SERENA

SERENA®
BUSINESS MANAGER

SBM Application Administrator Guide

Trademarks

U.S. Government Rights

Part number: Product version: 10.1.5.1

Publication date: 2015-04-13

Table of Contents

Chapter 1: Introduction to SBM Application Administrator

Audience and Scope

The information you find here is intended for administrators who will use SBM Application Administrator to configure deployed applications in an SBM environment.

Information for both on-demand and on-premise systems is included, but exceptions in functionality are called out as needed.

Guide to SBM Documentation

The SBM documentation set includes manuals for all user audiences.

Most documents are installed with SBM and are also available here:

- Serena support: http://www.serena.com/support
- Documentation Center

Readme

The SBM readme contains important information about a particular SBM release, including what's new, additional changes, and steps for upgrading from a prior verison of SBM. Refer to the readme for each SBM upgrade that you perform.

The readme is located on the Documentation Center.

End-user Documentation

Title	Description
Serena Work Center Guide	Provides guidance using Work Center. This document is available on the Documentation Center.
SBM User's Guide	Instructions on using the SBM User Workspace.
SBM Reporting Guide	Provides guidance for using the SBM's robust reporting feature.

Process App Designers and Administrators

Title	Description
SBM Composer Guide	Provides details on using SBM Composer to create the tables, fields, workflows, forms, and other design elements comprised in process apps. Information about saving, versioning, importing, and exporting process apps is also provided. This document is intended for individuals who want to design and maintain process apps.
SBM Orchestration Guide	Provides information about using SBM Composer to create orchestrations that use Web services to coordinate the interaction between an SBM application and one or more external systems. Advanced information, such as how to raise events through e-mail messages and JMS queues, is also provided.
SBM Application Administrator Guide	Explains how to configure deployed applications. Instructions for managing projects, user and group accounts, and notifications are included.

System Administrators

Title	Description
SBM Installation and Configuration Guide	Provides information on installing SBM and creating a database. Database and Web server configuration information is also provided.
SBM Application Repository Guide	Provides information on using SBM Application Repository to deploy process apps to runtime environments and to promote configured applications from one environment to another.
SBM System Administrator Guide	Provides information on administering the SBM Application Engine. Instructions for database utilities and system settings are included.
SBM Licensing Guide	Explains how to manage licenses for Serena® Business Manager. License types are discussed, along with instructions for installing and using the Serena License Manager. This guide is intended for administrators who will install and implement Serena® Business Manager.

Title	Description
Moving to Serena® Business Manager	Provides migration information for existing TeamTrack customers who are moving to SBM. It explains how to upgrade your existing system, and it explains the expanded SBM paradigm in relation to the TeamTrack paradigm.

Developers

Title	Description
SBM Web Services Developer's Guide	Provides an overview of all SBM Web services, including descriptions for all calls, arguments, and responses. Installation instructions and information about the sample Web service programs are also provided.
SBM JavaScript Library Guide	Provides information about using the functions in the SBM JavaScript library to create dynamic custom forms.
SBM AppScript Reference	Provides information on customizing SBM using SBM AppScript, a programming language built around VBScript 4.0. This guide is intended for VBScript programmers who want to use SBM AppScript to implement custom features in an SBM system.

About Application Administration

SBM Application Administrator enables you to perform application configuration tasks—such as adding projects and assigning them to workflows, creating user accounts and assigning them to roles and groups, and creating notifications.

You can also use Application Administrator to import users, import data from spreadsheets, manage record locks, create business calendars, and manage items in auxiliary tables.

Note: Application Administrator requires the Adobe Flash Player. If the Flash Player is not installed or enabled for your browser, you are prompted to install or enable it when you open Application Administrator. If you are using Internet Explorer 11 or later, you must use Adobe Flash Player 13 or later.

Administrative Concepts

Make sure that you understand the following administrative concepts before you use SBM Application Administrator.

SBM Composer

SBM Composer is used to design applications, including workflows, states, transitions, forms, roles, and other process elements. Once deployed, these applications are configured using SBM Application Administrator.

Applications

An application is a collection of elements that work together in an interactive process to solve a business requirement, such as managing work tasks or tracking customer support calls. An application is based on a single primary table and typically contains workflows, fields, forms, roles, projects, reports, and notifications. Applications are created in SBM Composer as part of a process app, which can contain multiple applications.

Projects

Projects serve as storage bins for primary items, which follow a workflow. Projects are grouped by application.

Projects enable you to organize groups of primary items in a way that makes sense for your workflow. For example, you can create a project for each functional team working on a product or for each version of the product.

Workflows

A workflow is a collection of states, transitions, and fields that define a process. Workflows are created in SBM Composer and deployed to your runtime environment. You can then assign projects to workflows. This two-fold system enables you to first define your processes, and then assign them to projects to track primary items at various levels. Several projects may use the same workflow.

Roles

A role is a collection of application-related privileges. Users may have different roles in different projects, and a user can be assigned to multiple roles. Examples of the types of permissions associated with a role are the ability to view and update fields; the ability to perform specified actions on items, attachments, notes, and reports; and the ability to specify access to, or restriction from, certain transitions. Designers create roles in SBM Composer as part of an application.

User Accounts

Each user has an account with characteristics such as a user login ID, password, and e-mail address. Each account has privileges associated with it that determine the information the user can access and functions the user can perform. Privileges are assigned to users as part of their group membership and role assignment.

Groups

A group is a named collection of users who have the same privilege set. A group might be created for a particular project, for example, or for a division within the company. A user can be assigned to multiple groups.

The core privileges available for groups and roles are generally the same. However, groups contain additional privileges, such as system and administrative privileges that are not available with roles. Typically, complex process apps require a combination of roles with the additional privileges that groups provide.

Resources

Resources enable you to manage resource team assignments, scheduling, job functions, and skills of employees in your organization. Resources can be based on SBM user accounts or for employees who do not have SBM accounts. This information can be used for assigning resource teams to plans in Serena Demand Center or for other planning purposes.

Notifications

Notifications are generated when certain events occur in the system. For example, users can be sent e-mail notifications when an item is assigned to them. Notifications can also be used to execute scripts, call Web service functions, and automatically add and remove items from folders.

"Quick" Administrator Features

When a new process app is deployed, certain features are automatically enabled. This eases the process of adding new applications.

"Quick" Administrator features include:

- A project is created for each application workflow. The project name is the workflow name, appended with the string "Project". If the workflow name includes "Workflow", it is replaced by "Project". If necessary, the whole name is truncated to 32 characters to comply with database constraints.
- The application workflow hierarchy becomes the project hierarchy.
- The person who deployed the process app can view and submit items into the application's projects and is automatically assigned all roles on these projects.
- A default set of notifications are automatically created. For details, refer to Provided Notifications [page 270].

Key Benefits

- Eases the process of configuring applications.
- Allows for quick testing of applications as they are being developed.
- Provides a foundation for a more complex project hierarchy.

Managed Administration

Depending on your product-access type and privileges, you may only be able to administer specific applications and application features, users, and groups. For details, refer to Chapter 6: Managing Administrators [page 255].

Administrative Locking

Application Administrator does not lock application elements with features, such as projects, roles, users, groups, and notifications.

If multiple administrators edit the same feature, such as a project, at the same time, and one administrator saves his or her changes, a pop-up opens for the next administrator who attempts to save changes. This administrator can select one of the following options:

- **Save My Changes**

Delete changes made by the first administrator and save your changes.

- **Get Data**

  Delete your changes and update the page with the changes made by the first administrator.

- **Cancel**

  Cancel the save operation.

Steps for Configuring Applications

Below is the typical process followed in Application Administrator when a process app is first deployed from SBM Composer.

1. A project is automatically created for each application workflow the first time a process app is deployed. Configure this project or create additional projects and assign them to the application workflow as needed. For details, refer to Working With Projects [page 30].
2. Create groups to organize sets of users. For details, refer to Working With Groups [page 172].
3. Add user accounts and assign users to roles included in the application or to groups. Verify that these users have the privileges they need to access the projects, work with data, and transition items. For details, refer to Working With User Accounts [page 145].
4. Further configure projects by setting field overrides, configuring e-mail submission, and more.
5. Add selections to *User*, *Multi-User*, and *Multi-Group* fields as needed. For details, refer to Adding User and Group Values [page 81].
6. Modify the default set of notifications and notification rules for each workflow in your application, or create your own rules and notifications. For details, refer to Working With Notifications [page 274].
7. Create accounts for other administrators as needed. For details, refer to Chapter 6: Managing Administrators [page 255].
8. Set deployment privileges for the process app for other administrators in Application Repository. For details, refer to *SBM Application Repository Guide*.
9. Log in to one of the end-user interfaces and test your work:
   - Serena Work Center

     `http://serverName/workcenter`

   - SBM User Workspace

     `http://serverName/tmtrack/tmtrack.dll?`

Modern Browser Support

Many SBM features require Web browsers that support HTML5. Some of these features are not available in older browsers, such as Internet Explorer (IE) 8.

These features include:

- Serena Work Center
- Rich Text Editor for applying formatting to e-mail messages, notes, and certain *Text* fields.
- Updated form styling and modern themes
- Drill-down display options for Distribution, Advanced Distribution, Summary, Time to State, Elapsed Time, Trend, Backlog Trend, Entering a State, Open and Completed, and State Activity reports (if Flash components are also disabled)
- Elapsed Time reports (if Flash components are also disabled)
- User profile card
- Group member lists for *Multi-User* fields on State forms
- Translated strings in the workflow diagram
- Second background colors and corner radius settings on custom forms

If you have problems using these features, you can:

- Upgrade your browser, or
- Contact your administrator and ask for HTML5 features to be disabled.

In addition, Compatibility Mode should be disabled in all versions of Internet Explorer.

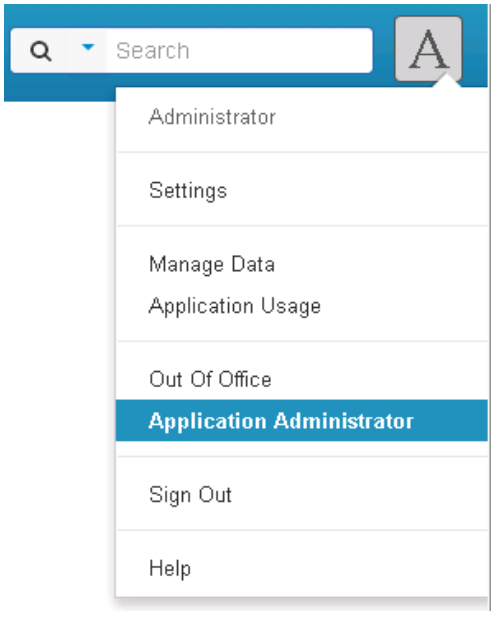
Note: Administrators who use Internet Explorer 8 and who need to disable HTML5 features should log directly into SBM Application Administrator using this URL: `http://serverName/tmtrack/tmtrack.dll?StdPage&Template=newwebadmin/index.html`.

Parts of the SBM Application Administrator Interface

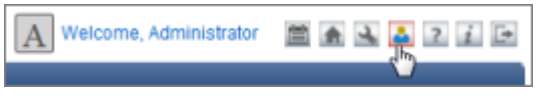
The Administrator Portal

The Application Administrator provides access to application configuration features and utilities.

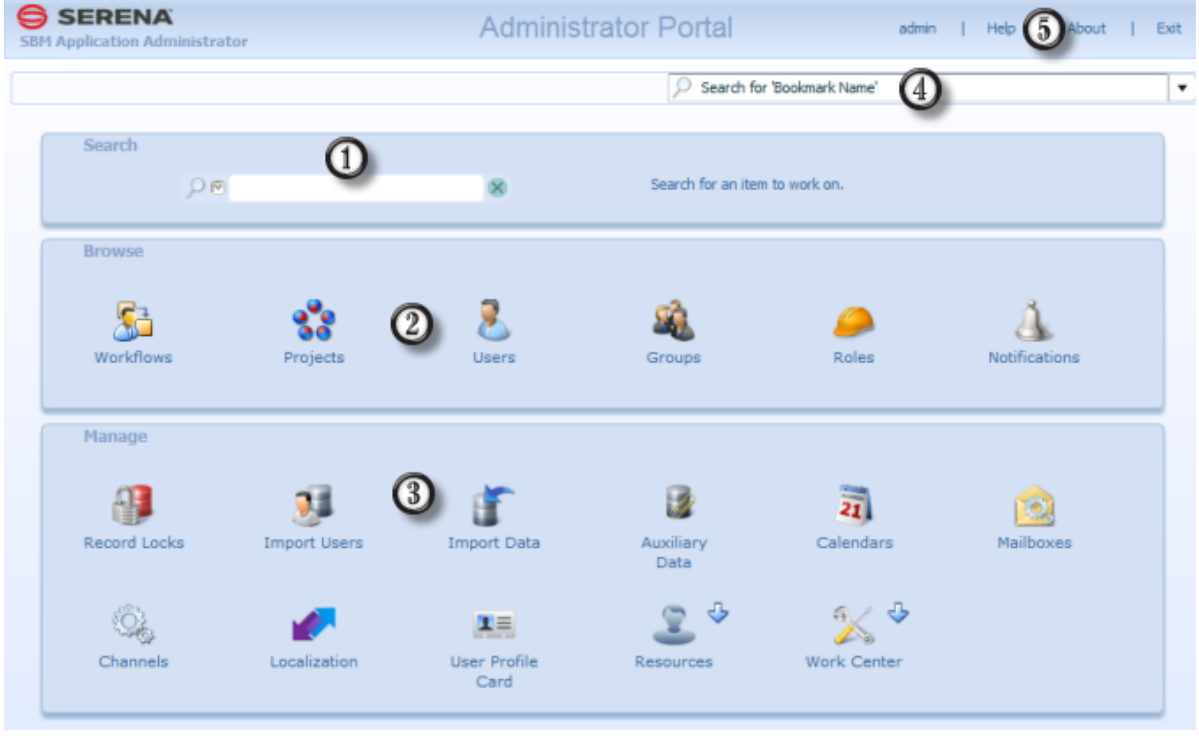
To open the Application Administrator from Serena Work Center, click the user icon in the upper right corner, and then select Application Administrator.



To open the Application Administrator from the SBM User Workspace, click the **Administrator** icon.



The **Administrator Portal** has the following parts:



1. **Search**

Search for users, groups, and projects by name. Select an item in the results list to open links to quick actions, such as **Edit User** (when a user is selected) or **Edit Project** (when a project is selected).

2. **Browse**
   Click the icons to configure application elements. For details, refer to:
   - About Workflows [page 81]
   - About Projects [page 29]
   - About User Accounts [page 144]
   - About Group Accounts [page 172]
   - About Roles [page 168]
   - About Notifications [page 269]
3. **Manage**
   Click the icons to open administrative utilities. For details, refer to:
   - About Record Locks [page 349]
   - About User Import [page 350]
   - About Data Import [page 378]
   - About Auxiliary Data [page 389]
   - About Calendars [page 390]
   - Chapter 11: E-mail Setup [page 435]
   - About Channels [page 395]
   - About Localization [page 397]
   - About the User Profile Card [page 250]
   - About Resources [page 407]
   - About Work Center [page 327]
4. **Bookmarks**

   Select or search for a bookmark in the list. Bookmarks enable you to quickly access to certain features, such as users, groups, roles, projects, and notifications. For details, refer to Using Bookmarks [page 25].
5. **Toolbar**
   Provides the following links and information:
   - ***User Name***

     Indicates the user logged into the system.
   - **Help**

     Click to open online help for the page you are viewing.

- **About**

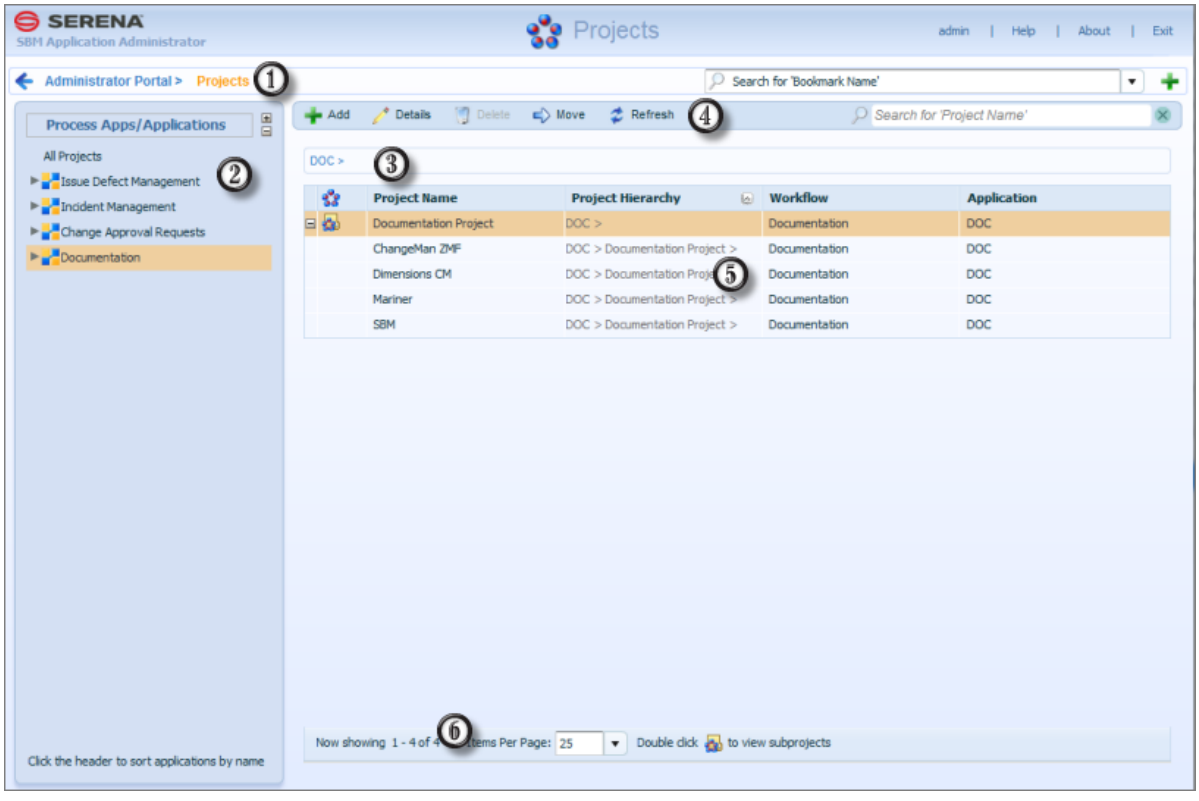
  Click to view version and configuration information.

- **Exit**

  Click to log out of Application Administrator.

Feature Views

Views refer to the main pages for specific areas of the interface, such as the **Projects** view or the **Notifications** view. The following figure shows an example of a view and explains the terminology used to describe the most common parts of the interface.



1. **Navigation Links**

   Use this link to return to the **Administrator portal**. If you have drilled down into a specific feature, such as a user account, you can also use this link to return to the **Users** view, for example. The orange text indicates the page you are currently viewing.

2. **Navigation Pane**

   Refers to the left pane, which is used to navigate to specific feature areas. Some features, such as projects and notifications, require you to navigate the applications list. Other features, such as users and groups, provide tabs that open content pages.

3. **Bread Crumbs**

Use bread crumbs to return to the **Administrator Portal**. If you have drilled down into a specific feature, such as a user account, you can also use this link to return to the **Users** view, for example.

4. **Toolbar**

   All content pages include a toolbar containing buttons and links that enable you to add, edit, delete items and more. A **Search** box is also available on the toolbar for most features. This search mechanism applies to the feature you are working with. For example, from the **Users** view, you can search for users by name or login ID.

5. **Content Pages**

   Refers to pages that enable you to view and configure various features. Most of your work will be done in these pages, which may be divided into various panes.

6. **Pagination**

   Use **Items Per Page** to set the number of items to display on pages that contain long data lists, such as projects, fields, users, and groups. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Screen Resolution and Sizing

SBM is designed for screen resolutions of 1024x768 or higher. You may experience problems if you use a lower resolution, such as 800x600.

If SBM is difficult to read at the minimum resolution of 1024x768, you can increase the browser's Zoom setting. For example, changing the browser's Zoom to 125 percent will increase the size of text, buttons, and other controls throughout the interface. Be aware that increasing the Zoom from 100 percent may require you to scroll through pages as you work, however.

Using Bookmarks

Bookmarks enable you to save personal links to frequently used features, such as users, groups, and projects.

You can open these bookmarks in SBM Application Administrator or in the SBM User Workspace if "auto folder items" are enabled for your system and your user profile.

You can create bookmarks from the following administrative features:

- **User Accounts**

  Create bookmarks to the **Users** view or to the **Details** page for one or more user accounts.

- **Groups**

  Create bookmarks to the **Groups** view or to the **Details** page for one or more group accounts.

- **Roles**

  Create a bookmark to the **Roles** view.

- **Projects**

Create a bookmark to the **Projects** view or to the **Details** page for a specific project.

- **Workflows**

  Create a bookmark to the **Workflows** view or to the **Details** page for a specific workflow.

- **Notifications**

  Create a bookmark to the **Notifications** view.

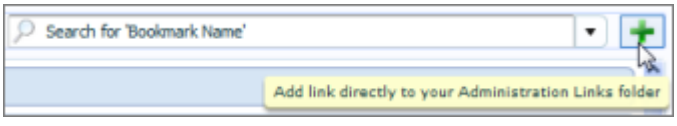
- **Resources**

  Create a bookmark to the **Resources**, **Resource Teams**, **Job Functions**, or **Skills** views.

Adding Bookmarks

To add a bookmark:

1. Navigate to one of the pages listed in the previous section. For example, edit a user account.
2. Click the green plus sign in the upper right corner.



3. In the dialog box that opens, rename the bookmark as needed, and then click **OK**.

Opening Bookmarked Page

You can open bookmarked administrative pages from SBM Application Administrator or the SBM User Workspace.

To open a bookmark from SBM Application Administrator, select the bookmark from the list, or search for a bookmark, and then select it.

To open an administrative bookmark from the SBM User Workspace:

1. Verify that "auto folders" are enabled in your user profile. In the SBM User Workspace, this setting is located on the **Display** tab of your user profile.

   Note: If the **Auto Folders** option is not available, this feature has not been enabled for your system.

2. In the navigation pane, select the **Favorites** tab.
3. Expand the **Administration Links** folder, and then select a bookmark.

The administrative feature opens in the content pane of the SBM User Workspace.

Deleting and Renaming Bookmarks

You can delete bookmarks by removing them from the Administration Links Favorites folder in the SBM User Workspace. You can also rename administrative bookmarks in this folder.

If you have permissions to edit your user account in SBM Application Administrator, you can also delete bookmarks from the **Content** tab of your user preferences.

Chapter 2: Managing Projects

The following topics describe how to administer projects in SBM Application Administrator.

About Projects

Serena Business Manager simplifies the process of managing an organization's work efforts by enforcing a process for these efforts. Application workflows are defined in SBM Composer and determine how work efforts, referred to as primary items, are tracked as they move through the established process.

Projects serve as storage bins for primary items and enable you to organize groups of items in a way that makes sense for your workflow. For example, you can create projects to store items for each team working on a product, or you can create projects for each version of the product. You can then configure the project by overriding specific workflow properties. You control access to items in the project by enabling roles for the project or assigning privileges to users and groups.

After you deploy an application from SBM Composer, you create projects in SBM Application Administrator and assign them to workflows. Once projects are established and contain primary items, users can create reports that provide critical information about the items in projects. This structure provides visibility and control over your processes.

Key Benefits

- Organize items tracked in your process by team, function, or other categories.
- Control access to items by enabling roles for specific projects or assigning privileges to users and groups for specific projects.
- Create reports based on items in projects.
- Use overrides to tailor certain settings inherited from the workflow.
- Use inheritance to easily assign parent project properties, privileges, and role assignments to any or all sub-projects.

About the Project Hierarchy, Inheritance, and Overrides

Projects follow a hierarchy structure that allows for flexibility and easy maintenance of project settings through inheritance.

