3 business days of approval, the path would start with the "Approved" state and end with the "Completed" state. If a technician needs information from a customer before proceeding, then the "Waiting for Input" state should be defined as a "paused" state, because the time an item is in this state should not be counted against the time remaining.

> **Tip:** Click **Show Workflow** in the toolbar to view the entire process flow.

- **Start State**

Select the start state from the list, or type ahead to search for states containing the characters you type. Click ✕ to clear the search and start over.

- **End State**

   Select the end state from the list, or type ahead to search for states containing the characters you type. Click ✕ to clear the search and start over.

- **Paused State(s)**

   Click the box or the button, and then select the states to exclude from SLA calculations.

Qualifying Conditions

You must define at least one condition that evaluate to "true" before the clause takes effect. For example, the SLA might only be relevant if the value of the *Customer Rank* field is "Gold."

To add or edit a condition:

1. To add a condition, click **Add condition** and then click **Click here to edit**.

2. To edit a condition, click the condition.

3. Select the field you want to evaluate.

4. Select a comparison operator.

5. Select or type a value to compare to the field, or type ahead to search for a value.

6. Click **OK**.

If you define multiple conditions, they are joined by logical operators. **AND** means that both conditions must evaluate to "true" before the clause is put into effect; **OR** means that only one condition must evaluate to "true." Click the logical operator to toggle between them.

You can view a string that represents the conditions in the **Summary** section.

SLA Clause Action Options

Actions define what should happen when items are in violation or at risk of being in violation of the conditions defined in a clause. When you click the **Actions** tab, a list of existing actions is displayed. The list includes the name and description of each action.

The following toolbar options are available:

- **Add**

   Click to add a new action.

- **Details**

   Select an action and then click this button to view or edit the action.

- **Delete**

   Select an action and then click this button to delete the action.

- **Refresh**

  Click to refresh the page to its last saved state.

SLA Action Options

The following options are available when you add or edit an action:

Toolbar Options

- **Save**

  Click to save changes made on the page.

  > **Note:** If you make changes and do not click **Save**, you are prompted to save your changes when you navigate away from the page.

- **Discard**

  Click to discard changes made on the page.

Basic Action Options

- **Name**

  Type a name. Names must be unique within a clause.

- **Description**

  Type an optional description.

Conditions

You must define at least one **WHEN** or **IF** condition.

- **WHEN**

  You can specify that a notification be sent before an SLA reaches a state of violation or risk so that preemptive actions can be taken. The WHEN condition specifies this time period. For example, you may want a manager to be notified when a service request has not been fulfilled, and only four hours remain before the SLA is violated.

  To add or edit a WHEN condition:

  1. To add a condition, click **Add condition** in the **WHEN** section, and then click **Click here to edit**.

  2. To edit a condition, click the condition.

  3. Type a number and select **minutes**, **hours**, **days**, or **weeks**.

  4. Select **High**, **Medium**, or **Violation**.

  5. Click **OK**.

- **IF**

  IF conditions define conditions other than timing that must be true before the action is taken. IF conditions are based on field values. For example, the action only needs to be taken WHEN you are six hours from high risk IF the value of the *Priority* field is "High."

To add or edit a condition:

1. To add a condition, click **Add condition** in the **IF** section, and then click **Click here to edit**.

2. To edit a condition, click the condition .

3. Select the field you want to evaluate.

4. Select a comparison operator.

5. Select or type a value to compare to the field, or type ahead to search for a value.

6. Click **OK**.

- **Summary**

A string that represents the conditions is displayed in this section.

- **THEN**

The THEN condition defines the action to take when the WHEN and IF conditions are met. When you click the **+** icon next to **Run notification**, the **Add Notification** page opens. When you click the icon next to an existing notification, the **Edit Notification** page opens. Refer to the notifications documentation for instructions on defining and editing notifications.

> **Note:**
>
> - The Notification Actions that are available for SLAs are **NO ACTION**, **SEND E-MAIL**, **RUN SCRIPT** (on-premise only), and **RUN WEB SERVICE**.
>
> - There are no SLA-specific Notification template tags; it is recommended that you create e-mail templates for SLAs, and include pertinent SLA information in each template.
>
> - Not all notification options are available for SLAs.

Chapter 4: Additional Information

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

- Integrations Between Applications [page 43]

- Additional ITIL References [page 43]

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/