Each application typically has a set of parent projects assigned to corresponding workflows. Projects inherit settings from these workflows. You can override workflow settings at a parent project, and child projects can inherit these settings when you select the **Use Parent Project's Workflow** checkbox on the **General** page for the project. Or, you can override settings at a child project, if necessary.

In addition, applications may have sibling projects, which can have a unique set of overrides.

Tip: To ease maintenance, overrides should be applied at the highest level possible. For example, if a workflow is used for two sets of projects, apply overrides at the parent of each project set.

The Base Project

All projects are ultimately children of the Base Project, which sits at the top of the project hierarchy. The Base Project is a header project and cannot be deleted; therefore, it always exists. Primary items cannot be submitted into the base project.

When you apply settings for the Base Project, you are essentially applying settings for all projects in the system. Some of these settings can be overridden for specific projects or a set of projects. For details, refer to Enabling System Settings From the Base Project [page 37].

To navigate to the Base Project, select **All Projects** at the top of the **Process Apps/ Applications** list.

About Projects Provided by Quick Administrator

To accelerate the setup process, a project is automatically created for each application workflow and sub-workflow in a process app after it is deployed for the first time. These projects inherit all properties from the workflow to which they are assigned, including the project name. If the workflow name includes the word "Workflow", it is replaced by "Project". For example, if your workflow is named "Widgets Workflow," a project named "Widgets Project" is created and assigned to the Widgets Workflow.

Projects added by Quick Administrator are set to allow new items to be submitted and to use the parent project's item numbering sequence. You can modify these settings as needed, as well as rename the project or add sub-projects. You must also manually assign roles to these projects, if applicable.

Working With Projects

Project configuration tasks are performed exclusively in Application Administrator. There are two types of project configuration tasks:

- Project-specific settings
- Overrides to the application workflow defined in SBM Composer

Project-specific Settings

- Add, edit, delete, and reorder projects
- Assign workflows to projects
- Enable or disable submissions for projects

- Set primary item numbering sequence
- Set dependent *User*, *Multi-User*, or *Multi-Group* field selections for independent *User* fields
- Configure mailboxes used for e-mail submissions
- Create custom response templates for e-mail submissions
- Map enumerations for *User*, *Folder*, and *Project* fields defined in Web service actions.

Project Overrides

- Override default state and transition forms
- Override default project, state, and transition field ordering when quick forms are used
- Override field attributes and default values for projects and transition fields
- Override display options for fields in projects and transition fields (except *Binary/ Trinary*, *Date/Time, Numeric,* and *Text* fields)
- Override dependent field selections for independent *Single Selection* fields
- Override transition button ordering
- Override authentication settings for transitions
- Override project settings for Post and Subtask transition types
- Override application variables values used by rules

For details on project configuration tasks, refer to:

- Working With Projects [page 30]
- Working With States and Transitions in Projects [page 60]
- Working With Fields [page 94]
- Mailboxes and E-mail Submission [page 435]
- About Application Variables [page 77]
- Frequently Asked Questions About Projects [page 79]

Navigating Projects

Projects follow a hierarchy structure that allows for easy maintenance of project settings. All projects are ultimately children of the Base Project, which sits at the top of the project hierarchy. Each application typically has a set of parent projects assigned to corresponding workflows, with child projects inheriting from the parents. You can also have sibling projects, which may have a unique set of overrides. For details on the benefits of the project hierarchy, refer to About the Project Hierarchy, Inheritance, and Overrides [page 29].

In SBM Application Administrator, you can navigate the project hierarchy to view and work with projects. To get started, select the **Projects** icon on the **Administrator Portal**, and then follow the steps below as they apply.

If you do not know which process app contains your project or you do not know the project's exact name:

1. Type a few letters of the project's name in the **Search** box.
2. All projects meeting your search criteria are returned.
3. If needed, sort the list by project name, project hierarchy, or assigned workflow.
4. Double-click a project to open it.

If you know which process app contains your project:

1. The process apps and applications that you can access appear in the left pane.
2. Expand a process app, and then select an application.

   The application's parent projects appear in the **Project List** pane.

3. Navigate the hierarchy as follows:

   - Double-click a project that has a **Parent** icon ( ) to view the project hierarchy.
   - Click the plus sign to expand the list to all projects assigned to the parent project.
   - Click the column headers to alphabetically sort projects by name, project hierarchy, or assigned workflow. This sorting only applies to the view in Application Administrator; to change the project hierarchy and ordering as it is shown to users, click **Move**.

If you want to browse the project hierarchy for all process apps:

- Select **All Projects** in the Process Apps/Applications pane.
- Double-click the first project in the project list, which is typically called "Base Project."
- Navigate the hierarchy as follows:
  - Double-click a project that has a **Parent** icon ( ) to view the project hierarchy.

- Click the plus sign to expand the list to all projects assigned to the parent project.
- Click the column headers to alphabetically sort projects by name, project hierarchy, or assigned workflow. This sorting only applies to the view in Application Administrator; to change the project hierarchy and ordering as it is shown to users, click **Move**.

Browsing Tips:

- If your application contains a large number of projects, use the search feature or navigation options at the bottom of the page to find a specific project.
- To move quickly to a parent project in the displayed project hierarchy, click the appropriate link in the list of "breadcrumbs", which appear directly above the **Project Name** field.
- Double-click the "double dot" symbol `(..)` to return to the list containing the parent project.

Adding and Editing Projects

Depending on your administrative privileges, you can add and edit projects within an application's project hierarchy or at the Base Project level.

When you add a project beneath a parent project, the new project initially inherits the parent's workflow assignment, configuration settings, role assignments, and field overrides. You can change these as necessary.

To add or edit a project:

1. From the **Administrator Portal**, select the **Projects** icon. The process apps and applications that you can access appear in the left pane.
2. To add or edit a project for a specific application, expand the process app that contains the application by clicking the right arrow, and then select the application under the process app. The application's parent projects appear on the **Project Name** page.
3. Do one of the following:
   - To edit an existing project, navigate to or search for the project, select it in the list, and then click **Details**.
   - To add a sub-project, select the project that will serve as the parent for the new project, and then click **Add**.

     Note: You may need to expand the project tree to select the correct parent project. To do so, double-click the **Project** icon ( ).
   - To add a project at an application root, select **All Projects** in the navigation pane, select **Base Project** in the project list, and then click **Add**. Be sure to select the workflow that corresponds to the correct application on the **General** project settings page.
4. Specify settings on the **General** page. For details, refer to General Project Settings [page 40].

5. Specify field overrides for the project on the **Default Fields** page. For details, refer to Fields Page Settings [page 44].
6. Specify state and transition overrides for the project on the **States/Transitions** page. For details, refer to States and Transitions Page [page 46].
7. Specify role assignments for the project on the **Roles** page. for details, refer to Project Role Settings [page 48].
8. Override values for application variables as applicable. For details, refer to Overriding Values for Application Variables [page 78].
9. If the project will accept e-mail submissions, configure a mailbox. For details, refer to Mailboxes and E-mail Submission [page 435].
10. Save your changes.

Moving and Reordering Projects

You can organize projects by:

- Reordering them within their established hierarchy.
- Moving sub-projects to different parent projects within the same application.
- Moving a parent project and all of its sub-projects within the same application.

Consider the following information when moving or reordering projects:

- When a project is moved, all of its sub-projects are moved with it.
- You cannot move projects to the project hierarchy for another application.
- Moving projects can affect inherited properties, such as field ordering, transition order, and transition settings and unexpected changes in project functionality can occur. You can safely move projects if both the new and old parent projects inherit all fields, states, and transitions from a common parent.

To move or reorder projects:

1. From the **Administrator Portal**, select the **Projects** icon.
2. Select a process app in the left pane.
3. Click **Move**, and then:
   - To reorder projects at the same hierarchical level:
     a. Clear the **Position Within** check box.
     b. In the Destination list, navigate to the list of projects you want to reorder.
     c. Click the project sort icon ( ) to see the current sort order.
     d. Drag and drop projects to the preferred order.
   - To move a project and its sub-projects to a different parent:
     a. Select the **Position Within** check box.

b. In the Source list, search for or navigate to the project you want to move.

Tip: Use the project links at below the **Search** boxes to move through the project hierarchy in the Source and Destination lists.

c. In the Destination list, search for or navigate to the project that will serve as the new parent.

d. With both projects selected, click the right arrow button or drag the source project on top of the destination project.

e. You are prompted that you may lose inherited properties if you move the project to a different parent project. Click **Yes** to complete the move or **No** to cancel it.

4. Click **Undo** at any time to cancel your changes; click **Close** to save your changes.

Deleting Projects

When you delete a project, all primary items associated with that project are deleted, along with the change history for these items. Overrides and settings associated with the project, such as field properties, orderings, and selections, are deleted, along with role, user, and group privileges associated with the project. You can choose to keep the project's archived items stored in the database for use with third-party reporting tools, but users cannot view these archived items in SBM user interfaces.

CAUTION:

Once a project has been deleted, there is no way to recover the information, so use this feature with caution. Before deleting a project, consider the options in Alternatives to Deleting Projects [page 36].

To delete a project:

1. In the **Projects** view, navigate to the project you want to delete.
2. Select the project, and then click **Delete**.

Note: You cannot delete a parent project without first deleting its sub-projects.

3. A confirmation dialog box opens. Select one of the following options:
   - **Delete**

     Click to delete the project and all non-archived items. Archived items remain in the database for use with third-party reporting tools.
   - **Delete and Purge**

     Click to delete the project and all items, even archived items.
   - **Cancel**

     Click to cancel the delete operation.

Alternatives to Deleting Projects

When you delete projects, you also delete primary items stored in those projects. There may be times when this is appropriate; for example, if you create a project for testing purposes only, you may want to delete the project and all test data in that project.

In general, however, projects should rarely be deleted. Consider these alternatives for minimizing the project tree or amount of active data in your system:

- **To reduce the number of projects in the Submit tree** — For projects that users no longer need to submit items to, select the **Disallow Submissions** option on the **General** page for the projects. This removes the project from submits, but still allows users to search and report on the project.
- **To remove a project from all end-user views** — Remove all privileges assigned to roles, users, and groups.
- **To reduce the number of items in a project** — Use the Archive Wizard in SBM System Administrator to archive items in a project. You can also choose to archive change history for these items. For details, refer to the *SBM System Administrator Guide*. This feature is available to on-premise customers only.

Enabling Anonymous Submits for a Project

On-premise only.

The Anonymous Submit feature enables you to allow users who do not have SBM user accounts to submit items into selected projects. These users can only view the **Submit** form and the **Standard Fields** section on that form. They can add file and URL attachments and notes to items while they are submitting them. After they submit an item, however, they can no longer view it or any other part of SBM.

Consider the following information before implementing anonymous submits for a project:

- Anonymous submits are disabled by default and must be enabled for each project for which you want to enable this feature.
- When you enable anonymous submits for a project, a new user account is created with the user name "Anonymous Submit" and a login ID of "anonymous_submit." This user account does not appear on the **Users** page and you cannot modify the account.
- Anonymous submissions use the "Anonymous Submit" user when change history, state change history and system field values are populated. When users view change history, write notifications or report on anonymous submissions, they should look for this user name.
- Quick forms are always used for Anonymous Submits.
- If you are not using Form/URL/Cookie authentication, users must log in as "anonymous_submit."
- To use the Anonymous Submit feature with systems using NT Challenge Response or LDAP authentication, you must also enable external authentication.
- The **Submit** form for anonymous users is displayed in the system language specified in SBM System Administrator.

To enable the Anonymous Submit feature:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **Allow Anonymous Submit** option. The **URL** box populates with parameters that must be appended to the SBM URL to open the Anonymous Submit form.
3. Modify the provided URL to append it to the SBM URL. For example, if your SBM URL is: *http://serverName/tmtrack/tmtrack.dll?*, the anonymous submit URL might be *http://serverName/tmtrack/tmtrack.dll?AnonymousSubmitPage&projectid=16*.
4. Modify the Submit transition for the project and verify that all required fields are placed in the **Standard Fields** section or have default values set. If required fields are placed in other sections for the Submit transition, anonymous users cannot complete the transition.
5. Publish the URL to users who will anonymously submit items.

Enabling System Settings From the Base Project

Certain settings are available at the Base Project level. These settings control behavior for all projects in the system. Some settings apply only to the Base Project; others can be overridden for specific projects or sets of projects.

Note: Base Project settings can only be modified by system administrators or Managed Administrators who are granted the "Edit Project" privilege at the Base Project level.

The following settings can be modified only at the Base Project level:

- **Social View**

  Refer to The Social View [page 340].

- **Enable HTML5 Features**

  Refer to HTML Support Options (Base Project Only) [page 43] and Rich Text Editing [page 337].

- **Themes**

  Refer to Configuring Theme Settings [page 37].

The Item Sequence Numbering setting can be applied at the Base Project level, but overridden for child projects. For details, refer to Workflow and Sequencing Options [page 41].

Configuring Theme Settings

Themes determine the general appearance of the SBM User Workspace. A theme is a particular color scheme that applies to the templates, images, and strings that are part of the SBM User Workspace. This is a global setting applied at the Base Project, which means all users see the same theme in the SBM User Workspace.

The themes available to you depend on whether the **Enable HTML5 Features** check box is selected. "Modern" themes require HTML5, while legacy themes do not. For details on HTML5 support, refer to HTML Support Options (Base Project Only) [page 43].

The **Modern Sand** theme is used by default for new systems.

To change the appearance of the SBM User Workspace to a blue-colored theme, edit the Base Project. In the **SBM User Workspace Theme** section, select **Modern Blue**, and then click **Save**.

To revert back to the default theme, select **Modern Sand**, and then click **Save**.

Tip: You do not need to restart the Web server to change the theme. Users will see the new theme the next time they log in or when they refresh an active SBM User Workspace session. A full refresh of the browser session will display the new theme throughout SBM User Workspace.

(On-premise customers only) – You can also customize these themes or create your own theme. For more information, contact Serena Support.

Project Settings

The following sections discuss information and settings for projects.

Projects View Settings

The **Projects** view enables you to administer projects for applications for which you have privileges.

To open the **Projects** view, click the **Projects** icon on the **Administrator Portal**.

The following information and options are available on the **Projects** view:

Process Apps/Applications Pane - Use the left pane to navigate through the process apps and corresponding applications:

- Expand and collapse the nodes for each process app to view its application.
- Click the **Process Apps/Applications** link to alphabetically sort process apps. This sorting applies to the view in Application Administrator only.

- Select a process app or application to list its associated projects on the **Projects** page or workflows on the **Workflows** page.
- In the **Projects** view, select **All Projects** to list the Base Project on the **Projects** page. In the **Workflows** view, select **All Workflows** to open the Base Workflow on the **Workflows** page.

Project List

When you select a process app or an application, all parent projects you have privileges to administer that are associated with the application are listed, along with the workflow to which the project is assigned.

In addition:

- The **Project** icon () indicates that a project has sub-projects. Double-click the project row to view the project hierarchy. Use the plus sign to expand the project list to all projects assigned to the parent project.
- Click the column headers to alphabetically sort projects by name, project hierarchy, or assigned workflow. This sorting only applies to the view in Application Administrator only.
- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

For details on navigating projects, refer to Navigating Projects [page 31].

Project Toolbar

- **Add**

  Select a parent project, and then click to add projects. For details on creating a project at the root level or a sub-project, refer to Adding and Editing Projects [page 33].

- **Details**

  To edit a project, select it, and then click **Details**.

- **Delete**
  Select a project, and then click **Delete**. For details, refer to Deleting Projects [page 35].

  CAUTION:

  When you delete a project, all primary items associated with that item are also deleted, along with the change history for these items. All project settings, including user and group privilege assignments, are deleted as well. Use this feature with caution.

- **Move**

  Click to reorder projects in a particular hierarchy or to move projects to a new parent. For details, refer to Moving and Reordering Projects [page 34].

- **Refresh**

Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Project Search**

  Enter a project name or a portion of a name to return a list of projects that meet your criteria and that you have privileges to administer. Searches are case-insensitive.

General Project Settings

The following options are available on the **General** page when you add or edit a project:

- Toolbar Options [page 40]
- Project Name Options [page 40]
- Workflow and Sequencing Options [page 41]
- Item Submission Options [page 42]
- Project Form Options [page 42]
- Time Capture Options [page 42]
- Social View Option (Base Project Only) [page 43]
- HTML Support Options (Base Project Only) [page 43]
- Theme Settings (Base Project Only) [page 44]

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 open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

Project Name Options

- **Project Name**

  Indicates the project's display name. Note that sibling projects cannot have identical names.

- **Name Displayed to Users Without View Privilege**

  Indicates the name that users who do not have view privileges see for this project. For example, an organization may be working on a company proprietary proposal,

and users without view privileges should not see the actual name of the project. A different project name can be displayed to these users.

- **Internal Name**

  Indicates the unique database name automatically assigned to the project. Use this name to reference the project in scripts, Web service calls, and embedded reports based on an SBM Composer report definition that uses a primary table.

- **End-user Help Text**

  Add descriptive text that will appear to end users in Serena Work Center. For example, when users are searching for a project to submit items to, they can hover over the project name to see the information you provide here.

  Use the Rich Text Editor to apply formatting to help text.

  End-user help text is project specific and is not inherited by sub-projects.

Workflow and Sequencing Options

- **Use Parent Project's Workflow**
  If selected, this check box indicates that the project is using its parent project's workflow, which is specified in the **Workflow Name** list. The child project inherits modifications made to its parent. Clear this check box to use a different workflow for the project. In this case, the child project does not inherit any of the modifications made to its parent project.

  Note: If you clear the **Use Parent Project's Workflow** check box for a child project, all default values that are inherited from the parent project are removed. You should review all fields in the child project to ensure that default values are set as expected.

- **Use Parent Project's Sequence Numbers**

  The numbering sequence controls the *Item ID* value assigned to submitted items. For example, an item that is submitted into a project might be assigned the Item ID 00001; the next item that is submitted is assigned Item ID 00002.

  When the **Use Parent Project's Sequence Numbers** check box is selected, the sequence numbers for items in the project are assigned from a parent project. This ensures that unique IDs are assigned to all items in the parent and child projects. Clear this check box to assign a unique numbering sequence to items in the project.

- **Next Number**

  If the **Use Parent Project's Sequence Numbers** check box is cleared, use this option to assign the starting item number for the project. This is useful if you want different projects to have different starting numbers. For example, one project could start with 1000 and another project with 2000. You could then determine which project the item belongs to by its number.

- **Zero Fill to**

  Use this option to add the specified number of zeros to the beginning of an item number. Disable zero filling by entering a 1 in the **Zero Fill to** box. For best results, however, use zero filling since the item numbers are stored as strings and are sorted accordingly.

For guidance on using sequence options, refer to Frequently Asked Questions About Projects [page 79].

Item Submission Options

- **Allow New Items to be Submitted**

  If this option is selected, users can submit new items into the project.

- **Disallow Submission**

  If this option is selected, the project serves as a placeholder project and items cannot be submitted into it. You can also select this option if you want the project to be available for searching and reporting, but you do not want new items submitted into the project.

- **Allow Anonymous Submit**

  (On-premise only) - This option allows users without user accounts to submit items into the project. For details, refer to Enabling Anonymous Submits for a Project [page 36].

- **URL**

  Indicates the information that should be appended to the SBM URL for anonymous submit users. A sample final URL provided to anonymous users might be `http://serverName/tmtrack/tmtrack.dll?AnonymousSubmitPage&projectid=11`.

Project Form Options

- **Default State Form**

  Indicates the form that will be used for all states in the project, unless you override the form used for a specific state. Selections here override the default form specified for the workflow assigned to the project. Quick Form indicates that the built-in form will be used; other forms are custom forms created in SBM Composer.

- **Default Transition Form**

  Indicates the form that will be used for all transitions in the project, unless you override the form used for a specific transition. Selections here override the default form specified for the workflow assigned to the project. Quick Form indicates that the built-in form will be used; other forms are custom forms created in SBM Composer.

Time Capture Options

The Time Capture feature is enabled or disabled at various levels, but you can override inherited setting for all states and transitions in a project or set of projects. For details, refer to Time Capture [page 343].

Note: If Time Capture settings are explicitly set for a project rather than inherited, and you later change the settings to "inherited," time capture overrides set for states and transitions in that project are removed.

Project options are:

- **Time Capture**
  - **On**

Enables the Time Capture feature.

- **Off**

  Disables the Time Capture feature.

- **Inherited (On)/(Off)**

  Inherits the Time Capture settings from the system or a parent workflow or project.

- **States/Transitions**
  - **Visible**

    Displays Time Capture options on forms.

  - **Hidden**

    Hides Time Capture options on forms.

  - **Inherited (Visible/Hidden)**

    Inherits the setting from the system or a parent workflow or project.

- **Entry Required**

  With Time Capture options set to "on" and "visible" for transitions, you can choose to require users to enter time spent on an item when they execute a transition. This requirement is ignored for automated processes, such as Web services and scripts.

  - **Yes**

    Requires users to enter time spent on an item before they can complete a transition.

  - **No**

    Users are not required to enter time when they execute a transition.

  - **Inherited (Yes/No)**

    Inherits the setting from the system or a parent workflow or project.

Social View Option (Base Project Only)

You can enable or disable the **Social** view for all projects in your system at one time.

This setting is available only at the Base Project. To open the Base Project, select **All Projects** at the top of the **Process Apps/Applications** pane, select the Base Project, and then click **Details**.

To disable the **Social** view, clear the **Use Social View** check box.

To enable the **Social** view, select the **Use Social View** check box.

For details on the **Social** view, refer to The Social View [page 340].

HTML Support Options (Base Project Only)

The **Enable HTML5 Features** option enables modern HTML features, such as the Rich Text Editor, user profile card, and HTML5 form styling and layout. This option also determines which themes are available for the SBM User Workspace.

This setting impacts all projects in your system and is enabled by default. You can disable HTML5 features if you need to support legacy browsers, such as Internet Explorer 8 (IE8).

Note: For best results, users should disable Compatibility Mode in all versions of Internet Explorer when you enable HTML5 features for your system.

For details about the Rich Text Editor, refer to Rich Text Editing [page 337].

For details about HTML5 support for SBM, refer to Modern Browser Support [page 21].

Theme Settings (Base Project Only)

This option controls the theme that is used in the SBM User Workspace. The **Modern Sand** theme is selected by default.

This setting is available only at the Base Project. To open the Base Project, select **All Projects** at the top of the **Process Apps/Applications** pane, select the Base Project, and then click **Details**.

For details, refer to Configuring Theme Settings [page 37].

Fields Page Settings

The **Fields** page is available in the following areas:

- **Workflows**

  You can view all fields in a workflow and manage selections for *User*, *Multi-User*, and *Multi-Group* fields. This includes adding, deleting, and enabling or disabling selections. You can also set default values for these field types if overrides have been enabled for the field in SBM Composer.

- **Projects**

  You can override certain field properties for projects. For example, you may want a field to be required for one project but not in other projects. Changes made to fields in projects impact all states and transitions in the project and sub-projects unless you override field settings at a lower level.

- **Transitions**

  Transition fields offer great flexibility as users move items through the process. Changes made to transition fields impact that transition only, but are inherited by transitions in sub-projects unless you further override the transition field at a lower project level.

- **States**

  You can reorder fields for individual states. This reordering is inherited for states in sub-projects unless you further override the state fields at a lower project level.

Finding and Sorting Fields in the List

Fields are sorted by section by default. To navigate the fields list:

- Click the column headers to sort fields by name, type, section and attributes, such as Required and Read Only.
- Search for fields by display name.

- Filter the grid to show fields in a particular privilege section.
- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Sorting fields in the list does not impact field order on quick forms. To reorder fields on custom forms, click the **Reorder Fields** button when you are adding or editing a project.

Toolbar Options

- **Save**
  Click to save changes made to fields in the grid when you are adding or editing a project.

  Note: You are also prompted to save changes when you navigate to a different page or limit the list by searching for a field or changing the field section order that is displayed.

- **Discard**

  Click to discard changes made on the page.

- **Details**
  For default fields and transition fields, select a field in the list, and then click this button to view the field's properties or modify editable attributes.

  Note: If you are viewing the **Fields** list from a workflow, the **Details** button is only enabled when a *User*, *Multi-User*, and *Multi-Group* field is selected.

- **Reorder Fields**

  For fields in projects, click this button to override inherited field order. For details, refer to Reordering Fields [page 95].

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Show Workflow**

  Click to open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

Field List Options

The following options enable you to work with fields in the list:

- **Privilege Section**

  Filter the list of fields in the grid by selecting a privilege section from the list.

- **Search by Field Name**

  Type a field's display name in the box, and then click the **Search** icon. The grid is filtered to show fields meeting your search criteria. Searches are case-insensitive.

The field list contains the following options for default fields and transition fields:

- **Field Name**

  Each field's display name is shown.

- **Type**

  Shows the field's type, such as *Text*, *User*, or *Date/Time*.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Section**

  Indicates the section in which each field resides.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Read Only**

  Indicates that users can view but not edit the field.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Default Value**

  Displays the default value for each field. Default values can be set or overridden for most field types in projects. For workflows, you can set default values for *User*, *Multi-User*, and *Multi-Group* fields if overrides were enabled for them in SBM Composer.

  To modify a field's default value, select the field's row, and then click **Details**.

States and Transitions Page

The **States/Transitions** page lists the states and transitions defined for the workflow or project you are editing.

Note: Decisions are also listed on this page. You can view decision properties, but they should only be modified in SBM Composer.

To view the properties for individual states, decisions, and transitions and override some properties, select an item in the list, and then click **Details**.

To learn more about the state and transition settings you can modify in projects, refer to Working With States and Transitions in Projects [page 60].

To learn more about the transition settings you can modify in workflows, refer to Restricting Transitions [page 82].

Finding and Sorting Items in the List

By default, all states and decisions are listed first, followed by transitions. To sort and filter the list:

- Click the column headers to sort the list by type (states and decisions or transitions), name, origination state, destination state, status, and inheritance.
- Search for states or transitions by name.
- Filter the list to show only states and decisions or only transitions.
- Select the **Show Deleted States/Disabled Transitions** check box to include these items in the list.

Toolbar Options

- **Details**

  To edit a state, decision, or transition, select it in the list, and then click **Details**.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Show Workflow**

  Click to open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

- **Search**

  Use to search for states, decisions, or transitions by name. Searches are case-insensitive.

State and Transition Information

The following information is available:

- **Type**

  Indicates whether the item is a state (), transition (), or decision ().

- **Name**

  Indicates the display name.

- **From State**

  Indicates a transition's originating state.

- **To State**

  Indicates a transition's destination state.

- **Status**

  Indicates whether a state or decision is deleted or whether a transition is enabled or disabled.

- **Inherited From**

Indicates the workflow from which the item was inherited.

Project Role Settings

Use the **Roles** page to assign users and groups to roles for a project. All roles created for the application in SBM Composer are listed.

For guidance, refer to:

- About Roles [page 168]
- Assigning Roles for Specific Projects [page 170]

The following options are available on the **Roles** page when you are adding or editing projects:

- **Role Name**

  Shows the name provided for the role in SBM Composer.

- **Description**

  Shows the description provided for the role in SBM Composer.

- **User Assignment**

  With a role selected, click this button to assign users to the role.

- **Group Assignment**

  With a role selected, click this button to assign groups to the role.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Show Workflow**

  Click to open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

Role Assignment Page for User and Groups

Use the **Role Assignment** page to assign users and groups to roles.

This page opens when you are assigning users and groups to roles form the main **Roles** view or from the **Roles** page when you add or edit a project.

The following options are available:

- **User Assignment**

  Select this tab to assign users to the role.

- **Group Assignment**

  Select this tab to assign groups to the role.

- **Search**

If your system contains a large number of users and groups, you can search for users by login ID or name or for groups by name.

- **Enable**

  Select one or more users or groups, and then click this button to enable the role.

- **Inherit**

  Select one or more users or groups, and then click this button to apply the inherited status for the role.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **All**

  Filter the list by users or groups assigned to the role (Enabled), not assigned to the role (Disabled), or all users and groups.

  Note: You can also click the **Status** header to sort the list by users or groups who are enabled or disabled for the role.

Application Variables Page Settings

The **Application Variables** page lists the variables for the workflow assigned to the project you are editing.

By default, variables are listed alphabetically by name. You can sort the list by name, value, or description, or you can search for a variable. The value column also indicates whether the value is inherited from a parent project.

Important: Review and provide values for all application variables with an "undefined" value. Any rule referencing undefined values returns as false. This may cause unexpected results as users work with items.

For details, refer to:

- Overriding Values for Application Variables [page 78]
- Variable Value Settings [page 78]

Toolbar Options

- **Details**

  Click to view and override settings for a selected application variable.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Show Workflow**

  Click to open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

Project Mailbox View

Use the **Mailboxes** page to define mailboxes used for e-mail submission of a specific project.

To manage mailboxes for all projects, use the global mailbox feature. For details, refer to Global Mailbox View [page 439].

Mailboxes are listed alphabetically by mailbox login name, but you can click the column headers to sort by mailbox name and e-mail address.

The following options are available on the **Mailboxes** page:

- **Add**

  Click to add a mailbox for the project.

- **Details**

  Select a mailbox, and then click this button to edit the mailbox.

- **Delete**

  Select a mailbox, and then click this button to delete the mailbox.

- **Show Workflow**

  Click to open a graphical view of a workflow. When you are adding or editing a project, click this button to view the workflow assigned to the project.

"From" and "Send-to" E-mail Options

Use the options on the **Settings** tab to override system-level options for e-mail replies to messages that are sent from the Notification Server. You can also choose to remove the item link included in e-mails sent by users from their preferred e-mail client.

On-premise can set the system options in the SBM Configurator. Serena sets these options for on-demand customers.

Settings are inherited, enabling you to override them at a parent project, then set additional overrides for child projects.

Field Name	Description
From user who runs transition	Select this check box to have notification messages appear as though they are sent by the user who last transitioned the item. For example, if Bill transitions an item that generates a notification, the notification message will appear with Bill's e-mail address in the **From:** field. For escalation notifications, the message will show as **From:** the user who triggered the initial notification as well.  **Tip:** You might choose **From user who runs transition** if you want to ensure that the message's **From:** address contains the user that invoked the notification change, and not necessarily the user who made the last change to the item.

Field Name	Description
Reply to last modifier	Select this check box to automatically send reply messages to the user who last modified the item. The e-mail address of the user who last modified the item is inserted into the **Reply To:** field of the mail message header. In the **Default reply to address** field, enter an e-mail address as the default reply address for e-mail messages, which is usually the e-mail address of the person responsible for administering SBM. For best results, enter a **Default reply to address**, even if you have selected the **Reply to last modifier** check box. If a user needs to reply to a message and there is not a "last modifier" to send the reply to, the reply is then sent to this default address.
From last modifier	Select this check box to have all messages appear as though they were sent by the user who last modified the item. The e-mail address of the user who last modified the item is inserted into the **From:** field of the mail message header. In the **Default from address** field, enter an e-mail address that should appear as the default **From:** address for e-mail messages. For best results, enter a **Default from address**, even if you have selected the **From last modifier** check box.

Display name in e-mail address for notifications	Select this check box to include the user name in the **From:** field. For example:
	`From: Bill Admin <bill@serena.com>`
	If you clear this option, the **From:** field only displays the e-mail address:
	`From: bill@serena.com`

Show item link in preferred e-mail client	Clear this check box to remove the item link from messages that are sent by users from their preferred e-mail client.

SLA Settings

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.

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.

Important: SLA reports and the SLA widget only show data if projects have SLAs defined for them, and if one or more services have been associated with those projects in Serena Request Center.

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.

- **Copy**

  Click to copy a selected SLA to the current project or to a sub-project in its hierarchy. If you are copying to the same project, you must provide a unique name.

  Note: Actions and notifications defined for the SLA are not copied.

- **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 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.

- **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 54]. 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** and **User Submitter** are provided. You can also select user-defined calendars or calendars that are included in SBM.

- **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 three 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.

If you define multiple start and end states in a clause, the time an item spends in all paths is combined to calculate elapsed time. For example, suppose you have **New** and **Assigned** start states, and a **Closed** end state.

1. An item moves from the **New** to **Closed** state. The item spent two days in this path.
2. The item needs to be re-opened.
3. A manager executes the **Re-Open** transition on the **Closed** state form, and the item moves to the **Assigned** state. A technician moves the item to the **In Progress** state, and has been working on it for one day.

In the preceding scenario, the elapsed time for the item is three days, because the time since the item was re-opened is added to the previous time.

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

- **Start State(s)**

  Select the start state or states 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**(s)

  Select the end state or states 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)**

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

Qualifying Conditions

You must define at least one condition that evaluates 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. The **Actions** tab appears after you save your clauses on the SLA Clause General Options [page 54] page. 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**.
- You can use any notification e-mail tag for the item being monitored by an SLA; however, dynamic SLA-specific information cannot be included. If you want to include SLA information in an e-mail notification, create an e-mail template with static SLA information and then associate that template with the applicable action. For example, you could add "This item is at high risk of SLA violation" to an e-mail template and then select that template when you create a notification for a high-risk SLA clause.
- SLA notifications are distinct from standard notifications and are not listed in the **Notifications** view accessed directly from the Administrator Portal. Standard notifications cannot be used for SLAs.
- If a user or group is allowed to subscribe to SLA notifications, these notifications appear in the **Notifications** page when you edit the user or group and are also available for users in their user profile.
- You cannot discard SLA notifications.
- SLA notifications are distinct from standard notifications and are not listed in the **Notifications** view accessed directly from the Administrator Portal. Standard notifications cannot be used for SLAs.
- Not all notification options are available for SLAs.

About State and Transition Configuration

States represent a view of primary items as they reside at a specific point in the application workflow. States ensure the correct flow of each item through the application workflow because while an item resides in a specific state, it typically has a primary owner who is responsible for performing a specific task before the item can move on in the process. You can also set up a workflow so that one or more users are secondarily responsible for items while they reside in a particular state. For details on assigning ownership for states, refer to the *SBM Composer Guide*.

Transitions, on the other hand, move items from state to state. Most transitions are available as buttons on state forms. When users initiate a transition, they can enter data about the item before completing the transition.

In general, states provide a way to view data for items, while transitions provide a way to act on or add data to items.

Each state and transition contains a set of properties that are inherited throughout the workflow hierarchy defined in SBM Composer. This allows you to configure state properties once rather than for each workflow in the hierarchy. When you assign projects

to workflows, states and transition properties apply to that project and any further derived projects. You can modify certain state and transition properties for projects, however.

To learn more about configuring states and transitions in projects, refer to:

- Working With States and Transitions in Projects [page 60]
- State Types and Settings [page 69]
- Transition Types and Settings [page 72]

Working With States and Transitions in Projects

You can override specific state and transition properties for projects in SBM Application Administrator. These properties are inherited from the workflow defined in SBM Composer and enable you to provide unique views for individual states and transitions in projects.

For details, refer to:

- Overriding Forms for States [page 60]
- Reordering Transition Buttons on State Forms [page 61]
- Overriding Forms for Transitions [page 61]
- Overriding Transition Authentication Options [page 62]
- Overriding Post Project Settings [page 63]
- Calculating Values for Date/Time and Numeric Fields [page 64]
- Mapping Enumerations for User, Folder, and Project Fields [page 68]

Overriding Forms for States

State forms provide a view of primary items as they reside in a specific state. Quick forms are those provided by the system; all other forms are custom forms designed in SBM Composer.

Forms are assigned to states in SBM Composer, but you can override the inherited form for states in projects in SBM Application Administrator. This enables you to provide different state views for items in different projects.

Two types of overrides are available:

- **Project-level overrides** - You can override the form that will be used for all states in a project and its sub-projects.
- **State-level overrides** - You can override the form that will be used for individual states.

Overriding Forms for All States in a Project

To override a form for all states in a project and its sub-projects:

1. From the **Projects** view, select a project, and then click **Details**.
2. From the **Default State Form** list, select a form to use for all states in the project.

3. Save your changes.

Overriding a Form for a Single State

To override a form for a single state:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a state, and then click **Details**.
4. From the **State Form** list, select a form to use for the state.
5. Save your changes.

Reordering Transition Buttons on State Forms

By default, transition buttons appear on state forms in the order they were added to a workflow. In SBM Composer, you can change the order in which transition buttons appear for each state in a workflow. You can then override this order for states in projects in Application Administrator. This is useful for setting the transition buttons in the order they are most likely to be clicked by users.

To reorder transition buttons for a specific state form in a project:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a state, and then click **Details**.
4. Select the **Override Inherited Transition Order** check box.
5. Drag and drop transitions to reorder them as needed.
6. Save your changes.

Overriding Forms for Transitions

Transition forms enable users to provide new or updated data for items as they move through the process. Quick forms are those provided by the system; all other forms are custom forms designed in SBM Composer.

Forms are assigned to transitions in SBM Composer, but you can override the inherited form for transitions in projects in Application Administrator. Two types of overrides are available:

- **Project-level overrides** - You can override the form that will be used for all transitions in a project and its sub-projects.
- **Transition-level overrides** - You can override the form that will be used for individual transitions.

Overriding Forms for All Transitions in a Project

To override a form for all transitions in a project:

1. From the **Projects** view, select a project, and then click **Details**.
2. From the **Default Transition Form** list, select a form to use for all transitions in the project.
3. Save your changes.

Overriding a Form for a Single Transition

To override a form for a single transition:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a transition, and then click **Details**.
4. From the **Transition Form** list, select a form to use for the transition.
5. Save your changes.

Overriding Transition Authentication Options

You can set transitions to require that users provide their login ID and password for specific transitions. The transition will fail if users do not provide the correct login ID and password or if they attempt to provide the login ID and password of another user.

This setting can be defined for the workflow in SBM Composer, but you can override it in Application Administrator for transitions in projects.

You can also associate a *Date/Time* field to this authentication method to record the time each user performed the transition. This record is stored in the transition section of each item's **Change History** section. Consider the following information when selecting a *Date/Time* field for transition authentication:

- Consider naming the *Date/Time* field so that it is clear that is used for transition authentication. Examples include "Authentication Time" or "Electronic Signature recorded at:".
- Only custom *Date/Time* fields that are set to display the date and time or date only are available for this option.
- System fields and deleted fields cannot be used for transition authentication.
- The *Date/Time* field specified for transition authentication is always populated when the transition is executed. To prevent users from changing the date and time, consider moving the field to the **Hidden Fields** section or another section controlled by privileges. You can also set the field as read-only.
- Change history for transition authentication is not recorded on Submit, Copy, or Delete transitions.

The authentication methods used by your system impact how transition authentication options are applied. Your administrator can provide information about system

authentication methods, but you should consider the following information when setting authentication options for transitions:

- If your system uses NT Challenge/Response or Single Sign-On (SSO), passwords are checked against internal SBM passwords. Users should synchronize their SBM passwords and their network passwords, unless they choose to specify a unique password for authenticating transitions.
- If your system uses LDAP authentication, LDAP handles password verification.
- Authentication settings apply only to transitions that are executed manually by users. Automatic transitions that require authentication will fail. Use care when setting authentication options for transitions that are executed as part of actions, by e-mail submission, or by API programs.
- Smart Card users log in by selecting a certificate with their PIN rather than their SBM password. However, if SBM is configured to authenticate transitions, Smart Card users need to establish an SBM password to complete transition authentication requests.
- The password that is sent in response to the transition authentication request is not encrypted. Consider setting up SSL in Internet Information Services (IIS) to encrypt user passwords.

To override transition authentication options:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a transition, and then click **Details**.
4. In the **Authentication** area, select the **Override** check box.
5. Select the **Required** check box to require users to authenticate for this transition; clear the check box to remove this requirement.
6. From the **Date/Time Field to Update** list, select the field that will be used to record the authentication in the **Change History** section.

   Note: You are not required to select a *Date/Time* field for transition authentication, but the action is not recorded in the **Change History** section unless you do so.
7. Save your changes.

Overriding Post Project Settings

Prerequisites:

These options are only available for **Post**, **Subtask**, or **Copy** transitions that post to a primary table.

By default, the post-item project is set to **Select at Runtime** for **Post**, **Subtask**, or **Copy** transitions. This enables users to select the project to which they want to post an

item. When users execute the transition, they are presented with a list of projects into which they have privileges to submit items.

In Application Administrator, you can configure **Post**, **Subtask**, or **Copy** transitions so that posted items are submitted into a specific project. In this case, users are presented with the **Submit** form for that project when they execute the transition.

Note: Users must be granted privileges to submit items into projects before they can post to them. If you allow users to select a project at runtime, grant submit privileges to specific projects to which users can post items.

To override post project settings for Copy, Post, and Subtask transitions:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a **Post**, **Subtask**, or **Copy** transition from the list, and then click **Details**.
4. In the **Post Item Project** area, select the **Override** check box.
5. Select the **Select Project** option.
6. Select the project you want the copied or posted item to be added to from the project list. You may need to navigate to the project.

   Note: Only those projects for which users have submit privileges are available. In addition, projects must be set to allow new submits.

7. Save your changes.

Calculating Values for Date/Time and Numeric Fields

Transition field calculations provide a way to collect metrics as users move items through the process using *Date/Time* and *Numeric* fields. You can set calculations for transitions in workflows in SBM Composer, or you can configure a calculation for a transition in a project in SBM Application Administrator.

For guidance on creating calculations, refer to:

- Sample Calculation [page 66]
- Tips for Creating Calculations [page 66]
- About Operand Fields and Operator Selection Lists [page 67]

To calculate values for *Date/Time* and *Numeric* fields in transitions in projects:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **States/Transitions** tab.
3. Select a transition, and then click **Details**.
4. Select the **Fields** tab.
5. Select a *Numeric* or *Date/Time* field, and then click **Details**.
6. Select the **Allow Override** check box.

7. Select the **Set Value to Calculation** option.
8. Select one of the following options for determining when the calculation should be performed:
   - **Calculate Before Form**

     Select to perform the calculation to occur before the Transition form opens. **Calculate Before Form** is selected by default.
   - **Calculate After Form**

     Select to perform the calculation after the Transition form is submitted.
   - **Calculate Before & After Form**

     Select to perform the calculation to occur both before and after the Transition form is submitted.
9. Select the following calculation options:
   - **First Operand**

     Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], specify a constant value, field, or date/time keyword to use as the first operand in the calculation. This will be filled with the current value of the first operand. The field selected from the list cannot be the same field as the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.
   - **Operator**

     Select a valid operator for the calculation, using the guidelines and tips in Calculating Values for Date/Time and Numeric Fields [page 64].
   - **Second Operand**

     Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], enter a second constant or a valid field. Valid fields for the second operand are dependent on the field type, the first operand, and the operator. If the first operand or operator causes the second operand to be invalid, the second operator is changed to a valid constant. The second operand cannot be the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.
10. Select one of the following options for empty operand fields:
    - **Are Invalid**

      Select to require users to provide values for fields used as operands for the calculation before the transition can be completed.
    - **Skip Calculation**

      Select to allow users to complete the transition without providing values for fields used as operands for the calculation. The calculation is skipped if values are not provided.
    - **Treat as Zero**

Select to perform the calculation and treat empty values in fields used as operands for the calculation as zeros.

11. To add the calculation to the field's current value, select **Add Calculation to Current Value**. This enables you to increment the current value or to calculate the total of the calculation and the current value. This option is only available for *Numeric* fields and *Date/Time* fields set to record elapsed time.

12. Save your changes.

Sample Calculation

This example explains how to calculate how long help desk calls are in a queue before a support representative begins working the item. For this example, you would create two *Date/Time* fields with the following properties in SBM Composer:

Date/Time Field Name	Properties
Assigned To Support Rep	• **Style** – Date/Time • **Default Value** – Now • **Attributes** – Read only
Time In Assigned	• **Style** – Elapsed Time (Calculate Days and Show Seconds selected) • **Attributes** – Read only

Then, for a "Begin Work" transition that support representatives execute when they begin working on a ticket, set the calculation for the *Time In Assigned* field to:

Last State Change Date

– (minus)

Assigned to Rep

When support representatives execute the "Begin Work" transition, the amount of time that has passed before work began on the item is recorded in the *Time in Assigned* field. You can then create reports that reflect this data.

Tips for Creating Calculations

To ensure that you receive correct data from the calculation, set the field for which the calculation is set as read only and place it in the **Hidden** section.

Calculations do not work for system Date fields (Submit Date/Time, Close Date/Time, Last State Change Date, Last Modified Date) in a transition calculation for which the date will be calculated. Instead, use the "now" keyword, which gives you the same calculation.

The None operator is useful if you want to transfer the value of another field to this field during this transition.

If the calculation could result in a value that cannot be stored in the type of field, either a round or truncate version of the operator must be used. For example, if you define the calculation for a *Numeric* integer field and you want a division calculation, you must choose the round or truncating division operation. This is because the division can result in a fraction that can't be stored. With rounding operators, any fraction greater than or equal to a half will be rounded up to the next whole integer or date, while fractions less than a half are dropped. With truncating operators, the fractional part of the number is ignored. For example, seven divided by four would calculate to one with the truncating division and two with the rounding division.

About Operand Fields and Operator Selection Lists

The following table displays the valid choices for the operand fields and operator selection lists for a *Numeric* or *Date/Time* field using the calculation feature. The valid choices are based on the type of transition field being edited.

Field Type	1st Operand Constant	1st Operand Field Types	Operators	2nd Operand Constant	2nd Operand Field Types
Elapsed Time	Elapsed Time	Elapsed Time	None, +, -	Elapsed Time	Elapsed Time
Elapsed Time	Elapsed Time	Elapsed Time	*, Trunc/, Round/	Float	Numeric Int, Single Select, Summation
Elapsed Time	Elapsed Time	Elapsed Time	Trunc*, Round*, Trunc /, Round /	Float	Numeric Float
Elapsed Time	Date/ Time	Date/Time	-	Date/ Time	Date/Time, Date
Elapsed Time	N/A	Date	-	Date/ Time	Date/Time, Date
Date/ Time	Date/ Time	Date/Time	None, +, -	Elapsed Time	Elapsed Time
Date/ Time	N/A	Date	None, +	Elapsed Time	Elapsed Time, Time
Date/ Time	N/A	Date	-	Elapsed Time	Elapsed Time

Field Type	1st Operand Constant	1st Operand Field Types	Operators	2nd Operand Constant	2nd Operand Field Types
Date	Date	Date/Time, Date	None, Trunc +, Round +, Trunc -, Round –	Elapsed Time	Elapsed Time
Time	Time	Time	None, +, -	Elapsed Time	Elapsed Time
Time	N/A	Date/Time	None (assigns time portion of date/time)	N/A	N/A
Numeric Int	Int	Numeric Int, Single Select, Summation	None, +, -, *, Trunc/, (integer math), Round/	Int	Numeric Int, Single Select, Summation
Numeric Int	Int	Numeric Int, Single Select, Summation	Trunc +, Trunc -, Trunc *, Trunc /, Round +, Round -, Round *, Round /	Float	Numeric Float
Numeric Int	Float	Numeric Float	Trunc +, Trunc -, Trunc *, Trunc /, Round +, Round -, Round *, Round /	Int or Float	Numeric Int/ Float, Single Select, Summation
Numeric Float	Int or Float	Numeric Int/ Float, Single Select, Summation	None, +, -, *, /	Int or Float	Numeric Int/ Float, Single Select, Summation
Numeric Float	Int or Float	Numeric Int/ Float, Single Select, Summation	*	N/A	Elapsed Time (converted to hours)

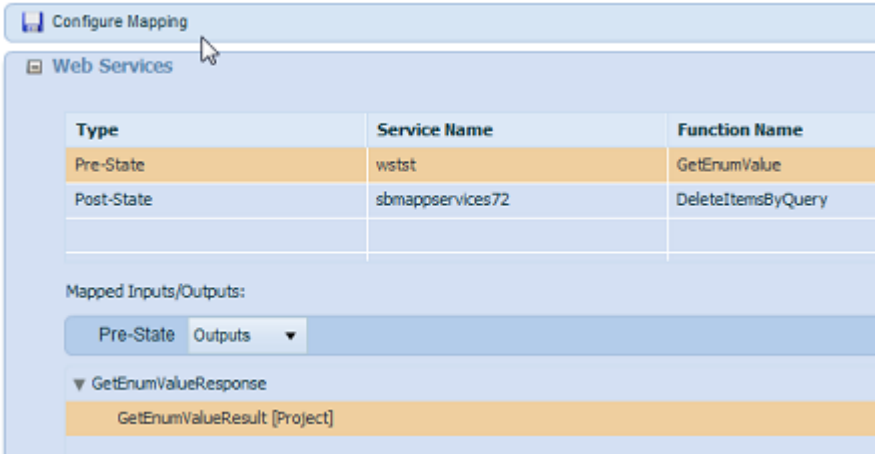
Mapping Enumerations for User, Folder, and Project Fields

Web service actions defined in SBM Composer may contain mappings between Web service enumeration types and SBM *User* and *Folder* fields and the system *Project* field. You must map values for these field types in SBM Application Administrator.

To map enumerations for *User*, *Folder*, and *Project* fields:

1. In SBM Composer, add a Web service to your application.
2. In SBM Composer, add a Web service action to a state or transition.

3. In SBM Composer, define service input and output mappings for SBM *User*, *Folder*, and the system *Project* fields as applicable.
4. Publish and deploy the process app that contains the application.
5. In SBM Application Administrator, click the **Projects** icon on the **Administrator Portal**.
6. Select the **Web Services** tab and verify that the Web service is listed.
7. Navigate to the process app that contains the Web service action, and then add or edit a project assigned to the applicable workflow.
8. Select the **States/Transitions** tab.
9. Select the state or transition that contains the Web service action, and then click **Details**.
10. Select the **Web Services** tab.
11. Select the Web service action in the top pane, and then select Inputs or Outputs from the **Mapped Inputs/Outputs** list.
12. Select the Web service enumeration that is mapped to an SBM *User* or *Folder* field or the system *Project* field, and then click **Configure Mapping**, as shown below.



13. Map enumerations to SBM values, using the information in Web Service Mapping Settings [page 300] for guidance.
14. Save your changes.

State Types and Settings

The following sections describe state types and settings:

- State Types [page 70]
- General State Settings [page 70]
- Web Services Settings for States and Transitions [page 72]

State Types

States are created in SBM Composer. All workflows contain several system states, however, that are visible in the visual workflow provided by SBM Composer and in the **From State** and **To State** columns for transitions on the **States/Transitions** page.

- **None**

  The "None" state is the state from which primary items are submitted. Also referred to as the Submit state, the "None" state cannot be a transition destination.

- **Any**

  Allows items residing in any state in the workflow move to one other state. For example, you can move items residing in any state move to the "Deferred" state.

- **Same**

  Allows items to remain in the same state after a transition is completed. This is useful for enabling users to update data in an item without moving the item to another state.

- **E-Mail**

  Represents a submit state used for e-mail submissions.

- **Deleted**

  Serves as the "To State" for "Delete" transition types. Items sent to this state are permanently deleted from the database.

General State Settings

Use the **General** page to:

- Override the form assigned to a state.
- Override the state's inherited transition order. For details, refer to Transition Ordering Settings [page 71].
- Override Time Capture options for specific states. For details, refer to Time Capture Settings [page 72].
- View general state and decision properties defined in SBM Composer.

The following information and options are available on the **General** page when you edit a state or decision.

Note: Decision properties should only be modified in SBM Composer.

General Settings

- **State Name**

  Indicates the display name for a state or decision.

- **Items in State**

  Indicates whether items residing in the state are active or inactive.

- **State Internal Name**

  Indicates the unique name assigned to the state. This name can be used to reference the state in scripts and Web service calls.

- **Owner**

  Indicates the single *User* field used to determine primary ownership for all items in the state.

- **Secondary Owner**

  Indicates the *User*, *Multi-User*, or *Multi-Group* field that establishes which users are secondarily responsible for items that reside in this state.

- **State Form**

  Indicates the form used for this state. By default, the form inherited from the workflow or project is used. You can override this default form for individuals states. Quick Form indicates that the built-in form will be used; other forms are custom forms created in SBM Composer. For details, refer to Overriding Forms for States [page 60].

- **End-user Help Text**

  Shows the description for the state or decision that was provided in SBM Composer. If provided, this information is shown to users who click **Get help for this Application** or **Get help for this Form** in items that use this workflow.

  Use the scroll bar to view long descriptions. To hide the text, collapse the **General** section.

  Note: HTML tags provided in SBM Composer are not rendered.

Transition Ordering Settings

Use the **Transition Ordering** settings to reorder transition buttons on the form for the state you are editing. For details, refer to Reordering Transition Buttons on State Forms [page 61].

- **Override Inherited Transition Order**

  Select this check box to enable the drag-and-drop capabilities so you can reorder transition buttons.

- **Transitions List**

  By default, lists the inherited order of transitions for this state. You can drag-and-drop transitions as needed.

Time Capture Settings

You can override Time Capture settings for states in a specific project as long as the Time Capture feature is enabled for the project. For example, you can hide Time Capture options on some state forms, but show them on others. For details, refer to Time Capture [page 343].

Note: If Time Capture settings are explicitly set for a project rather than inherited, and you later change the settings to "inherited," time capture overrides set for states and transitions in that project are removed.

Options are:

- **Time Capture**
  - **Visible**

    Displays Time Capture options on forms.
  - **Hidden**

    Hides Time Capture options on forms.
  - **Inherited (Visible/Hidden)**

    Inherits the setting from the system or a parent workflow or project.

Web Services Settings for States and Transitions

The **Web Services** page lists Web service actions defined in SBM Composer for states and transitions. Use this page to map Web service enumerations to values for SBM *User*, *Folder*, and the system *Project* fields.

Note: This mapping is defined in SBM Composer, but values for these SBM field types must be mapped in SBM Application Administrator.

The following options are available on the **Web Services** page:

- **Web Service Actions**

  Actions defined for the state or transition are listed, along with each action's type, the Web service name, and the function specified for the action. Select an action to map values for it.
- **Mapped Inputs/Outputs**
  From the drop-down list, select Inputs or Outputs as applicable, and then select the enumeration mapped to an SBM *User*, *Folder*, and the system *Project* field. An example of a mapped enumeration is:

  multiOption [Project]
- **Configure Mapping**

  With a mapped enumeration selected, click the **Configure Mapping** button. For details, refer to Web Service Mapping Settings [page 300].

Transition Types and Settings

The following sections describe transition types and settings:

- Transition Types [page 73]

- General Transition Settings [page 73]

Transition Types

SBM provides a variety of transition types that serve different purposes and provide unique functionality. Regular transitions are the simplest and most common type of transition because they move items from one state to another.

Other transition types allow users to copy primary items from one project to another, "post" items from projects in one table to projects in another, and to create subtasks from a principal primary item. These transition types include:

- **Post**

  Enables users to submit into a different project a new item from the item with which they are currently working. The posted item receives a new Item ID and follows the workflow of the project it is posted into.

- **Copy**

  Enables users to copy items into the same or a different project within the same application.

- **Subtask**

  Enables users to create an item that is associated with a principal task. Subtasks are typically used when a set of smaller tasks need to be worked on before a larger task, or principal task, can continue its progress in the application workflow.

- **Update**

  Enables users to update data in an item at a particular state in the workflow. The item does not move to another state, but data can be updated.

- **Delete**

  Enables users with correct privileges to delete an item at a particular state in the workflow.

- **Publish**

  (On-premise only.) Enables users to quickly publish problems and resolutions pertaining to primary items to the SBM Knowledge Base.

- **External Post**

  (On-premise only.) - Used for cross-database posting, which enables users to post items from one SBM database to another. For details, refer to *SBM System Administrator Guide*.

For details on using the various transition types, refer to the *SBM Composer Guide*.

General Transition Settings

Use the **General** page to override:

- The form assigned to the transition. For details, refer to Overriding a Form for a Single Transition [page 62].

- Authentication settings. For details, refer to Overriding Transition Authentication Options [page 62].
- Post project settings for **Post**, **Subtask**, and **Copy** transitions. For details, refer to Overriding Post Project Settings [page 63].
- Time Capture settings for transitions in projects. For details, refer to Time Capture Settings [page 76].

You can also view general transition properties defined in SBM Composer.

The following information and options are available on the **General** page when you edit a transition.

General Settings

The following options are available for all transition types.

- **Transition Name**

  Indicates the transition's display name.

- **From State**

  Indicates the transition's originating state or decision.

- **To State**

  Indicates the transition's destination state or decision.

- **Transition Internal Name**

  Indicates the unique database name assigned to the transition. Use this name to reference the transition in scripts and Web service calls.

- **Transition Type**

  Indicates the transition's type. Quick transitions, which enable users to bypass forms, are also noted. For details, refer to Transition Types [page 73].

- **Status**

  Indicates whether the transition is enabled or disabled for the project. Transition status is always inherited from the workflow.

- **Form**

  Indicates the form used for this transition. By default, the form inherited from the workflow or project is used. You can override this default form for individual transitions. Quick Form indicates that the built-in form will be used; other forms are custom forms created in SBM Composer. For details, refer to Overriding Forms for Transitions [page 61].

- **Required Attachment**

  Indicates whether an attachment is required to complete the transition. The type of attachment is also specified.

- **End-user Help Text**

Shows the description for the transition that was provided in SBM Composer. If provided, this information is shown to users who click **Get help for this Application** or **Get help for this Form** on items that use this workflow.

Use the scroll bar to view long descriptions. To hide the text, collapse the **General** section.

Note: HTML tags provided in SBM Composer are not rendered.

- **Submit of Behalf Another User**

  (**Submit** transitions only) – Enables you to inherit, enable, or disable the **Allow submit on behalf of another user** transition option found in SBM Composer. The options are:

  - **Inherited (On/Off)** – Inherits the parent workflow setting (either enabled or disabled).
  - **On** – Enables **Allow submit on behalf of another user** for this **Submit** transition.
  - **Off** – Disables **Allow submit on behalf of another user** for this **Submit** transition.

  Tip: You can enable users to submit on behalf of other users at the project level in SBM Application Administrator; however, you must add the *Submitting Agent* field to your primary table and deploy your process app first.

- **Update Submitter**

  (Regular transitions only) – Enables you to inherit, enable, or disable the **Update Submitter** option found in SBM Composer. The options are:

  - **Inherited (On/Off)** – Inherits the parent workflow setting (either enabled or disabled).
  - **On** – Enables **Update Submitter** for this transition.
  - **Off** – Disables **Update Submitter** for this transition.

Authentication Settings

Use these options to override authentication settings applied for the transition in SBM Composer. Transitions that require authentication prompt users to enter their login ID and password before they can complete the transition. If you specify a *Date/Time* field, the authentication option is recorded in the **Change History** section. For details on configuring transition authentication, refer to Overriding Transition Authentication Options [page 62].

The following options are available in Application Administrator:

- **Override**

  Select this check box to override authentication settings set in SBM Composer.

- **Required**

Select this check box to require users to provide a login ID and password before they can complete the transition.

- **Date/Time Field to Update**

  Select a *Date/Time* field used to record the action in the **Change History** section. You can choose from *Date/Time* fields set to display date and time or date only.

Post Item Settings

By default, the post project for Copy, Post, and Subtask transitions is set to "Select at Runtime." This enables users to select a project to submit a new item created by the post, copy, or subtask action. You can override this setting, however, to open a **Submit** form for a specific project submit when users execute a transition of one of these types.

For details, refer to Overriding Post Project Settings [page 63].

The following Post options are available in Application Administrator:

- **Post Item Table**

  Indicates the table to which items will be posted or copied. If the transition posts to an auxiliary table, the **Post Item Project** options are disabled.

- **Item Link Type**

  Indicates the type of item links specified for the transition in SBM Composer.

- **Override**

  Select this check box to override the post settings specified in SBM Composer.

- **Select at Runtime**

  Select this option to enable users to select from an applicable list of projects to post or copy items.

- **Select Project**

  Select this option to open a **Submit** form for the project selected in the project list. You may need to expand the project list to include projects that allow submits before this option is enabled.

- **Project List**

  With the **Select Project** option selected, you can select a project from the list. You may need to expand the list to find the project you need.

External Post Database Settings

Applicable to **External Post** transitions only, this setting indicates the external database to which items are posted when this transition is executed. For details, refer to the *Configuring Cross-database Posting* section of the *SBM System Administrator Guide*.

Time Capture Settings

You can override Time Capture settings for transitions in a specific project as long as the Time Capture feature is enabled for the project. For example, Time Capture may be turned on for a project, but required for a specific transition. For details, refer to Time Capture [page 343].

Time Capture options cannot be enabled for submit transitions.

Note: If Time Capture settings are explicitly set for a project rather than inherited, and you later change the settings to "inherited," time capture overrides set for states and transitions in that project are removed.

Options are:

- **Time Capture**
  - **Visible**

    Displays Time Capture options on forms.
  - **Hidden**

    Hides Time Capture options on forms.
  - **Inherited (Visible/Hidden)**

    Inherits the setting from the system or a parent workflow or project.
- **Entry Required**

  With Time Capture options set to "on" and "visible" for transitions, you can choose to require users to enter time spent on an item when they execute a transition. This requirement is ignored for automated processes, such as Web services and scripts.
  - **Yes**

    Requires users to enter time spent on an item before they can complete a transition.
  - **No**

    Users are not required to enter time when they execute a transition.
  - **Inherited (Yes/No)**

    Inherits the setting from the system or a parent workflow or project.

About Application Variables

Use application variables to override values specified for rules defined in SBM Composer. Rules and application variables are used together to dynamically route items and restrict transitions.

Application variables are optional, but if they are set for rules, you can override the values for individual projects assigned to a workflow.

For example, you may have a decision that sends items to an executive for approval if the value in a *Cost* field exceeds $10,000; otherwise, the item is sent to a manager for approval. For a Hardware Requests project, however, you may want an executive to approve items costing more than $5,000. In this case, you can override the variable value for the *Cost* field in the Hardware Requests project, leaving the variable value at $10,000 for all other projects assigned to the workflow.

Overriding Values for Application Variables

Prerequisites:

Application variables are only available in Application Administrator if they have been defined in SBM Composer for the workflow assigned to the project you are managing.

Override the application variable values for individual projects assigned to the workflow. This enables you to tailor rules based on business needs for various projects. For example, items in one project may need to move to a Review state based on one date; items in a second project may move to the Review state based on a different date.

To override values for application variables:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **Variables** tab.
3. Select a variable in the list, and then click **Details**.

   Important: Review and provide values for all application variables with an "undefined" value. Any rule referencing undefined values return as false. This may cause unexpected results as users work with items.
4. Provide a new value for the variable. Options for providing new values depend on the field type used by the variable.
5. Save your changes.

Variable Value Settings

- **General Settings**

  The following information is provided for application variables in SBM Composer and cannot be changed in Application Administrator.

  - **Variable Name**

    Indicates the name given to the variable in SBM Composer.

  - **Variable Description**

    Indicates the description provided for the variable in SBM Composer.

  - **Field Type**

    Indicates the field type on which the variable is based.

- **Field Value Settings**

  You can modify the inherited values for application variables as follows:

  - **Inherits Value From/Overrides Value From**

    Indicates the project from which the variable value is inherited or overridden.

  - **Value**

    Indicates the current value for the variable.

- **Allow Override**

  Select this check box to override the value provided for the variable in SBM Composer or for a parent project.

- **Field Values**

  Depending on the type of field used in the application variable, options vary for providing overridden values.

Frequently Asked Questions About Projects

- **When should I override workflow settings in my projects?**

  For maintenance purposes, project overrides to workflows should be kept to a minimum. Overrides can be beneficial, however, when all of your projects are assigned to a single workflow. This enables you to establish a solid process that you can tailor as needed.

- **How do I set unique Item IDs?**
  You can use the sequence options on the **General** tab to set the numbering options for items in projects. Options are:

  - **Unique Item IDs for your entire system**

    Select the **Use Parent Project's Sequence Number** for all projects in your system. This ensures that number sequencing is inherited from the Base Project and that all Item IDs will be unique.

  - **Unique Item IDs for a set of projects**

    Clear the **Use Parent Project's Sequence Number** check box for a parent project, but select it for child projects. This ensures unique IDs for the parent and child projects.

  - **Different Item IDs for all projects**

    While some level of unique Item IDs optimizes SBM's reporting and search capabilities, you can set different numbering sequences for each project if this meets your organization's needs. To do so, clear the **Use Parent Project's Sequence Number** check box for each project, including child projects.

  For each option described, you can define the starting number for item IDs and set the number of filled zeros. For details, refer to Workflow and Sequencing Options [page 41].

- **How can I prevent users from submitting items into a project?**

  You have two options:

  - Select the **Disallow Submits** option on the **General** page when you add or edit a project. This keeps the project available for searching and reporting, but prevents new items from being added to the project.

  - Remove the "Submit New Items" privilege for roles, users, and groups for a particular project. This also enables you to allow some users to submit new items, but not others.

- **How can I limit the list of projects users see without deleting the projects?**

  You have two options:

  - To reduce the number of projects in the Submit tree, select the **Disallow Submissions** option on the **General** page for the projects.
  - To remove a project from all end-user views, remove all project privileges assigned to roles, users, and groups. The removes the project from the Submit tree, search features, and reports.

Chapter 3: Managing Workflows

The following topics describe how to manage workflows in SBM Application Administrator.

About Workflows

Workflows define the process followed by items in projects. Each project is assigned a workflow, but a workflow can be assigned to multiple projects.

Workflows are defined in SBM Composer and are available in Application Administrator after a process app is deployed. Refer to Working with Workflows [page 81] for the workflow tasks you can perform in Application Administrator.

The Workflow Hierarchy and the Base Workflow

Workflows are organized in a hierarchy, similar to the project hierarchy. The Base Workflow always exists at the top of the workflow hierarchy. It is a header workflow and cannot be modified, but you can use it to navigate the entire hierarchy of workflows you have privileges to manage. To see the Base Workflow, select **All Workflows** in the **Process Apps/Applications** pane.

Working with Workflows

Most workflow settings and properties cannot be modified in Application Administrator, but you can:

- Add and delete selections for *User*, *Multi-User*, and *Multi-Group* fields. For details, refer to Adding User and Group Values [page 81].
- Enable and disable selections for *User*, *Multi-User*, and *Multi-Group* fields. For details, refer to Enabling and Disabling Selection Field Values [page 97].
- Set default values for *User*, *Multi-User*, and *Multi-Group* fields if overrides have been enabled for individual fields in SBM Composer. For details, refer to Setting Default Values for User-type Fields [page 96].
- Apply group restrictions to transitions and view role and item restrictions applied to transitions in SBM Composer. For details, refer to Restricting Transitions [page 82].

Adding User and Group Values

If you do not use roles to populate values for *User*, *Multi-User*, and *Multi-Group* fields, you can add users and groups as values for these fields. Selections for these field types are added to workflows so they are available for all projects assigned to a workflow. If

selections are not needed for all projects, you can disable them for specific projects or in sub-workflows.

Tip: For best results, add selections at the highest workflow level, and then disable and enable selections for sub-workflows and projects as needed.

For guidance on adding values to user-type fields, Values for User, Multi-User, and Multi-Group Fields [page 92].

1. From the **Administrator Portal**, click the **Workflows** icon.
2. Search for or navigate to the workflow you need, and then click **Details**.
3. Select **Default Fields**.
4. Search for or navigate to a *User*, *Multi-User*, or *Multi-Group* field.
5. Select the field, and then click **Details**.
6. On the **Attributes** tab, select:
   - **Manage User Selections** to add user values.
   - **Manage Group Selections** to add group values.
7. On the dialog box that opens, select values in the **Available** column, and then drag the values or click the arrow to move them to the **Selected** column.

   Tip: To find users across pages, search for them by name or login ID or use the navigation buttons at the bottom of the page.
8. Save your changes.

Restricting Transitions

SBM offers several mechanisms for restricting the transitions that are available to users.

Restricting Transitions for All Items

Privileges enable you to restrict transitions for all items in a project. You can grant or remove transition privileges for roles in SBM Composer or for individual users and groups in Application Administrator.

The following privileges are available for controlling transitions for all items in a project, depending on a user's product-access type:

- Transition All Items
- Transition Item if Owner
- Transition Item if Secondary Owner
- Transition Item if Submitter

In Application Administrator, transition privileges are located on the **Item** privileges page when you are working with users and groups.

Restricting Individual Transitions

In some cases, you may need to limit individual transitions that are available to users. For example, you may want to restrict an "Approved" transition to users with a Manager role. In this case, users with the "Transition All Items" privilege would not see the "Approved" transition unless they are assigned to the Manager role.

The following restriction types are defined in SBM Composer and are the best method for restricting individual transitions:

- **Role Restrictions**

  Transitions are not available to users assigned to restricted roles.

- **Rule Restrictions**

  Transitions are not available based on business rules, such as removing an "Escalate to Management" transition for low-priority items.

- **Item Type Restrictions**

  Transitions are not available based on item types. For example, you can restrict a "Send to Software Team" transition for items with a "Hardware Requests" item type.

Restricting Transitions for Groups

In SBM Application Administrator, you can restrict transitions so they are unavailable for members of specific groups. *(On-premise only.)*

Before you use this feature, consider the following:

- Group restrictions applied on the **Restrictions** page apply to all projects assigned to a particular workflow. You must have administrative privileges to edit the workflow to restrict transitions for groups.
- If role restrictions were specified for a transition in SBM Composer, the transition will be restricted to users assigned to the roles and groups selected on the **Restrictions** page.
- Transition restrictions are not allowed on Submit, Update, or Delete transitions, or transitions used on the Otherwise branch from a decision.
- A transition in a sub-workflow inherits the group restrictions set for the transition in the parent workflow. Group restrictions cannot be overridden, so the following steps must be performed if you need different group restrictions for the sub-workflow transition:

  1. In SBM Composer, disable the transition in the sub-workflow.
  2. Replace the disabled transition with a new transition.
  3. Redeploy the process app.
  4. In SBM Application Administrator, set the group restrictions for the new transition.

To restrict transitions for group members:

1. From the **Administrator Portal**, click the **Workflows** icon.

2. Search for or navigate to the workflow you need, and then click **Details**.
3. Select the **States/Transitions** tab.
4. Select a transition, and then click **Details**.
5. Select **Restrictions**.
6. In the **Groups** section, search for or navigate to groups in the **Groups You Can Manage** section.
7. Select one or more groups, and then click the right arrow to move them to the **Selected Groups** section.
8. Save your changes.

Workflow Settings

The following sections discuss information and settings for workflows:

- Workflows View Settings [page 84]
- General Workflow Settings [page 85]
- Transition Restriction Settings [page 86]
- Social View Settings [page 87]

Workflows View Settings

To open the **Workflows** view, click the **Workflows** icon on the **Administrator Portal**.

The following information and options are available on the **Workflows** view:

Process Apps/Applications Pane - Use the left pane to navigate through the process apps and corresponding applications:

- Expand and collapse the nodes for each process app to view its application.
- Click the **Process Apps/Applications** link to alphabetically sort process apps. This sorting applies to the view in Application Administrator only.
- Select a process app or application to list its associated projects on the **Projects** page or workflows on the **Workflows** page.
- In the **Projects** view, select **All Projects** to list the Base Project on the **Projects** page. In the **Workflows** view, select **All Workflows** to open the Base Workflow on the **Workflows** page.

Workflow List

When you select a process app or an application, all of its parent workflows that you have privileges to administer are listed, along with the workflow's application.

In addition:

- The **Parent** icon ()indicates that a workflow has sub-workflows. Double-click the workflow row to expand the workflow hierarchy.

- A "double dot" symbol (..) before a workflow name indicates that the workflows below it are sub-workflows.
- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Workflow Toolbar

- **Details**

  To edit a workflow, select it, and then click **Details**.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Workflow Search**

  Enter a workflow name or a portion of a name to return a list of workflows that meet your criteria and that you have privileges to administer. Searches are case-insensitive.

General Workflow Settings

The following workflow settings are specified in SBM Composer and cannot be modified in SBM Application Administrator.

Workflow Name Settings

- **Workflow Name**

  Indicates the name of the workflow. The primary table determines the fields that are available in the workflow.

- **Primary Table**

  Indicates the primary table on which the workflow is based.

- **End-user Help Text**

  The text entered here is shown to users who click **Get help for this Application** on items that use this workflow.

  Use the scroll bar to view long descriptions. To hide the text, collapse the **General** section.

  Note: HTML tags provided in SBM Composer are not rendered.

Workflow Form Settings

- **Default State Form**

  Indicates the form specified for all states in the workflow.

- **Default Transition Form**

  Indicates the form specified for all transitions in the workflow.

Time Capture Settings

Time Capture options are available when you are editing the Base Workflow. When you set these options, they apply to your entire system, but you can override the system setting at various levels. By default, the Time Capture feature is disabled. For details, refer to Time Capture [page 343].

The following options are available for the Base Workflow:

- **Time Capture**
  - **On**

    Enables the Time Capture feature.
  - **Off**

    Disables the Time Capture feature.
- **States**
  - **Visible**

    Displays Time Capture options on forms.
  - **Hidden**

    Hides Time Capture options on forms.
- **Transitions**
  - **Visible**

    Displays Time Capture options on forms.
  - **Hidden**

    Hides Time Capture options on forms.
- **Entry Required**

  With Time Capture options set to "on" and "visible" for transitions, you can choose to require users to enter time spent on an item when they execute a transition. This requirement is ignored for automated processes, such as Web services and scripts.
  - **Yes**

    Requires users to enter time spent on an item before they can complete a transition.
  - **No**

    Users are not required to enter time when they execute a transition.

Transition Restriction Settings

SBM offers several mechanisms for restricting the transitions that are available to users.

Use the **Restrictions** page to:

- View role restrictions applied to a transition in SBM Composer.
- View Item Type restrictions applied to a transition in SBM Composer.

- Apply group restrictions to a transition. For details, refer to Restricting Transitions [page 82].

Note: The **Restrictions** page is only available to on-premise customers in SBM Application Administrator. On-demand customers can set role and Item Type restrictions in SBM Composer, however.

Social View Settings

Use the **Social View** tab to select the notifications that are sent to users who "follow" items. If you do not select at least one notification for a workflow, the "Follow" feature is disabled for all projects assigned to the workflow.

For details, refer to Enabling the "Follow" Feature [page 342].

Chapter 4: Configuring Fields

The following topics describe how to configure fields in SBM Application Administrator.

About Field Configuration

Data collection is the cornerstone of many applications, which depend on accurate and complete data. Compiling relevant historical data into management reports also depends on effective data collection.

Fields are used to collect data as users submit, transition, and update primary items and work with auxiliary items. SBM provides many types of fields, most of which have sets of properties that define the behavior of the fields. These fields can be customized to meet the data collection requirements of your applications.

Fields are defined in SBM Composer. For primary tables, these fields are inherited throughout the workflow hierarchy. When a workflow is assigned to a project in SBM Application Administrator, the project inherits the fields, ordering, and field properties from the assigned workflow. These properties define how the field looks and acts to users, as well as how the fields are ordered when quick forms are used.

In Application Administrator, you can override many of these settings for projects and transitions in projects. You can also define user and group selections for certain field types in workflows. For auxiliary tables, you may need to configure some fields in SBM System Administrator.

Key Benefits

- Enables customization of fields in projects to meet varied business needs.
- Provides a mechanism for configuring design elements, such as *User* fields.

To learn more about fields, refer to:

About Field Organization

Field sections are provided for organizing fields on state and transition forms. Organizing fields in sections provides a way to group fields for display, as well as to limit user accessibility to certain fields. When quick forms are used, field sections are used to control security and field layout. When custom forms are used, field sections are used to control security only.

In SBM Composer, you assign fields to privilege sections when you create them in tables. You can also override privilege sections for each field for workflows, states, and transitions. These settings apply to quick forms and custom forms.

In Application Administrator, you can override inherited field order fields for projects and for individual states and transitions.

There are three ways to control access to fields in sections:

- **Roles**

  Grant field section privileges to roles in your application in SBM Composer.

- **Groups**

  Grant privileges to field sections for your application to groups in Application Administrator.

- **Users**

  Grant privileges to field sections for application users in Application Administrator.

Tip: You may want to restrict access to the *Owner*, *Secondary Owner*, *Project,* and *State* fields from most users. These fields are generally handled automatically by the system; therefore, most users should not have access to change the field values. There may be situations, however, where a manager or administrator might want to manually change the values in these fields.

For details on changing field order, refer to Reordering Fields [page 95].

Provided Field Sections

Provided field sections enable you to control access to fields through role-based privileges and user and group privileges.

Note: On-premise customers can change the names of all field sections in your system on the **Labels** tab in the **Settings** dialog box in the SBM System Administrator. Field section names can also be changed for each primary or auxiliary table in SBM Composer. These custom field section labels appear on forms.

The following set of field sections are provided:

- **Standard Fields**
  The fields contained in this section are always visible to users who have privileges to submit, view, update, or transition items for a particular project. On quick forms, the **Standard Fields** section and set of fields are displayed at the top of each form.

  Tip: Place required fields in this section to ensure users can provide values as they work with items.

- **User Fields**
- **Advanced Fields**
- **Manager Fields**
- **System Fields**

Use this section to store fields that are visible to users with privileges to fields in this section. Typically, this section is used to store fields that are automatically populated by the system, such as the *Owner* or *State* fields. You can then limit access to this section so that users cannot inadvertently change your process.

- **Hidden Fields**

  Provides a place to store fields that you may not want users to view or update for a particular workflow, state, transition, or project.

- **Not Used Field Section**

  Provides a place to store fields that are not used in a particular workflow or auxiliary table. Fields placed in this section for tables or workflows are not available for modifications for projects, states, or transitions.

- **Deleted Field Section**
  This field section contains fields that have been deleted, allowing you to restore them at any time using SBM Composer. For example, you can reuse deleted fields by restoring them and then renaming them and resetting properties. Reusing deleted fields helps with database table field limits.

  Note: The **Not Used** and **Deleted** field sections are not visible in Application Administrator.

About Selection Field Values

SBM offers many different field types for gathering information about primary and auxiliary items in your system. Many "selection" field types are available, with each type offering flexibility to users as they work with items. *User*, *Single Selection*, *Multi-Selection*, and *Single Relational* fields are examples of selection-type fields.

Values for selection fields are added in different interfaces, depending on the field type. Refer to the online help in each interface for detail information on setting selection and default values for fields.

Add values for the following field types in SBM Composer:

- Single Selection
- Multi-Selection
- Binary/Trinary

Add values for the following field types for primary items in SBM Application Administrator. For auxiliary items, add values for these field types in SBM System Administrator.

- User
- Multi-User
- Multi-Group
- Folder

Note: You can add roles as values for *User*, *Multi-User*, and *Multi-Group* fields in SBM Composer. User and group selections are added in Application Administrator. For guidance, refer to Values for User, Multi-User, and Multi-Group Fields [page 92].

Add values for the following field types in auxiliary tables using the Auxiliary Data feature in SBM Application Administrator:

- Single Relational
- Multi-Relational

Values for User, Multi-User, and Multi-Group Fields

SBM offers several options for adding values to user-type fields (*User*, *Multi-User*, and *Multi-Group* fields). Depending on the field type, roles, groups, and users can be used to populate value lists.

The following options are available for adding values to *User*, *Multi-User*, and *Multi-Group* fields:

- **Roles**

  Associate roles with the fields in SBM Composer, and then assign users or groups to the role in Application Administrator.

- **Groups and Users**

  Add users and groups as values for default fields in workflows in Application Administrator. Refer to Adding User and Group Values [page 81].

The following sections explain the various value options for user-type fields:

Values Derived From User Accounts

You can assign individual users to *User* and *Multi-User* fields in Application Administrator, but this should only be done in cases where one or two individuals will be needed as values for the field. The best practice is to assign roles or groups to these fields. This eases maintenance over time, since the field values will be based on role assignments or group membership rather than by manually editing fields as users change in your system.

Values Derived From Groups

Groups are assigned to user-type fields in Application Administrator. Group values appear as [Members of: *Group Name*] in the **Values** list on the **Attributes** page.

When you add groups as selections, they become available for you to set as default values in Application Administrator, and for users to select as values, as follows:

- **User Fields**

  A list of users assigned to the groups is available.

- **Multi-User**

  The list of values will contain users or users and groups, depending on the selection mode specified in SBM Composer.

- **Multi-Group Fields**

  A list of groups is available.

Current User Value

Current User is available as a default value for *User* and *Multi-User* fields. This automatically sets the value for a field as the user performing an update or transition. For *Multi-User* fields, the user performing the update or transition can be one of the values.

The following considerations apply to the Current User default value:

- Users who are valid Current User selections must be added to the field's selection list. If the user updating or transitioning an item is not included in the selection list, the field is set as required and the user's name is labeled as disabled. The user performing the update or transition must select a valid user selection.

- Take special care when you use the Current User setting for fields that determine ownership. If you select Current User as the default value for a *Multi-User* field used for the secondary ownership property for a state, the user transitioning items to this state must have ownership privileges. If not, the field is set as required and even though the selection looks valid, users are warned that they must pick a user with correct privileges.

Values Derived From Roles

Roles are assigned to user-type fields in SBM Composer. When you edit the field in Application Administrator, these values appear as [Acting As: *Role Name*] in the **Values** list on the **Attributes** page.

Note: You cannot disable role values for user-type fields in Application Administrator. You must remove the role association from the field in SBM Composer.

When you assign users or groups to roles, they become available for you to set as default values in Application Administrator, and for users to select as values, as follows:

- **User and Multi-User Fields**

  A list of user names is available. The list includes individual users assigned to the role in Application Administrator, as well as users who are members of groups assigned to the role.

- **Multi-Group Fields**

A list of group names is available. Users can select one or more groups.

Working With Fields

Most field properties are defined in SBM Composer and those properties are inherited from workflows and parent projects. You can, however, override certain field properties:

- **Project Field Overrides (Projects)**

  Changes made to default fields apply to the project and all sub-projects, unless you further override properties for a sub-project or a transition in a project.

- **Transition Field Overrides**

  Changes made to fields for a specific transition apply to the transition for the project and all sub-projects, unless you further override the transition field in a sub-project.

- **Workflow Field Overrides**

  Set default values for *User*, *Multi-User*, and *Multi-Group* fields, if overrides were enabled for the fields in SBM Composer. These values can then be overridden in sub-workflows and projects. For details, refer to Setting Default Values for User-type Fields [page 96].

For default fields and transition fields in projects, you can:

- Move fields to a different section or reorder them in an existing section. For details, refer to Reordering Fields [page 95].
- Override common field attributes. For details, refer to Overriding Common Field Attributes [page 94].
- Override default values.
- Override display options (except *Binary/Trinary*, *Date/Time, Numeric,* and *Text* fields). For details, refer to Overriding Display Options for Selection Fields [page 98].

For default fields in projects only, you can:

- Set dependent *User*, *Multi-User*, or *Multi-Group* field selections for independent *User* fields. For details, refer to Configuring User Field Dependencies [page 102].
- Override dependent field selections for independent *Single Selection* fields. For details, refer to Overriding Dependent Selections for Single Selection Fields in Projects [page 101].

For transition fields only, you can override calculations for *Date/Time* and *Numeric* fields. For details, refer to Calculating Values for Date/Time and Numeric Fields [page 64].

Overriding Common Field Attributes

You can quickly override common attributes for multiple default fields in projects or for transition fields. These attributes are:

- Read Only
- Required

- Allow Mass Update

Tip: You can also view all properties for individual fields and override allowable attributes for each field by selecting a field in the list, and then clicking **Details**.

To override common attributes for fields:

1. From the **Projects** view, select a project, and then click **Details**.
2. Do one of the following:
   - To override fields for all transitions in a project, select **Default Fields**.
   - To override fields for a specific transition, select the **States/Transitions** tab, edit a transition, and then select **Fields**.

   The list of fields opens in the **Fields** page. Fields are initially sorted by section.
3. Select or clear the **Read Only**, **Required**, and **Allow Mass Update** for each field as needed.

   Note: When you select or clear an attribute for a field, the **Allow Override** check box is automatically selected.
4. Use the arrows at the bottom of the page to navigate to more fields, or search for specific fields to override.
5. Save your changes.

Reordering Fields

Projects inherit default field ordering and user access from their assigned workflows. You can override default field ordering and user access for specific projects, states, and transitions, however.

If a quick form is specified on the for the project, state, or transition, field ordering you apply on the **Fields** page controls the order of fields on the form and user access to those fields. If a custom form is specified, field ordering controls user access to fields.

For details on organizing fields, refer to About Field Organization [page 89].

To reorder fields:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select one of the following:
   - To reorder fields for all states and transitions in a project, select the **Default Fields** tab.
   - To reorder fields for a specific state or transition, select the **States/Transitions** tab, select a state or transition and click **Details**, and then select the **Fields** tab.
3. Click **Reorder Fields**. The **Reorder Fields** dialog box opens.
4. Select the **Override Inherited Field Order** check box.
5. To move fields to a different section:

a. To move a single field, search for and select the field you want to move. To move multiple fields, double-click a field section to expand it, and then select the fields you want to move.

b. Drag the fields from the source section on the left to the destination section on the right. If needed, you can double-click the destination field section to view the existing fields in that section.

6. To reorder fields in a section:
   a. Expand the destination field section for which you want to reorder fields.
   b. Drag and drop fields to reorder them.
7. Close the dialog box to save your changes.

Tip: Click **Undo** to discard your changes if necessary.

Setting Default Values for User-type Fields

After you define selections for *User*, *Multi-User*, and *Multi-Group* fields following the instructions in Adding User and Group Values [page 81], you can specify default values for these fields types by setting them for:

- A workflow so they are available for all projects assigned to the workflow and for sub-workflows.
- Specific projects. For example, you may want to select a manager as a default value for a *User* field for one project, but a different manager as a default value for other projects.
- Specific transitions in projects. For example, you may want to select an IT technician as the default value for a user field for a project, but a manager as the default value for the field for an "Escalate" transition.

Note: Before you can set default values for fields in workflows, the **Override field properties** check box must be selected for the field on the **Field Overrides** tab for the workflow in SBM Composer.

To set default values for *User*, *Multi-User*, and *Multi-Group* fields:

1. Do one of the following:
   - To set a default value for the field for all transitions in a workflow or project, select the **Default Fields** tab.
   - To set a default value for a field for a specific transition in a project, select the **States/Transitions** tab, select a transition, click **Details**, and then select the **Fields** tab.
2. Search for or navigate to a *User*, *Multi-User*, or *Multi-Group* field.
3. Select the field, and then click **Details**.
4. If you are editing a default field, select the **Attributes** tab.

5. Select **Manage User/Group Defaults**. Selections available as default values are listed in the left pane.
6. Select values in the left pane, and then click the right arrow. You may need to search or navigate through the list to find valid values.

   Note: For *User* fields, you can only add a single default value. You can also select "Current User" to set the default value to the user performing an update or transition.
7. Save your changes.

Enabling and Disabling Selection Field Values

You can enable and disable values for certain selection fields, such as *Single Selection* for projects. Selections for *User*, *Multi-User*, and *Multi-Group* fields can be enabled or disabled for workflows or projects.

This allows you to tailor the list of values users can select, depending on the project they are using.

For example, you may want to limit the values in the *Item Type* field, which is a *Single Selection* field, so that users can select only defects and enhancements for a hardware development project. For a software development project, however, users may need to select defects, enhancements, and change requests. You would add all of these selections to the *Item Type* field in SBM Composer, and then disable the change requests selection in the hardware projects.

These overrides can be made for default fields in projects for the following field types:

- *Single Selection*
- *Multi-Selection*

These overrides can be made for default fields in workflows or projects for the following field types:

- *User*
- *Multi-User*
- *Multi-Group*

To enable or disable values for fields:

1. Edit the workflow or project for which you want to enable or disable selections.
2. Select **Default Fields**.
3. Search for or navigate to an applicable field.
4. Select the field, and then click **Details**.
5. Select the **Attributes** tab.
6. In the Values area, select the value you want to change, and then click one of the following options:
   - **Enabled**

Allows users to select the value for the field.

- **Disabled**

  Selections are not available as new values or for report search filters. If a selection is disabled after it has been used as a value by users, it appears as "(Disabled)" when they transition or update items.

- **Default**

  Indicates the selection is inheriting its status from the workflow or parent project.

7. Save your changes.

Overriding Display Options for Selection Fields

You can override the display options for selection-type fields, such as *User* and *Single Relational* fields. This allows you to set a field to allow searching in one project, but display it as a drop-down list in another project, for example.

These overrides can be made for default fields in projects and transition fields in projects for the following field types:

- *Single Selection*
- *Multi-Selection*
- *User*
- *Multi-User*
- *Multi-Group*
- *Single Relational*
- *Multi-Relational*
- *Folder*

To override display options for selection fields:

1. From the **Projects** view, select a project, and then click **Details**.
2. Do one of the following:
   - To override the display option for a field in a project, select the **Default Fields** tab.
   - To limit the override to a transition field in a project, select the **States/ Transitions** tab. Select the transition, click **Details** and then select the **Fields** tab.
3. Select the field to override, and then click **Details**.
4. Select the **Attributes** tab.
5. For fields that allow users to select a single value, such as *User*, *Single Selection*, *Single Relational*, and *Folder* fields, select one of the following:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **Single Drop-down List**

  Allows users to select a value from a drop-down list.

6. For fields that allow users to select multiple values, such as *Multi-Selection*, *Multi-User*, *Multi-Relational*, and *Multi-Group* fields, select one of the following:

   - **Allow Searching**

     Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

   - **List Box**

     Enables users to select one or more values from a list.

   - **Check Boxes**

     Enables users to select one or more values from check boxes populated with selections listed in the Selections area.

   - **Height of List Box**

     Indicates the number of rows that display values for the field on forms. You can set the number of rows to be displayed as appropriate for the number of expected values for the field. This option is available for the **List Box** and **Allow Searching** options.

7. Save your changes.

Working With Field Dependencies

Field dependencies enable you to control the values that are available for a field based on the selection users make for a different field.

For example, you can limit the values in an *Employee* field when users make a selection in a *Manager* field. In this example, when users select a manager, the values in the *Employee* field are limited to the manager's employees.

Each dependency is made up of an independent field and one or more dependent fields. In the example above, the *Manager* field is the independent field, and the *Employee* field is the dependent field because its values are dependent on the value selected in the independent field.

Field dependencies are defined in SBM Composer, but depending on the independent field type, some configuration may be required in Application Administrator. For auxiliary tables, some field dependency configuration tasks must be completed in SBM System Administrator.

The following tutorials explain the steps for defining and configuring each type of field dependency:

- Single Selection Field Dependency Tutorial [page 103]
- User Field Dependency Tutorial [page 104]

- Relational Field Dependencies Tutorial [page 107]

Dependency Field Types

The following table lists the available independent field types and the field types that allow dependencies.

Independent Field Types	Allowable Dependent Field Types	How to Configure
Single Selection field	*Single Selection*, *Multi-Selection*, *Multi-Group, Multi-User,* and *User* fields	1. Define the dependency in SBM Composer. 2. **Single Selection and Multi-Selection fields** — Configure dependent field values in SBM Composer. 3. **User, Multi-User, and Multi-Group fields** — Configure dependent values for projects in Application Administrator. Configure dependent values for auxiliary tables in SBM System Administrator. 4. Override dependent field values for projects in Application Administrator. For details, refer to Overriding Dependent Selections for Single Selection Fields in Projects [page 101].
Single Relational field	*Single Relational* and *Multi-Relational* fields	1. Define the dependency in SBM Composer. 2. Use the Auxiliary Data feature in Application Administratorin to add items to relational field auxiliary tables. For an example, refer to Relational Field Dependencies Tutorial [page 107].

Independent Field Types	Allowable Dependent Field Types	How to Configure
User field	*Single Selection*, *Multi-Selection*, *Multi-Group, Multi-User,* and *User* fields	1. Define the dependency in SBM Composer. 2. Configure dependent values for projects in Application Administrator. For details, refer to Configuring User Field Dependencies [page 102]. Configure dependent field values for auxiliary table fields in SBM System Administrator. 3. Override dependent field values for projects in Application Administrator.

Overriding Dependent Selections for Single Selection Fields in Projects

Prerequisites:

You must define the relationship between the independent and dependent fields before you can override dependent field selections for independent *Single Selection* fields in projects. This relationship is defined for primary tables in SBM Composer. For an example of how to define a dependency based on a *Single Selection* field, refer to Single Selection Field Dependency Tutorial [page 103].

You can override the dependent field selections for independent *Single Selection* fields in projects. You can override these settings for a parent project and inherit them in child projects, or override these settings for each project in the hierarchy.

To override dependent selections for *Single Selection* fields for projects:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **Default Fields** tab.
3. Navigate to or search for the independent *Single Selection* field, and then click **Details**.
4. Select the **Dependencies** tab.
5. From the **Select value to override** list, search for or select a value.
6. In the **Fields Dependent on *Independent Field Name*** pane, select the dependent field for which you want to override the available values.

7. In the **Selections in *Dependent Field Name*** pane, clear the check boxes for the values that should not be available for the value you are configuring, or select values that should be available. You can search for values as needed.
8. Optionally, select a default value from the **Default Value** list. You can also search for a value to set as a default.
9. Repeat steps 5-7 for each independent field selection.
10. Save your changes.

Configuring User Field Dependencies

Prerequisites:

You must define the relationship between the independent *User* field and its dependent field before you can configure dependent values. The dependency relationship is defined in SBM Composer. For an example of how to define a dependency based on a *User* field, refer to User Field Dependency Tutorial [page 104].

The following steps explain how to configure dependencies for a project in which a *User* field is the independent field. For steps on how to configure this setup for an auxiliary table, refer to *SBM System Administrator Guide*.

You can also override the dependent field selections for independent *User* fields in projects. You can override these settings for a parent project and inherit them in child projects, or override these settings for each project in the hierarchy.

To configure *User* field dependencies in projects:

1. From the **Projects** view, select a project, and then click **Details**.
2. Select the **Default Fields** tab.
3. Navigate to or search for the independent *User* field, and then click **Details**.
4. Select the **Attributes** tab, and then verify that the field has user values. If not, add selections following the instructions in Adding User and Group Values [page 81].

   Note: Users set as values should have privileges to view, submit, and update items in the projects for which dependencies are defined.

5. Select the **Dependencies** tab.
6. From the **Select value to override** list, select a value.
7. In the **Fields Dependent on *Independent Field Name*** pane, search for or select the dependent field for which you want to override the available values.
8. In the **Selections in *Dependent Field Name*** pane, clear the check boxes for the values that should not be available for the value you are configuring, or select values that should be available. You can search for user values as needed.
9. Optionally, select a default value from the **Default Value** list. You can also search for a user to set as a default value.

10. Repeat steps 6-8 for each independent field selection.
11. Save your changes.

Field Dependency Tutorials

The following tutorials explain how to set up field dependencies:

- Single Selection Field Dependency Tutorial [page 103]
- User Field Dependency Tutorial [page 104]
- Relational Field Dependencies Tutorial [page 107]

Single Selection Field Dependency Tutorial

Prerequisites:

- This tutorial assumes you have an application workflow created in SBM Composer and are familiar with basic application tasks, such as adding fields and field selections.
- To test this tutorial in the SBM User Workspace, you must have privileges to deploy to a running environment.

The following tutorial explains how to configure field dependencies that tailor the value list for a *Single Selection* field. You can reproduce this example for other field dependencies as needed.

In this example, you will create a *Product* field that has two available values: Product A and Product B. You will set dependencies to limit the values available in a *Version* field depending on the selection made in the *Product* field. For example, if a user selects Product A from the *Product* field, a set of available values unique to Product A are listed in the *Version* field.

This tutorial is configured exclusively in SBM Composer. You can log in to the SBM User Workspace to test the tutorial.

Tip: You can override dependent field values for independent *Single Selection* fields in projects in Application Administrator. For details, refer to Overriding Dependent Selections for Single Selection Fields in Projects [page 101].

To establish a dependency for two *Single Selection* fields:

1. In an application primary table in SBM Composer, create a *Single Selection* field named *Product*.
2. Select the **Options** tab for the *Product* field. Add the following values:
   - Product A
   - Product B
3. In the same table, create a *Single Selection* field named *Version*.
4. Select the **Options** tab for the *Version* field. Add the following values:

- 2.0
- 2.5
- 3.0
- 3.1

5. Select the *Product* field, and the select the **Dependencies** tab.
6. Select the *Version* field from the fields list to set it as the dependent field.
7. Select the **Edit Value Restrictions** link, and then select the workflow that contains the *Version* field. The **Dependencies** tab for the workflow opens.
8. Select **Product A** in the left pane, and then select the *Version* field check box in the middle pane. In the right pane, clear the **3.0** and **3.1** check boxes.
9. Select **Product B** in the left pane, and then select the *Version* field check box in the middle pane. In the right pane, clear the **2.0** and **2.5** check boxes.
10. Save, check in, publish, and deploy your changes.
11. Log in to the SBM User Workspace as a user who has privileges to view and update items in the application that contains the field dependency you added.
12. Submit an item into a project associated with the application workflow that contains the field dependency.

Values for the **Version** field are now dependent on the selection users make for the **Product** list. In this example, when Product A is selected from the **Products** list, the user can choose the None, 2.0, or 2.5 selections. When Product B is selected from the Products list, the user can choose the None, 3.0, or 3.1 selections.

Note: You can further enhance the dependency relationship by setting a default value for the dependent field. For example, you can set the **Version** field to default to *2.5* when *Product A* is selected in the **Product** field.

User Field Dependency Tutorial

Prerequisites:

- This tutorial assumes you are familiar with basic application tasks, such as adding fields and field selections, and with checking in, publishing, and deploying process apps.
- You must use SBM Composer and Application Administrator to set up the dependency. To complete this tutorial, you must have privileges to deploy to a running environment.
- Your application should contain two *User* fields with valid user selections. The fields should be called *Manager* and *Employee*. Users who are values should have privileges to view, submit, and update items in the application.

The following tutorial explains how to configure field dependencies that tailor the selection list for a *User* field. Dependencies will be set that limit the selections available in an *Employee* field depending on the selection made in the *Manager* field. For example, if a user selects Kathy Manager from the *Manager* field, Chris Tester and Hans Tester are available selections for the *Employee* field; if the user selects Joe Manager from the *Manager* field, Laura Engineer and Newton Engineer are available as selections for the *Employee* field.

Establish the Dependency in SBM Composer

In this step, you will create two *User* fields and establish a dependency between those fields.

To establish a dependency for a *User* field:

1. Open a process app in SBM Composer.
2. From the App Explorer, select the primary table for your application.
3. Add a *User* field named *Manager*.
4. Add another *User* field named *Employee*.
5. Select the *Manager* field, and then select the **Dependencies** tab.
6. In the list of available dependent fields, select *Employee*.
7. Save, check in, publish, and deploy your changes.

Add User Selections for the Independent and Dependent Fields

In this step, you will add user selections to the fields created in the previous step. To illustrate the example, sample users are added to the field.

To add user selections:

1. In Application Administrator, edit the workflow that contains the *Manager* and *Employee* fields.
2. Select the **Default Fields** tab.
3. Select the *Manager* field, and then click **Details**.
4. Select the **Attributes** tab.
5. In the **Values** section, click **Manage User Selections**, and then add Kathy Manager and Joe Manager as selections.
6. Save your changes.
7. Select the *Employee* field, and then click **Details**.
8. Select the **Attributes** tab.
9. In the **Values** section, click **Manage User Selections**, and then add Laura Engineer, Newton Engineer, Chris Tester, and Hans Tester as selections.

10. Save your changes.

Set Dependent Field Selections

In Application Administrator, you will specify which field selections are available for the dependent field based on the selection users make for the independent field. For example, when a user selects Kathy Manager from the *Manager* field, Chris Tester and Hans Tester are the only selections available in the *Employee* field.

To set dependent field selections:

1. In Application Administrator, edit the project for which the dependent values should be set.
2. Select the **Default Fields** tab.
3. Select the *Manager* field, and then click **Details**.
4. Select the **Dependencies** tab.
5. From the **Select Value to Override** list, select Joe Manager.
6. In the **Fields Dependent on *Manager*** pane, select the *Employee* field.
7. Clear the check boxes next to Chris Tester and Hans Tester.
8. From the **Select Value to Override** list, select Kathy Manager.
9. In the **Fields Dependent on *Manager*** pane, select the *Employee* field.
10. Clear the check boxes next to Laura Engineer and Newton Engineer, and then click **OK**.
11. Save your changes.

Test the Dependency

To test the dependency:

1. Log into the SBM User Workspace as a user who has privileges to the application that contains the dependency.
2. Submit an item into the project that you modified in Application Administrator in the previous steps.
3. On the **Submit** from, select Kathy Manager from the *Manager* field. Notice that Chris Tester and Hans Tester are available as selections for the *Employee* field.
4. Select Joe Manager from the *Manager* field. Notice that Laura Engineer and Newton Engineer are available as selections for the *Employee* field.

Relational Field Dependencies Tutorial

Prerequisites:

- This tutorial assumes you are familiar with basic application tasks, such as adding tables, and with checking in, publishing, and deploying process apps. You should also understand how to add items to auxiliary tables using the Auxiliary Data feature.
- You must use SBM Composer to set up the dependency. To complete this tutorial, you must have privileges to deploy to a running environment.

The following example explains how to configure field dependencies that tailor the value list for a *Single Relational* field added to a primary table. You can reproduce this example for other field dependencies as needed.

In this example, you will create two auxiliary tables: a *Products* table and a *Versions* table. You will then establish a relationship between the two tables that allows specific version records in the *Versions* table to be available for each product in the *Products* table. For example, if Version 1 and Version 2 only apply to Product A, those versions are the only available values when Product A is selected from the *Products* field.

To set up this Relational field dependency:

1. In SBM Composer, create two auxiliary tables: a *Products* table and a *Versions* table. For this example, the *Products* table is the independent field table and the *Versions* table is the dependent field table.
2. Add a *Single Relational* field of the independent field type to the dependent field table. For this example, add a *Single Relational* field to the *Versions* table, and select Products from the **Table** list located on the **Options** tab.
3. Open the application's primary table, and then add a *Single Relational* field that will serve as the independent field. For this example, name the field *Products*, and then select "Products" from the **Table** list on the **Options** tab for the *Single Relational* field.
4. In the same table, add another *Single Relational* field that will serve as the dependent field. For this example, name the field *Versions*, and then select "Versions" from the **Table** list on the **Options** tab for the *Single Relational* field.
5. Select the *Single Relational* field that serves as the independent field. For this example, select the *Products* field.
6. Select the **Dependencies** tab, and then select the *Versions* table from the dependent fields list.
7. Click the **Edit Value Restrictions** link, and then select the workflow for which you will restrict dependent field values.
8. Verify that the *Products* field is selected in the left pane, and then select the *Versions* field in the middle pane.
9. Select the *Products* field from the right pane.

10. Grant privileges to the *Products* and *Versions* tables. You can do this in SBM Composer by granting role privileges for each table, or you can assign user or group privileges to the table in Application Administrator after you deploy the process app. For this tutorial, users should be able to submit, view, and update items in both tables.
11. Save, check in, publish, and deploy your changes.
12. Log in to the SBM User Workspace as a user who has privileges to manage the *Products* and *Versions* tables.
13. To open the Auxiliary Data feature:
    - From the **Search** tab, select **Manage Data**.
    - If you have administrative privileges, select the **Administrator** icon, and then select the Auxiliary Data icon on the **Administrator Portal**.
14. Populate the *Products* table with items. For this example, add "Product A" and "Product B" items.
15. Populate the *Versions* table with the following items. When you add these items, select the listed value from the *Products* field:
    - Version 1 – Product A
    - Version 2 – Product A
    - Version 3 – Product B
    - Version 4 – Product B
    - Version 5 – Product B
16. Open the **Submit** form for a project used by the workflow in which you created the dependencies.
17. Click the **Find** button for the *Products* field. Notice that "Product A" and "Product B" are available as selections.
18. Select "Product A." Notice that for the *Versions* field, "Version 1" and "Version 2" are available.
19. Select "Product B" from the *Products* field. Notice that "Version 3," "Version 4," and "Version 5" are available as selections in the *Versions* field.

Field Types and Settings

In SBM Application Administrator, general properties can only be viewed, but some attributes can be modified for certain field types. The following sections describe the properties available for each field type.

- General Field Settings [page 109]
- Binary/Trinary Fields [page 112]
- Date/Time Fields [page 113]

- Folder Fields [page 116]
- Multi-Group Fields [page 118]
- Multi-Relational Fields [page 120]
- Multi-Selection Fields [page 122]
- Multi-User Fields [page 124]
- Numeric Fields [page 126]
- Single Relational Fields [page 129]
- Single Selection Fields [page 131]
- Summation Fields [page 133]
- Text Fields [page 134]
- User Fields [page 136]

General Field Settings

General field properties are set in SBM Composer, but you can view them in Application Administrator. The following table describes these properties.

Field Property	Description	Applicable Field Types
Name and Description Settings		
Logical Field Name	Indicates the name of the field as it appears to users. You can change this name in SBM Composer.	All
Database Field Name	Indicates the field name as it is stored in the database. The database field name cannot be changed or removed.	All, except *Sub-Relational*
End-user help text	The text entered here is displayed to users who hover the mouse pointer over the field name and in a help window users can opens from forms. Use the scroll bar to view long descriptions. To hide the text, collapse the **General** section.  **Note:** HTML tags provided in SBM Composer are not rendered.	All
Relationship		

Field Property	Description	Applicable Field Types
Table	Indicates the relational field table.	*Single Relational* and *Multi-Relational*
Relational Field	Indicates the *Single Relational* field associated with the *Sub-Relational* field.	*Sub-Relational*
Sub-Field	Indicates the field from the relational field table whose value will be displayed on forms.	*Sub-Relational*
Display and Query Settings		
Spans Entire Row on Forms	If selected, this check box indicates that the field will appear on a single row on quick forms. If this check box is cleared, the field appears with another field on a row.	All field types, except *Text* fields that are set as memo fields or fixed length fields whose length is greater than the **Max Text Field Size** setting for your database. This settig is located on the **Display** tab of the **Settings** dialog box in SBM System Administrator.

Field Property	Description	Applicable Field Types
Appears in Report Field List	When this check box is selected, the field is included on report forms. This enables you to simplify field lists for users who are creating reports. Depending on the type of field you are creating, when the **Appears in Report Field List** check box is selected, the field appears in the **Field Specification**, **Select Columns to Display**, **Add Columns of Calculations**, and **Sorting** lists on report forms. The field is also included in the **Row** and **Column** lists on **Distribution** reports and the **Trend** lists on **Trend** reports. By default, the **Appears in Report Field List** check box is selected. In addition, if a field is used on a report and the **Appears in Report Field List** check box is later cleared, the setting is ignored for that report.	All
Appears on Lookup Form and Relational Field Value Lookup	If this check box is selected, the field is added to the Auxiliary Data search form in SBM Application Administrator and the Advanced Lookup Tool and Relational Field Value Lookup forms.  **Tip:** The field order for the Advanced Lookup Tool and Relational Field Value Lookup forms is determined by the default field order of the table's first project in the project hierarchy. To display fields in a different order, add another project to this hierarchy, clear the **Allow New Items to Be Submitted** check box, and drag the project to the top of the hierarchy for this table. You can also remove all user privileges for this project so that the project is only used to determine field order for search forms.	
Allow Searching	This option enables Value Find and Relational Field Value Lookup capability for the field. Value Find allows users to enter search criteria, such as an entire word, a few letters, or an asterisk, and then click a search icon or press **Enter** to perform the search. Results appear in a list, allowing users to select a value for the field. Relational Field Value Lookup provides an advanced searching mechanism that enables user to find values for *Single Relational* and *Multi-Relational* fields. If enabled, an additional search icon is available.	*Folder*, *Single Relational*, *Multi-Relational*, *Single Selection*, *Multi-Selection*, *User*, *Multi-User*, and *Multi-Group* fields

Field Property	Description	Applicable Field Types
Show Full List	This option allows users to select a value from a fully populated list rather than search for values.	*Folder*, *Single Relational*, *Multi-Relational*, *Single Selection*, *Multi-Selection*, *User*, *Multi-User*, and *Multi-Group* fields
Automatically Prepend Wildcard to Lookup Text	When this check box is selected, wildcard characters are prepended to the search text for this field as long as there are no wildcard characters within the text. This allows users to easily search for keywords. When this check box is selected, a percent sign (%) appears next to the field on Advanced Lookup Tool and Relational Field Value Lookup forms and on the Auxiliary Data search form in SBM Application Administrator. Note that when this check box is cleared, a wildcard character is automatically appended to the entered search text as long as there are no wildcard characters within the text.	*Text* fields, except for the *Item ID* system field

Binary/Trinary Fields

Binary/Trinary fields can store either two values or three values that are defined in SBM Composer. *Binary/Trinary* fields are also used to determine subtask status. The values provided as first, second, and third values correspond to actions based on subtask status.

Attributes

The following *Binary/Trinary* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Defaults

Indicates the pre-selected value for this field. For fields set to be displayed as a check box, "Checked" and "Not Checked" are available as default values.

Display Options

You can view display settings for default *Binary/Trinary* fields. These settings are defined in SBM Composer and cannot be modified in Application Administrator.

- **Listbox**

  Users select a value from a list populated with first, second, or trinary/third values. This option is available for *Binary* and *Trinary* fields.

- **Radio Button**

  Users select a value from a radio button list populated with the first, second, or trinary/third values. This option is available for *Binary* and *Trinary* fields.

- **Checkbox**

  The **Logical Field Name** field property is the label for the field. Users either select or clear the check box. This option is only available for *Binary* fields.

- **First Value, Second Value, Third Value (if applicable)**

  Indicates the values for the field. If the field is used to determine subtask status, the values can be used to specify which values relate to the three applicable subtask statuses: In Review/Progress, Accepted/Complete, and Rejected/Reverted.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Date/Time Fields

Date/Time fields store date and time values. *Date/Time* fields can display the date only, date and time, time only, or elapsed time.

The following information applies to *Date/Time* fields:

- *Date/Time* values are stored in the DBMS native date data type.
- Values for *Date/Time* fields set to record time only or elapsed time are stored as integers. Assuming a default value of "Now", the value stored in the database is equal to the number of seconds that have passed since 12:00:00 a.m. in the submitter's or modifier's time zone.
- The system interprets modified Julian dates in *Date/Time* fields that are not set as elapsed time fields. For example, if users enter 09092008 into a *Date* field, the date is saved as 04/16/1970. The date entered was interpreted as a modified Julian date, which is seconds since Jan. 1, 1970.

Attributes

The following *Date/Time* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Defaults

Specify a prefilled value for the field as needed. You can use a special value, such as "Start of Tomorrow," or you can use the calendar to select an exact value.

Display Options

You can view display settings for default *Date/Time* fields. These settings are defined in SBM Composer and cannot be modified in Application Administrator.

- **Style**
  - Date and Time (mm/dd/yyyy hh:mm:ss)
  - Date Only (mm/dd/yyyy)
  - Time of Day (hh:mm:ss)
  - Elapsed Time ([d] hh:mm:ss)
- **Stopwatch**

If selected, indicates that elapsed time is recorded between the time a form is opened and closed.

- **Calculate Days**

  If selected, indicates that numbers of days are calculated from the provided value and displayed to users.

- **Show Seconds**
  If selected, indicates that elapsed time values are displayed in 00:00:00 format.

  Note: Seconds are always stored, but are only displayed to users if the **Show Seconds** check box is selected.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

The following options apply to calculation options for *Date/Time* and *Numeric* fields. For details, refer to Calculating Values for Date/Time and Numeric Fields [page 64].

- **Set Value to Calculation**

  Select this option to define a calculation that executes when the transition is executed, and then select the following options:

  - **Calculate...**

    From the first list, choose to perform the calculation before the **Transition** form opens, after the open form is submitted, or both.

  - **First Operand**

    Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], specify a constant value, field, or date/time keyword to use as the first operand in the calculation. This will be filled with the current value of the first operand. The field selected from the list cannot be the same field as the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.

  - **Operator**

    Using the guidelines and tips in Calculating Values for Date/Time and Numeric Fields [page 64], select a valid operator for the calculation.

- **Second Operand**

  Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], enter a second constant or a valid field. Valid fields for the second operand are dependent on the field type, the first operand, and the operator. If the first operand or operator chosen causes the second operand to be invalid, the second operator is changed to a valid constant. The second operand cannot be the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.

- **Empty Operand Fields**

  Select one of the following options:

  - **Are Invalid**

    Select to require users to provide values for fields used as operands for the calculation before the transition can be completed.

  - **Skip Calculation**

    Select to allow users to complete the transition without providing values for fields used as operands for the calculation. The calculation is skipped if values are not provided.

  - **Treat as Zero**

    Select to perform the calculation and treat empty values in fields used as operands for the calculation as zeros.

- **Add Calculation to Current Value**

  Select to add the calculation to the field's current value. This enables you to increment the current value or to calculate the total of the calculation and the current value. This option is only available for *Numeric* fields and *Date/Time* fields set to record elapsed time.

Folder Fields

Folder fields allow users to link primary or auxiliary items to a **Public** or **Knowledge Base** folder.

Note: Information for the *Project*, *State*, and *Contact* system fields is also shown on this page.

Folders must be created and configured correctly in SBM System Administrator before they can be used as selections for *Folder* fields. Specifically:

- The **Allow New Items to Be Added to this Folder** check box must be selected. You can select this check box when you add or edit a folder.
- You must grant users or groups the "Add Items to Folder" privilege located on the **Folders** privileges page.

Attributes

The following *Folder* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **Single Drop-down List**

  Allows users to select a value from a drop-down list.

Defaults

Specify a default value from the possible selections. For *Folder* fields, you can choose a Public and Knowledge Base folder defined in SBM System Administrator. Possible selections vary for system fields, such as the *Project* and *State* fields, but use caution when selecting default values for system fields because doing so may impact system behavior.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Multi-Group Fields

Multi-Group fields allow you to define one or more groups for users to choose from.

Multi-Group fields are useful for assigning multiple groups of people to be secondarily responsible for items while they reside in a particular state. For example, you may want customer requests to be owned by a product management group and a marketing group when they are first added to the system. You can specify these groups as secondary owners in the "New" state. This configuration is made in SBM Composer. For details, refer to the *SBM Composer Guide*.

Multi-Group fields are defined in SBM Composer, but you can perform the following overrides and configuration tasks in Application Administrator:

- Add and delete selections for these fields in workflows so they are available for all projects assigned to the workflow. For details, refer to Adding User and Group Values [page 81].
- Enable and disable selections for these fields in workflows or projects. For details, Enabling and Disabling Selection Field Values [page 97].
- Set default values for these fields in workflows or projects.
- Override the default values for these fields for projects and for transitions in projects.
- Override display options for *User* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

The **Allow Override** check box is automatically selected when you modify attributes and value and display options when you are adding or editing a project.

Attributes

You can override the following *Multi-Group* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transitions fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

- **Check Boxes**

  Enables users to select one or more values from check boxes populated with selections listed in the Selections area.

- **Height of List Box**

  Indicates the number of rows that display values for the field on forms. You can set the number of rows to be displayed as appropriate for the number of expected values for the field. This option is available for the **List Box** and **Allow Searching** options.

Value Options

Use the Values section to add or remove selections for fields in workflows or and enable or disable group selections for fields in workflows or projects.

Note: Roles may be associated with the field in SBM Composer. You cannot disable role values for the field in Application Administrator. You must remove the role association from the field in SBM Composer.

The following options are available on this pane:

- **Enable**

  Select one or more values, and then click **Enable** to allow users to select the group as a value.

- **Disable**

  Select one or more values, and then click **Disable** to prevent the users from selecting the value on forms or for report search filters.

  Note: If a group account is deleted or the value is disabled after it has been used as a value, it appears as "(Disabled)" when users update or transition items. Users are required to provide a valid value for the field.

- **Use Inherited**

  Select a value, and then click **Use Inherited** to use the value's status from the parent workflow.

- **Manage Group Selections**

  Click this link to add group selections to the field. This option is only available when you are editing a workflow. For details, refer to Adding User and Group Values [page 81].

- **Show Selections Referencing Deleted Groups**

  Includes in the list groups that were previously specified as selections and later deleted. You can then delete the referenced selection.

Defaults

Set a default value by selecting **Manage User/Group Defaults**. Default values can be set for workflows if overrides have been enabled for the field in SBM Composer. You can also set or override default values in projects. For details, refer to Setting Default Values for User-type Fields [page 96].

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Multi-Relational Fields

Multi-Relational fields allow users to select one or more items from a primary or auxiliary table as values. This associates items with a particular table or workflow.

For example, you can create an auxiliary table that stores versions of products. You can then create a *Multi-Relational* field in a primary table that tracks data related to customer-reported defects, and set the versions table as the relational field table. This allows users to select multiple product version numbers for each defect being tracked.

Multi-Relational fields are defined in SBM Composer. Use the Auxiliary Data feature in Application Administrator to add values for *Multi-Relational* fields based on auxiliary tables. Values for *Multi-Relational* fields based on primary tables are created by users as they submit items into projects.

The following overrides and configuration tasks are performed in Application Administrator:

- Specify default values for these fields for projects and transitions in projects.
- Override display options for *Multi-Relational* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

Note: Default values for *Multi-Relational* fields in auxiliary tables are set in SBM System Administrator.

Attributes

You can override the following *Multi-Relational* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transitions fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

- **Check Boxes**

  Enables users to select one or more values from check boxes populated with selections listed in the Selections area.

- **Height of List Box**

  Indicates the number of rows that display values for the field on forms. You can set the number of rows to be displayed as appropriate for the number of expected values for the field. This option is available for the **List Box** and **Allow Searching** options.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Value Options

The field's default values, if applicable, are listed. Select default values as needed. Possible default values are determined by the active records in the relational field table listed on the **General** page for the field. For example, if the relational field table is a *Versions* table, possible default values are version records in the table.

Multi-Selection Fields

Multi-Selection fields allow users to select one or more values for the field.

Multi-Selection fields, selections, and selection ordering are defined in SBM Composer, but you can perform the following overrides and configuration tasks in Application Administrator:

- Set or override the default values for these fields for projects and for transitions in projects.
- Enable or disable selections for fields in projects. For details, refer to Enabling and Disabling Selection Field Values [page 97].
- Override display options for *Multi-Selection* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

The **Allow Override** check box is automatically selected when you modify attributes and value and display options.

Attributes

You can override the following *Multi-Selection* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transitions fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

- **Check Boxes**

  Enables users to select one or more values from check boxes populated with selections listed in the Selections area.

- **Height of List Box**

  Indicates the number of rows that display values for the field on forms. You can set the number of rows to be displayed as appropriate for the number of expected values for the field. This option is available for the **List Box** and **Allow Searching** options.

Value Options

Use the Values section to set default values for the field and change the status of selections as needed. For example, you may want to enable a set of hardware products for a Products field for one project, but disable them in a project used to store information about software products.

The following options are available on this pane:

- **Default Value**

  The field's default values, if applicable, are selected. You can change the default values as needed by selecting or clearing the box next to each value.

- **Value**

  The selection values defined in SBM Composer are listed.

- **Status**

  Indicates the value's status. You can change the status by selecting one or more values, and then clicking one of these options:

  - **Enabled**

    Allows users to select the value for the field.

  - **Disabled**

    Selections are not available as new values on forms or for report search filters. If a selection is disabled after it has been used as a value, it appears as "(Disabled)" when users transition or update items and a valid value must be selected before the form can be completed.

  - **Use Inherited**

    Indicates the selection is inheriting its status from the workflow or parent project.

- **Show Deleted**

  Select this check box to show deleted selections in the list.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Multi-User Fields

Multi-User fields allow you to define one or more users or groups as selections. This enables users to select multiple users as values. This is particularly useful for defining secondary ownership for items. Secondary ownership assigns multiple users responsibility for items that reside in a particular state. For details, refer to the *SBM Composer Guide*.

Multi-User fields are defined in SBM Composer, but you can perform the following overrides and configuration tasks in Application Administrator:

- Add and delete selections for these fields in workflows so they are available for all projects assigned to the workflow. For details, refer to Adding User and Group Values [page 81].
- Enable and disable selections for these fields in workflows or projects. For details, Enabling and Disabling Selection Field Values [page 97].
- Set default values for these fields in workflows or projects.
- Override the default values for these fields for projects and for transitions in projects.
- Override display options for *User* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

The **Allow Override** check box is automatically selected when you modify attributes and value and display options when you are adding or editing a project.

Attributes

You can override the following *Multi-User* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transition fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

- **Check Boxes**

  Enables users to select one or more values from check boxes populated with selections listed in the Selections area.

- **Height of List Box**

  Indicates the number of rows that display values for the field on forms. You can set the number of rows to be displayed as appropriate for the number of expected values for the field. This option is available for the **List Box** and **Allow Searching** options.

Value Options

Use the Values section to add or remove user and group selections for fields in workflows. Also, use these options to enable or disable user and group selections for fields in workflows or projects.

Note: Roles may be associated with the field in SBM Composer. You cannot disable role values for the field in Application Administrator. You must remove the role association from the field in SBM Composer.

The following options are available on this pane:

- **Enable**

  Select one or more values, and then click **Enable** to allow users to select the value. Enabled groups allow users to select a member of the group.

- **Disable**

  Select one or more values, and then click **Disable** to prevent the users from selecting the value on forms or for report search filters.

  Note: If a user or group account is deleted or the value is disabled after it has been used as a value, it appears as "(Disabled)" when users update or transition items. Users are required to provide a valid value for the field.

- **Use Inherited**

  Select a value, and then click **Use Inherited** to use the value's status from the parent workflow.

- **Manage User Selections**

  Click this link to add user values to the field. This option is only available when you are editing a workflow. For details, refer to Adding User and Group Values [page 81].

- **Manage Group Selections**

  Click this link to add group values to the field. This option is only available when you are editing a workflow. For details, refer to Adding User and Group Values [page 81].

- **Show Selections Referencing Deleted Users and Groups**

  Includes in the list users and groups that were previously specified as selections and later deleted. You can then delete the referenced selection.

Defaults

Set a default value by selecting **Manage User/Group Defaults**. Default values can be set for workflows if overrides have been enabled for the field in SBM Composer. You can also set or override default values in projects. For details, refer to Setting Default Values for User-type Fields [page 96].

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Numeric Fields

Numeric fields store signed integers, floating point values, or fixed precision values. A prefix and suffix can also be set for *Numeric* fields.

Tip: *Numeric* fields can be used as weights in **Trend** reports; to ensure accurate results when you use weights, ensure fields that use weighting always have values by setting a default value or setting the field as required.

Attributes

The following *Numeric* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Settings

The following display settings are defined in SBM Composer and can only be viewed in this interface:

- **Style** — Indicates the field's style:
  - **Integer**

    Allows for integer values. The maximum positive integer accepted is 2147483643 and the minimum negative integer accepted is -999999999.

  - **Floating Point**

    The maximum and minimum accepted range of values are determined by your server hardware.

  - **Fixed Precision**

    The maximum and minimum accepted range of values are determined by your server hardware. The number of digits that will be displayed after the decimal point (with a minimum of 0 and a maximum of 15) is also indicated.

- **Prefix**

  Indicates the prefix that appears before the *Numeric* field value.

- **Suffix**

  Indicates the suffix that appears after the *Numeric* field value.

- **Show thousands separator**

  Indicates that values will be displayed with commas. For example, after selecting this check box, a *Numeric* field would appear as 1,000 rather than 1000.

Defaults

Specify a prefilled value for the field as needed.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

The following options apply to calculation options for *Date/Time* and *Numeric* fields. For details, refer to Calculating Values for Date/Time and Numeric Fields [page 64].

- **Set Value to Calculation**

  Select this option to define a calculation that executes when the transition is executed, and then select the following options:

  - **Calculate...**

    From the first list, choose to perform the calculation before the **Transition** form opens, after the open form is submitted, or both.

  - **First Operand**

    Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], specify a constant value, field, or date/time keyword to use as the first operand in the calculation. This will be filled with the current value of the first operand. The field selected from the list cannot be the same field as the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.

  - **Operator**

    Using the guidelines and tips in Calculating Values for Date/Time and Numeric Fields [page 64], select a valid operator for the calculation.

  - **Second Operand**

    Using the guidelines in About Operand Fields and Operator Selection Lists [page 67], enter a second constant or a valid field. Valid fields for the second operand are dependent on the field type, the first operand, and the operator. If the first operand or operator chosen causes the second operand to be invalid, the second operator is changed to a valid constant. The second operand cannot be the field being edited, a field that could cause a recursive calculation, a deleted field, or a field in the **Not Used** section.

- **Empty Operand Fields**

  Select one of the following options:

  - **Are Invalid**

    Select to require users to provide values for fields used as operands for the calculation before the transition can be completed.

  - **Skip Calculation**

    Select to allow users to complete the transition without providing values for fields used as operands for the calculation. The calculation is skipped if values are not provided.

  - **Treat as Zero**

    Select to perform the calculation and treat empty values in fields used as operands for the calculation as zeros.

- **Add Calculation to Current Value**

  Select to add the calculation to the field's current value. This enables you to increment the current value or to calculate the total of the calculation and the current value. This option is only available for *Numeric* fields and *Date/Time* fields set to record elapsed time.

Single Relational Fields

Relational fields are used to establish relationships between data in primary and auxiliary tables. *Single Relational* fields allow users to select a single item from a primary or auxiliary table as a value for the field.

For example, you could create a relationship in a primary table used to track defects to knowledge base articles in the Problems table. While users are entering information about a defect, they could select a problem record that is stored in the Problems table. This enables users to see information in the Problems table while they are working with items in the primary table.

Single Relational fields are defined in SBM Composer. Use the Auxiliary Data feature in Application Administrator to add values for *Single Relational* fields based on auxiliary tables. Values for *Single Relational* fields based on primary tables are created by users as they submit items into projects.

The following overrides and configuration tasks are performed in Application Administrator:

- Specify default values for these fields for projects and transitions in projects.
- Override display options for *Single Relational* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

Note: Default values for *Single Relational* fields in auxiliary tables are set in SBM System Administrator.

The **Allow Override** check box is automatically selected when you modify attributes and value and display options when you are adding or editing a project.

Attributes

You can override the following *Single Relational* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transitions fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

Defaults

The field's default value, if applicable, is selected. You can change this value as needed. Possible default values are determined by the active records in the relational field table listed on the **General** page for the field. For example, if the relational field table is a Customers table, possible default values are customer records in the table.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Single Selection Fields

Single Selection fields allow users to select a single value for the field.

Single Selection fields, selections, and selection ordering are defined in SBM Composer, but you can perform the following overrides and configuration tasks in Application Administrator:

- Override the default values for these fields for projects and for transitions in projects.
- Enable or disable selections for fields in projects. For details, refer to Enabling and Disabling Selection Field Values [page 97].
- Override display options for *Single Selection* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

The **Allow Override** check box is automatically selected when you modify attributes and value and display options when you are adding or editing a project.

Attributes

You can override the following *Single Selection* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transition fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **List Box**

  Enables users to select one or more values from a list.

Value Options

Use the Values section to set a default value for the field and change the status of selections as needed. For example, you may want to disable the "low" selection for a

Priority field for a project that stores customer complaints, but enable it for a project that stores employee complaints.

The following options are available on this pane:

- **Default Value**

  The field's default value, if applicable, is selected. You can change the default value by selecting the box next to the value.

- **Value**

  The selection values defined in SBM Composer are listed.

- **Status**

  Indicates the value's status. You can change the status by selecting one or more values, and then clicking one of these options:

  - **Enabled**

    Allows users to select the value for the field.

  - **Disabled**

    Selections are not available as new values on forms or for report search filters. If a selection is disabled after it has been used as a value, it appears as "(Disabled)" when users transition or update items and a valid value must be selected before the form can be completed.

  - **Use Inherited**

    Indicates the selection is inheriting its status from the workflow or parent project.

- **Weight**

  Indicates the numeric value given to the field's selections in SBM Composer. Weights can be used in Trend reports and in *Summation* fields when users sum the values contained in the *Single Selection* field.

- **Prefix**

  Indicates prefixes defined in SBM Composer for the system *Item Type* field.

- **Show Deleted**

  Select this check box to show deleted selections in the list.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Summation Fields

Summation fields sum the values contained in *Single Selection* fields by the assigned weights or in *Numeric* fields set as integers. *Summation* fields are defined in SBM Composer, but you can view fields selected to sum.

Attributes

The following *Summation* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Note: For *Summation* fields, the **Set Value to Default Value** option overrides the field's automatic behavior.

Text Fields

Text fields allow users to enter information about primary and auxiliary items. The number of characters allowed in *Text* fields depends on the DBMS you are using and the **Style** options selected for the field in SBM Composer.

Attributes

The following *Text* field attributes can be modified for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Allow Override**

  For projects, select this check box to override field properties inherited from the parent project or workflow.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Defaults

Set or override a default value for the field as needed.

Note: You cannot change the default value for the system *Item ID* field.

You can use a Rich Text Editor to format default values for Memo and Journal fields if the **Enable Rich Text** check box is selected in the **Display Options** section.

If you choose to manually enter HTML as a default value, be aware that obviously "suspicious" ("dangerous") HTML is not rendered at runtime.

The following tags are considered suspicious:

- `<applet`, `</applet`
- `<embed`, `</embed`
- `<form`, `</form`
- `<frame`, `</frame`
- `<iframe`, `</iframe`
- `<input`, `</input`

- `<script`, `</script`
- `<textarea`, `</testarea`

The following tags may not be rendered at runtime unless they are added using the Rich Text Editor. These tags will not be rendered if they contain suspicious attributes, such as `onload` or `onclick`:

- `<a`, `</a`
- `<img`, `</img` (Rendered only when added at runtime)

Remember: Improper or invalid HTML could have a negative impact on the field and possibly on the entire form. Refer to the World Wide Web Consortium Web site at http://www.w3.org for information about HTML syntax.

If the **Enable Rich Text** check box is cleared for the field, only plain text is allowed. Carriage or hard returns can be entered in the default values for Memo and Journal fields, but not for Fixed Length fields.

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Note: For *Text* fields that are set as Journal fields, the default value is always appended to current values, if they exist.

Display Options

You can also view the following settings, which are defined in SBM Composer. These settings cannot be modifed in Application Administrator.

- **Style** — Indicates the field's style:
  - **Memo**

    Allows users to enter up to approximately 64,000 unicode characters.

  - **Journal**

    Automatically inserts a date, time, and user ID when users add text to the field. The *Journal* field's timestamp entry is stored in the database as the modified Julian date, which is the number of seconds since Jan. 1, 1970 in UTC.

  - **Fixed Length of n characters**

    Indicates the number of allowed unicode characters, up to a maximum of 255.

- **Require Appended Text**

  Available for Journal fields only. Indicates that users are required to append text to information already provided for the field.

- **Append Only**

  Available for Journal fields only. Indicates that users can only append text to existing Journal entries. If this check box is cleared, users can modify data in existing entries.

- **Prefix and Suffix**

  Indicates provided prefix and suffix for values for the field. The prefix and suffix can contain formatting HTML or plain text.

- **Include Field in Keyword Searches**

  Indicates that users can search for data in this field using Basic Search, Advanced Search, Global Search, and the Knowledge Base.

- **Enable Rich Text**

  Indicates that the Rich Text Editor is enabled for the field. This enables users to apply basic formatting to text in the field, and for you to format default values.

  If HTML5 features are disabled for your system, HTML tags added to the field are rendered at runtime if this option is selected.

  The **Enable Rich Text** option applies only to Memo and Journal fields. This setting can be changed in SBM Composer.

Note: If you enable Rich Text for a field, but HTML5 features are disabled for your system, users can manually type HTML tags into the field, and they will be rendered on State form.

User Fields

User fields allow users to select a single user in the system as a value. This is useful for defining ownership of primary items, and for recording user data in primary and auxiliary items.

For example, you can specify a *Manager* field for a state's Owner property. Users who are values for the Manager field through a role, user, or group assignment are available as values for that state. You can configure your process so that users select an owner as they transition items into a state, or so that owners are automatically defined in each state.

User fields are defined in SBM Composer, but you can perform the following overrides and configuration tasks in Application Administrator:

- Add and delete selections for these fields in workflows so they are available for all projects assigned to the workflow. For details, refer to Adding User and Group Values [page 81].
- Enable and disable selections for these fields in workflows or projects. For details, Enabling and Disabling Selection Field Values [page 97].

- Set default values for these fields in workflows or projects.
- Override the default values for these fields for projects and for transitions in projects.
- Override display options for *User* fields in projects and transitions in projects. For details, refer to Overriding Display Options for Selection Fields [page 98].

The **Allow Override** check box is automatically selected when you modify attributes and value and display options when you are adding or editing a project.

Attributes

You can override the following *User* field attributes for default fields in projects and transition fields. Attributes set for fields in the Default Fields list apply to all transitions; attributes set for fields for a transition apply only to that transition.

- **Required**

  Indicates that users are required to provide a value for this field. If a value was previously set for the field, the field label appears in green, italic text on forms.

- **Allow Mass Update**

  Indicates that the field is available when users mass update items in a project. Mass updates allow users to simultaneously transition, update, or delete multiple primary items and to simultaneously update or delete multiple auxiliary items.

- **Read Only**

  Indicates that users can view but not edit the field.

Display Options

You can override the following display options for default fields in projects and transition fields:

- **Allow Searching**

  Indicates that the *Value Find* feature is enabled for the field on submit, transition, and update forms. This allows users to enter to search for values.

- **Single Drop-down List**

  Allows users to select a value from a drop-down list.

Value Options

Use the Values section to add or remove user and group selections for fields in workflows. Also, use these options to enable or disable user and group selections for fields in workflows or projects.

Note: Roles may be associated with the field in SBM Composer. You cannot disable role values for the field in Application Administrator. You must remove the role association from the field in SBM Composer.

The following options are available on this pane:

- **Enable**

  Select one or more values, and then click **Enable** to allow users to select the value. Enabled groups allow users to select a member of the group.

- **Disable**

  Select one or more values, and then click **Disable** to prevent the users from selecting the value on forms or for report search filters.

  Note: If a user or group account is deleted or the value is disabled after it has been used as a value, it appears as "(Disabled)" when users update or transition items. Users are required to provide a valid value for the field.

- **Use Inherited**

  Select a value, and then click **Use Inherited** to use the value's status from the parent workflow.

- **Manage User Selections**

  Click this link to add user values to the field. This option is only available when you are editing a workflow. For details, refer to Adding User and Group Values [page 81].

- **Manage Group Selections**

  Click this link to add group values to the field. This option is only available when you are editing a workflow. For details, refer to Adding User and Group Values [page 81].

- **Show Selections Referencing Deleted Users and Groups**

  Includes in the list users and groups that were previously specified as selections and later deleted. You can then delete the referenced selection.

Note: Values are automatically added to the system *Owner*, *Secondary Owner*, and *Submitter* fields.

Defaults

Set a default value by selecting **Manage User/Group Defaults**. Default values can be set for workflows if overrides have been enabled for the field in SBM Composer. You can also set or override default values in projects. For details, refer to Setting Default Values for User-type Fields [page 96].

Transition Actions

The following options are available for fields when you are editing a transition and enable you to control field values for the transition. For example, you may want to clear an existing value for a required field when a transition is executed, forcing users to provide a new value. These options apply to all field types for transitions.

- **Leave Value Unchanged**

  Select to retain the field's current value when the transition is complete.

- **Clear Value**

  Select to clear the field's current value.

- **Set Value to Default Value**

  Select to use a default value for the field as the user executes the transition. You can then select a default value.

Chapter 5: Managing Users, Roles, and Groups

The following topics describe how manage security in SBM Application Administrator through users, roles, and groups.

About User Management and Security

SBM offers highly configurable security mechanisms through users, groups, and roles. You can control access to specific applications, including information in individual items, the actions users can perform on these items, access to reports, and more. You can also control administrative access to each application.

About User Management

There are four key elements for managing users in SBM:

- **Roles**

  A role is a set of application-related privileges. Roles are defined in SBM Composer, and users and groups are assigned to roles in SBM Application Administrator. For details, refer to About Roles [page 168].

- **Groups**

  A group is a set of users, to which you can assign roles, additional privileges, an initial set of preferences, and notification subscriptions. For details, refer to About Group Accounts [page 172].

- **Users**

Each user must have an individual account that at a minimum includes a unique login ID, a user name, and a product-access level. You can then assign users to groups so they can inherit role assignments, privileges, and notification subscriptions. For details, refer to About User Accounts [page 144].

- **Administrators**

  You can have multiple administrators, each with varying amounts of responsibility and access. For details, refer to Chapter 6: Managing Administrators [page 255].

To effectively manage user accounts, follow these basic steps.

1. In SBM Composer, create roles for your applications to organize sets of privileges, and then:
   a. Assign appropriate application-related privileges to each role.
   b. Assign roles as values for *User*, *Multi-User*, and *Multi-Group* fields in tables located in the **Data Design** area.
   c. Assign primary and secondary owners to states in your workflows.
   d. Deploy your process app to make the roles available in Application Administrator.

   For details on these steps, refer to the *SBM Composer Guide*.
2. In Application Administrator, create groups to organize sets of users, and then:
   a. Assign an appropriate product-access level to each group. This impacts which users can be members of the group, as well as which privileges apply to the group. For details, refer to Product-Access Types [page 143].
   b. Assign roles to each group.
   c. Assign any non-application-related privileges to the group, such as the ability to modify user profile settings, and for administrators, the ability to perform configuration and administration tasks.
   d. Set an initial set of preferences and settings to members of the group.
   e. Subscribe the group to notifications.

   For details on these steps, refer to Working With Groups [page 172].
3. Use one of the methods described in About User Accounts [page 144] to establish user accounts for your system. If you choose to manually create user accounts, edit multiple user accounts in Application Administrator, and then:
   a. Assign a product-access level based on the groups to which you will assign the users.
   b. Assign users to applicable groups. They will inherit their role assignments, notification subscriptions, and additional privileges from these groups.
   c. Modify password settings for the users, if applicable.
4. Optionally, set default values for *User*, *Multi-User*, and *Multi-Group* fields in workflows or projects in Application Administrator. Possible values are determined by

the roles assigned to the field in SBM Composer, and the users and groups assigned to the roles in Application Administrator.

Product-Access Types

Product-access types determine the set of privileges available for user and group accounts. You must assign product access to all user and group accounts before you can assign privileges to those accounts.

If you associate a user or group with a role, and the role contains privileges that conflict with the user or group level of product access, those privileges are not granted to the user or group. For example, if you associate a user who has External User product access with a role that has privileges to transition all items, that user will not be able to transition items because External User access does not grant that privilege.

On-premise Product-access Types

Product-access types are tied to software licenses you have purchased for your system. For details, refer to the *SBM Licensing Guide* available at http://www.serena.com/support or contact your Serena sales representative.

The following product-access types are available:

- **None**

  No product access granted. This access type can be used to set up general information for an account before assigning an access type. None can also be used to remove product access.

- **External User**

  Allows a limited set of privileges. Users with this access type can submit primary items, view primary items they submit or that are submitted by users from the same company, self register (if this feature is enabled), submit primary items by e-mail, access the Knowledge Base, and run guest-level reports based on primary tables.

- **Occasional User**

  Allows users to own primary items they submit, update and transition primary items they own or submit, view all field sections for primary items they submit, and add and edit attachments and notes to items they submit. You can also grant Occasional Users privileges to run guest-level reports against auxiliary tables, search for auxiliary items, and view items in auxiliary tables. Occasional Users can also update their user profiles.

- **Regular User**

  Grants the potential for full access to your system. Each user's privilege set can be customized as needed.

- **API/Script**

Allows integration products to run scripts and other automated services, including orchestrations and the SBM API. Accounts granted API/Script access can be granted the same privilege and preference set as accounts granted Regular User access; however, because accounts with API/Script access cannot log on to user interfaces, such as Serena Work Center and the SBM User Workspace, some privileges and preferences may be irrelevant.

Note: Certain user preferences are required for accounts with API/Script access. When you grant API/Script access to a user account, required preferences are set automatically. You should not modify these settings.

- **Managed Administrator**

  This access type grants users Managed Administrator access. This enables you to limit the administrative capabilities of these users. For details, refer to Chapter 6: Managing Administrators [page 255].

On-demand Product-access Types

- **None**

  No product access granted. This access type can be used to set up general information for an account before assigning an access type. None can also be used to remove product access.

- **Regular User**

  Grants the potential for full access to your system. Each user's privilege set can then be customized as needed.

- **Occasional User**

  Allows users to be assigned to the Submitters group and other groups with Occasional User access. These users can submit primary items, own primary items they submitted, update and transition primary items that they own or submitted, run guest-level reports, and update their user profile. Occasional users can also be granted privileges to view all field sections for primary items they submitted.

- **Managed Administrator**

  This access type grants users Managed Administrator access. This enables you to limit the administrative capabilities of these users. For details, refer to Chapter 6: Managing Administrators [page 255].

For a list of privileges associated with available groups, refer to Groups for On-Demand Customers [page 176].

About User Accounts

Each user in the system must have an account that at a minimum includes a login ID, name, and product-access level. Typically, each user account is assigned roles and group membership, which provides their privilege set and notification subscriptions.

SBM offers several mechanisms for adding user accounts to your system. You can:

- Manually add multiple user accounts in SBM Application Administrator using the steps in Adding Users [page 145].

- Use the "copy" feature to quickly add a single user based on another user account. For details, refer to Copying User Accounts [page 148].
- Import multiple users at once using a spreadsheet exported from an LDAP store or that you manually created. For details, refer to About User Import [page 350]
- Import or update users and contacts from an LDAP store. For details, refer to Importing Users and Contacts From LDAP [page 359].

On-demand customers can add as many users as their account allows. Once the limit is reached, an error message appears and no more users can be allocated until this limit is increased.

On-premise customers who use seat licenses can add users until the number of seats available is exceeded for a specific product-access type. Once you reach this number, you can add users to the system, but you cannot grant product access to them until you add more seats.

Once user accounts are established, use roles or groups to effectively manage privilege sets, notification subscriptions, and more. For details, refer to About User Management [page 141].

Working With User Accounts

The following sections provide guidance for managing user accounts:

To learn more about managing administrators, refer to Chapter 6: Managing Administrators [page 255].

Adding Users

The following steps explain how to add individual user accounts in SBM Application Administrator. While possible, this is not the most efficient way to add new users to your system. For alternatives, refer to About User Accounts [page 144].

To manually add user accounts:

1. From the **Administrator Portal**, do one of the following:
   - Hover over the **Users** icon, and then click the plus sign.
   - Click **Users** icon, and then click **Add**.

2. Provide login information and product access to the user. For details, refer to General User Settings [page 158].

   Note: If your system uses seat licenses and you have exceeded the number of seats available to you for a specific product-access type, you can add users to the system, but you cannot grant product access to them until you add more seats.

3. Save your changes, and then repeat these steps for each account you need to create.

4. Follow the steps in Comparing and Changing User and Group Accounts [page 146] to apply the remaining settings to multiple accounts at once.

Comparing and Changing User and Group Accounts

When you edit multiple user and group accounts, you can compare the differences between those accounts. This helps you quickly determine which properties need to change for each account. In most cases, you can change properties as you compare changes. For example, you can edit several users, compare their role assignments for specific projects, and then change those assignments for all of the users or for individual users.

To compare settings for multiple user or group accounts:

1. From the **Administrator Portal**, select the **Users** or **Groups** icon.

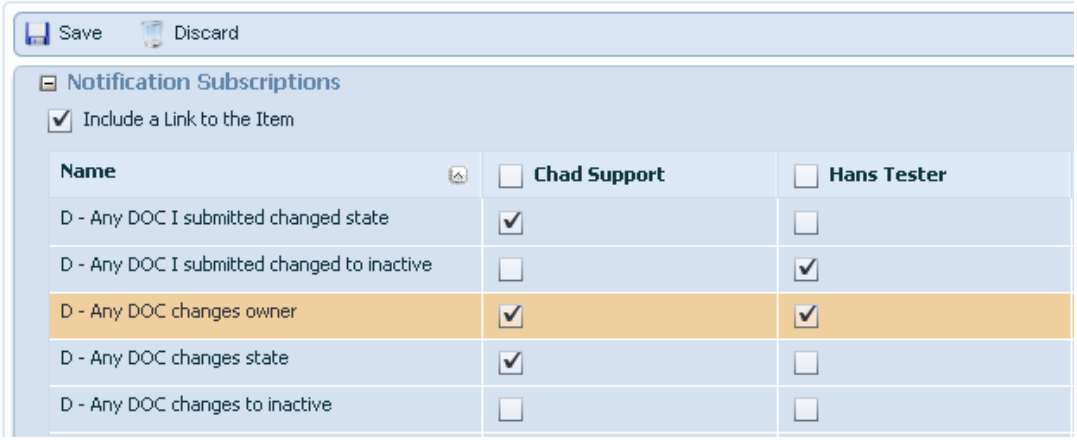
2. Select one or more accounts.

   Tip: To select accounts on multiple pages, use the CTRL or SHIFT keys to select users or groups on one page, and then use the navigation buttons at the bottom of each page to move to other pages. Use the CTRL or SHIFT keys to select users or groups on these pages. A count of selected accounts is available at the bottom of the **Users** view.

3. Click **Details**. The **Product Access** page opens, with **All** selected. Each user or group is listed below the toolbar in reverse order of selection, as shown in the following figure.

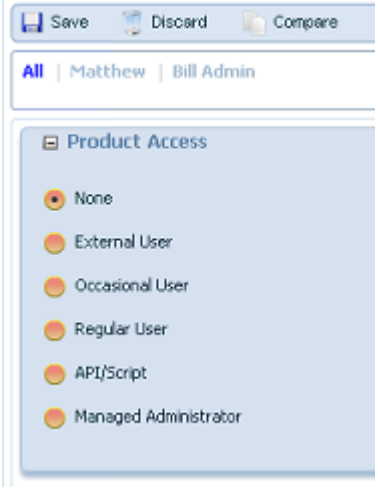
4. Compare and change accounts as needed, using the following information for guidance.

   - **Side-by-side comparisons** - Compare and change role, group membership, privileges, and notification subscriptions in a grid format, as shown in the following figure.



Note: If you select a role already associated with a group for a specific user, you are adding the role at the user level, but you are not changing the user's association assigned through group membership.

- **Compare feature** - Use the Compare feature to compare and change general settings and preferences for users and groups and password settings for users. If these settings differ for the selected user or group accounts, the differences are highlighted in red, as shown in the following figure.



You can:

  - Change a setting, but doing so applies the change for all users.
  - Select each user individually to view and change settings as needed.

5. For guidance on individual settings, refer to:
   - General User Settings [page 158]
   - Role Settings for Users and Groups [page 160]
   - Membership Settings for Users and Groups [page 160]
   - About Privileges [page 180]

- About Preferences [page 242]
- Notification Subscriptions for Users and Groups [page 162]
- User Channel Settings [page 162]
- User Password Settings [page 163]
- User Reference Settings [page 165]
- Delegation of Items View [page 167]

6. Save your changes.

Copying User Accounts

Copying user accounts enables you to easily add users based on a "template" account. The copied user account contains all of the privileges, preferences, application settings, and options of the template account, except for personal data, such as login ID, password, and e-mail address. Preferred projects set for the template account are copied to the new account.

To copy user accounts:

1. From the **Administrator Portal**, select the **Users** icon.
2. Navigate to or search for the user account that you want to copy.
3. With the account selected, click **Copy**.
4. Provide login settings for the user. For details, refer to Login Settings [page 158]
5. Save your changes.
6. Modify settings on other pages as needed, and then save your changes.

Deleting User Accounts

To protect historical information, user accounts can be deleted and restored as needed. Users can continue to view data pertaining to deleted users, such as Change History records and data provided by these users, but be aware that some areas of your system may need to be modified when you delete user accounts.

Before you delete user accounts:

- Use the **References** feature to view application settings, such as notification subscriptions and fields where the user is set as a default value. You can then permanently transfer these settings to a different user. For details, refer to Transferring Application Settings to Another User [page 151].
- Consider the role deleted users played in any orchestration or Web service data mapping or SBM AppScript, and manually modify these elements as needed.

After you delete user accounts:

- When you delegate a default value setting to another user, existing primary items are not automatically updated to reflect this change. Use reports to find and update existing primary items as needed.

- If you choose not to update items where a deleted user is selected as a field value, users must select an active user when they update or transition items.

To delete a user account:

1. From the **Administrator Portal**, select the **Users** icon.
2. Navigate to or search for the user account that you want to delete.
3. Click **Delete**.

Note: Administrators cannot delete their own accounts.

Restoring Deleted User Accounts

To restore a deleted user account:

1. From the **Administrator Portal**, select the **Users** icon.
2. Select the **Show Deleted Users** check box.
3. Navigate to or search for the user account that you want to restore.
4. Select the user, and then click **Restore**.

Enabling Disabled User Accounts

Depending on settings made in SBM System Administrator, user accounts may be disabled after a specified number of failed login attempts. The following steps explain how to enable these accounts.

To enable disabled user accounts:

1. From the **Administrator Portal**, select the **Users** icon.
2. Navigate to or search for the disabled user account.
3. Select the account, and then click **Enable**.

Managing External Users

External users can be granted a minimal set of privileges that enables them to submit and view certain items and run reports that are created for them. For a list of privileges available to external users, refer to the privilege tables in About Privileges [page 180]. For information about external users and system tables, refer to Privilege Behavior for System Tables [page 241].

Self-registration of external users is also available for on-premise customers. This feature is enabled in SBM System Administrator.

Automatically Adding External Users to a Group

You can designate a group to which new external users should automatically be added. This enables you to quickly grant access to customers and others who need limited access to your system. This feature is also used for self-registration of external users, which is enabled in SBM System Administrator. *(On-premise only.)*

Note: Only one group in your system can be set as the group to which external users can be added.

To automatically add external users to a group:

1. From the **Administrator Portal**, select the **Groups** icon.
2. Create or edit a group with External User product access.
3. Select the **Add New External Users Automatically** check box.
4. Save your changes.

Setting Up Reports for External Users

External users can run guest-level reports that contain primary items submitted by the external user or by other contacts from the external user's company. External users must be granted privileges to view items in a particular project, as well as to run guest-level reports. In addition, guest-level reports appropriate for external users must be created in a project that external users can access.

External users can also run built-in reports if they are granted privileges to view primary items. Privileges determine the information returned by the built-in report.

Note: By default, the home page report for external users who have privileges to submit items is set to the "All Items I Submitted" built-in report. Items from the projects they can submit into appear in the report.

To set up reports for external users:

1. Prepare the workflow associated with the project from which external users will generate reports. External users can only view fields in the **User Fields** section, so make sure fields pertinent to users are placed in this section. In addition, move fields you do not want external users to view into a different section. For details, refer to *SBM Composer Guide*.
2. Verify that external users are granted the following Item privileges for the project associated with the workflow you prepared in Step 1:
   - **View Items If Submitter**

     Grant this privilege to enable external users to view items they submitted. Users must also be granted the "Submit New Items" privilege.

   - **View Item If Contact**

     Grant this privilege to enable external users to view items for which they are selected in a *Contacts* relational field based on the system *Contacts* table. This privilege enables them to view items submitted by others users as long as they are selected as a contact and their *Contact* record is associated with their user

account. This setting is located on the **General** tab when you add or edit a user account.

- **View Item If Contact's Company**

  Grant this privilege to enable external users to view items for which their company is selected in a *Companies* relational field based on the system *Companies* table. Items may include those submitted by the external user, those submitted by external users from the same company, or items submitted by other users as long as company is set to that of the external user. In addition, users' contact records must be associated with user accounts. This setting is located on the **General** tab when you add or edit a user account.

3. Grant the "Run Guest Level Reports" Report privilege for the project or projects you want external users to run reports against.

Transferring Application Settings to Another User

References enable you to view and transfer certain application settings from one user to another. For example, if a user leaves your organization, you can use this feature to transfer *User* field selections and default values, role assignments, and other settings to a different user.

Use references to transfer the following application settings:

- **Field Selections**

  This is useful for transferring selections for all *User* and *Multi-User* fields from one user to another.

- **Default Values for *User* and *Multi-User* Fields**

  This is particularly useful for transferring ownership of items in a particular state to a different user. For example, newly submitted items may be routed to a manager who is set as the default value for a field during an "Assign" transition. You can use references to change this default value to a different manager. The setting can be transferred for workflows or projects.

- **Field Dependencies**

  This enables you to see where a user is defined as part of a field dependency so you can transfer those settings to another user. For example, selections in a *Manager* field may limit the selections in an *Employee* field. If a manager leaves the company, you can replace her with another manager so that the dependency remains intact.

- **Notification Subscriptions**

  This ensures that critical information continues to be sent to an appropriate user if someone leaves your organization.

- **Groups**

  When you transfer group membership, all privileges, role assignments, and notifications are transferred to the new user. In addition, if groups are used to populate *User* or *Multi-User* fields, transferred users are available as selections for these fields.

- **Roles**

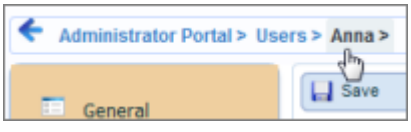
All privileges associated with roles are transferred to new users. In addition, if roles are used to populate *User* or *Multi-User* fields, transferred users are available as selections for these fields.

Use the **References** page to view these application settings for a user. You can then transfer the individual settings multiple users, or use the "Replace User" feature to transfer all of the listed settings to a single user at once.

Transferring Settings to a Single User

To transfer one user's application settings to a single user:

1. In SBM Application Administrator, select the **Users** icon.
2. Search for or navigate to the user who is assigned application settings that need to be transferred to another user, and then click **Details**.
3. Select the **References** tab.
4. Select the **Replace user** button.
5. Search for or navigate to the user to whom settings will be transferred.
6. Select the user, and then click **OK**.
7. You will be warned that replacing the application settings is irreversible. Click **Yes** to continue.
8. Click the **Log** tab to view a list of the settings that were transferred. You can copy this log to the clipboard so you can paste it into another document. For details, refer to Replace User Log Page [page 166].
9. Click the original user's name in the breadcrumb to return to the **References** page.

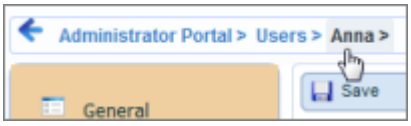


The list of application settings for the original user should be empty.

Transferring Settings to Multiple Users

To transfer one user's application settings to multiple users:

1. In SBM Application Administrator, select the **Users** icon.
2. Search for or navigate to the user who is assigned application settings that need to be transferred to another user, and then click **Details**.
3. Select the **References** tab.
4. Double-click a setting. For example, to transfer a notification subscription to another user, double-click it.
5. Change the setting to transfer it to another user. For example, change the notification subscription, and then save your changes.
6. Select the original user's name in the breadcrumb to return to the **References** tab:



7. Repeat these steps for all settings that need to be transferred.

Tips for Working With References

- When you delegate a default value setting to another user, existing primary items are not automatically updated to reflect this change. Use reports to find and update existing primary items as needed.
- Review the list of references carefully before delegating them to another user to make sure that the changes apply to the user's product-access level and responsibilities in your organization.
- Managed administrators can only transfer settings for users and application settings for which they have been granted administrative privileges. In addition, they cannot use the "Replace User" feature unless they have privileges to manage the original and replacement users and all application settings assigned to the original user.

Delegating Primary Items to Another User

You can use the out-of-office feature to delegate active primary items owned by one user to another user for a specific time period. This is useful for ensuring that items are addressed during vacation periods, holidays, or other times when users may be unavailable.

For example, Nancy, an IT support technician, may own several outstanding requests for service. She can create an out-of-office entry to delegate these items to Chad, another support technician, for her two-week vacation period. Once the entry is active, the outstanding items are delegated to Chad, who is now responsible for them, along with incoming items that may normally be assigned to Nancy.

Delegations are recorded in the State Change History and Change History sections for each item. The user who created the out-of-office entry is reflected in this audit trail.

Once the out-of-office entry expires, all delegated items are returned to Nancy, except for items that Chad has moved to another state or to a different owner.

Considerations for Item Delegation

Consider the following information before delegating items to another user:

- Users can delegate their items to another user, or administrators can delegate items on behalf of users. The user who created the out-of-office entry is listed on the **Delegation of Items** page.
- Delegation only applies to fields defining primary ownership of items. For example, an *IT Technician* field may be set as the owner in an "Assigned" state. The system will update this field based on out-of-office entries, but it will not modify fields used solely for data collection, such as *Submitter* or *Last Modifier*.
- Use State Change or Change History reports to view delegation actions for specific projects or sets of users.

- By default, the system checks for items to be delegated every 30 minutes. Administrators can modify this setting, however. For details, refer to the Knowledgebase at serena.com.
- You can only delegate one user's items to one other user for each project. For example, you can delegate Chad's items to Nancy in Project X, but not to Nancy and Samir in the same project. You can, however, delegate Chad's items in Project X to Nancy and items in Project Z to Samir.
- If you specify delegation for parent project, items in sub-projects are delegated as well. You must set up separate out-of-office entries for sibling projects, however.
- You cannot set out-of-office entries for the base project.
- Users to whom items are delegated must have privileges to own items in the selected parent project.
- Active out-of-office entries cannot be deleted, and only the end date can be modified.

Creating Out-of-Office Entries

Users and administrators open the out-of-office delegation settings differently, but the steps for creating entries are the same.

To open delegation settings from the SBM User Workspace:

1. Click your user name in the upper right corner.
2. Select the **Advanced** tab.
3. Click the **Edit** button next to **Delegation While Out of Office**.

To open delegation settings from Serena Work Center:

1. Click your user icon in the upper right corner.
2. Select **Out Of Office**.

To open delegation settings from SBM Application Administrator:

1. From the **Administrator Portal**, select the **Users** icon.
2. Search for or navigate to the user for whom an out-of-office entry will be created, and then click **Details**.
3. Select the **Out Of Office** tab.

To create out-of-office entries:

1. On the **Delegation** view, click **Add**.
2. Select start and end dates and times for which items should be delegated. By default, times are set at 00:00, which represents midnight of the selected day.

Tip: To cancel a delegation, set the end date and time to the current time.

3. Search for or navigate to the project that contains items to be delegated.
4. Select the **Delegate items in sub-projects too** check box to delegate items in the selected project and its sub-projects.
5. Click **Find** to search for a user to whom items will be delegated. Only users who have privileges to own items in the selected project are listed.
6. Save your changes.

User Settings

The following sections describe options and information available for user accounts.

Users View Settings

The **Users** view lists the users you have privileges to administer. Use this view to search for users and to add, edit, copy, and delete user accounts.

Finding and Sorting Users in the List

By default, users are sorted alphabetically by login ID. Depending on the number of users in your system, you may need to navigate the list to find users. To navigate the list of users:

- Click column headers to sort fields by login ID, user name, status, product-access type, or memo.
- Search for users by login ID or user name.
- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Tip: To select users on multiple pages, use the CTRL or SHIFT keys to select users on one page, and then use the navigation buttons at the bottom of each page to move to other pages. Use the CTRL or SHIFT keys to select users on these pages. A count of selected users is available at the bottom of the **Users** view.

Use these options to include various types of users in the list:

- Show Deleted Users
- Show External Users
- Show Occasional Users

Users View Options

The following options enable you to work with users in the list:

- **Add**

  Click to add a user account. For details, refer to Adding Users [page 145].

- **Details**

  Select one or more users, and then click to edit them. For details, refer to Comparing and Changing User and Group Accounts [page 146].

- **Delete**

  Select one or more users, and then click to delete the accounts. For details, refer to Deleting User Accounts [page 148].

- **Restore**

  This button is enabled when the **Show Deleted Users** check box and a deleted user is selected. Click **Restore** to restore the deleted user.

- **Enable**
  This button is enabled when users have exceeded a specified number of login attempts and their accounts have been disabled. To enable these accounts, select a disabled user in the list, and then click **Enable**.

  Note: Use SBM System Administrator to set the number of allowed login attempts before user accounts are disabled. *(On-premise only.)*

- **Copy**

  Select a user, and then click to copy the account. For details, refer to Copying User Accounts [page 148].

- **Import**

  Click to open the Import Users utility. For details, refer to About User Import [page 350].

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

User Information

The following information is available for each user:

- **Login ID**
- **Name**
- **Status**

  If empty, the user is active. Deleted users are listed is the **Show Deleted Users** check box is selected.

- **Access Type**

  Indicates each user's assigned product-access level.

- **Memo**

  Information from the **Memo** box for each user is shown, it available.

- **Out of Office**

  Lists scheduled and active out-of-office entries for each user. For details, refer to Delegating Primary Items to Another User [page 153].

User Counts and Seat License Usage

On-premise customers can view user counts and seat license usage details for their system at the bottom of the **Users** view.

Accounts with Regular User or Managed Administrator product access are listed as "Regular Users." Accounts with Occasional User product access are listed as "Occasional Users." Accounts with External User product access are listed as "External Users."

For systems using seat licenses, the number of available seat licenses is provided. Because the number of user accounts in your system cannot exceed the number of seat licenses, this count helps you monitor seat license availability.

Note: Requestor seat licenses are consumed by users with External User product access.

General User Settings

The following options are available on the **General** page when you add or edit user accounts.

Note: When you edit multiple user accounts, the **General** page opens to the Product Access section for all selected users. Click **Compare** to view general information for all users, or click each user's name to view and change information and options for that user. For details, refer to Comparing and Changing User and Group Accounts [page 146].

Login Settings

- **Login ID**
  Provide a unique name with which the user will log in to the system. The login ID can contain up to 64 characters.

  Note: For on-demand users, the login ID must be the user's e-mail address.

- **Password**

  Provide a password of no more than 36 characters for the user based on system password criteria. On-premise customers can set system password criteria in SBM System Administrator. You can override system system settings on the **Passwords** page. For details, refer to User Password Settings [page 163].

- **Re-enter Password**

  Provide the password again.

- **Name**

  Provide the user's display name in the user interface and as values for user-type fields. The name can contain up to 64 characters.

  If you plan to create *Contacts* records for users, note that the first word in the name is added to the *First Name* field, the second word (if applicable) is added to the *Middle Name* field, and the last word is added to the *Last Name* field.

- **Title**

  Provide an optional title for the user account.

- **Telephone**

  Optionally, provide a phone number for the user.

- **Mobile Phone**

  Optionally, provide a mobile phone number for the user.

- **Memo**

  Provide an optional description for the user account. This information appears in the **Memo** column on the **Users** view.

- **Preferred Contact Method**

Select the user's preferred contact method. This enables users to know which method to use to contact the user.

- **E-mail Address**
  Provide an e-mail address to:
  - Enable the user to receive e-mail notifications.
  - Enable e-mail links and ease the process of sending e-mails based on the user's SBM account name.
  - Enable the system to verify that e-mail submissions and e-mail messages sent from external mail clients are received from users with valid user accounts.

  Separate multiple e-mail addresses with a semicolon. (The number of characters cannot exceed 128 unicode characters.) E-mail notifications and messages sent from items are mailed to each provided address. The first provided e-mail address is designated as the "from" address.

- **E-mail Aliases**

  Provide an e-mail address to enable the system to verify that e-mail submissions and e-mail messages sent from external mail clients are received from users with valid user accounts. E-mail messages are never sent to the provided aliases; they are used solely for verification. Separate multiple e-mail addresses with a semicolon. (The number of characters cannot exceed 128 unicode characters.)

- **E-mail Notification CC:**
  Provide the login IDs or user names of those who should receive copies of e-mail notifications on behalf of the user. Separate multiple login IDs or user names with semicolons, up to 2,000 unicode characters.

  Note: Users specified in the CC list do not receive copies of e-mail messages sent from SBM items.

- **Login Creation Date**

  Shows the date and time the user account was created.

- **Last Login Date**

  Shows when the user last logged into the system. If the user has never logged in, this property is empty.

Product Access Settings

You must assign a product-access type to each user. For details, refer to Product-Access Types [page 143]

Note: Administrators cannot change their own product-access type.

Associated Contact Settings

You can automatically create Contact records that contain a user's name, telephone number, and e-mail address. When you make changes to these fields in Application Administrator, those changes are also applied to the user's Contact record. These records

are stored in the system *Contacts* table and can be accessed using the Auxiliary Data feature. For details, refer to About Auxiliary Data [page 389].

- **Create/Update Record for User**
  Select this option to create a Contact record for the user or to update information in the record's *Name*, *Telephone*, and *E-mail* fields.

  Note: Contact records are automatically created for new users with External User and Occasional User product access. If necessary, you can delete these records later.

- **Don't Update Contact Record**

  Select this option to prevent the system from updating the user's Contact record based on changes you make here.

- **Delete Associated Contact Record**

  Select to delete the user's existing Contact record. This option is not available for external users. Note that you can also delete a Contact record using the using the Auxiliary Data feature; however, the corresponding user record is not deleted unless the record belongs to an External user. In this case, both the external user account and corresponding Contact record are deleted.

Role Settings for Users and Groups

Use the **Roles** page in the **Users** or **Groups** views to make role assignments for one or more users or groups in one or more projects.

For guidance, refer to:

- About Roles [page 168]
- Assigning Users to Roles [page 171]
- Assigning Groups to Roles [page 171]

The following options are available on the **Roles** page when you are adding or editing user or group accounts:

- **Projects**

  Navigate to or search for the project for which you want to assign roles, and then select the project.

- **Roles**

  Shows the name provided for the role in SBM Composer. Select the check box for each user or group to enable the role; clear the check box to return to the inherited status.

- **Changes**

  Role changes for the users or groups you are editing are listed in this section. This enables you to save your changes at one time rather than incrementally. Review the list of changes before you click **Save**.

Membership Settings for Users and Groups

Use the **Membership** page in the **Users** or **Groups** view to assign group membership.

You can only assign users to groups with the same or a lower level of product access. For example, you cannot assign users with External User access to a group with User product access.

Important: When you add members to an existing group, group preferences are not automatically applied. If you want to set preferences for new members, you must edit the group and then apply preferences on the **Group Preferences** tab. For details. refer to Applying Preferences to New Group Members [page 175].

The following options are available on the **Membership** page when you are adding or editing user accounts:

- **Group Access Type**

  Filter the list of groups by product access type. For details, refer to Product-Access Types [page 143].

- **Search**

  Filter the list of groups by searching for them by name. Searches are case-insensitive.

- **Sorting**

  By default, groups are listed alphabetically. Click the headings for individual users to sort the list by membership assignments.

- **Membership**

  All groups are listed, but only those with a product-access type compatible with the user's type are enabled for selection.

- **User Name**

  Indicates the user accounts you are editing. Select the check boxes to assign group membership to the users.

The following options are available on the **Membership** page when you are adding or editing group accounts:

- **User Access Type**

  Filter the list of users by product access type. For details, refer to Product-Access Types [page 143].

- **Search**

  Filter the list of users by searching for them by user name or login ID. Searches are case-insensitive.

- **Sorting**

  By default, users are listed alphabetically. Click the group headings to sort the list by membership assignments.

- **Users**

  All users are listed, but only those with a product-access type applicable to the group are enabled for selection.

- **Group Name**

  Indicates the groups you are editing. Select the check boxes for users to assign membership.

Notification Subscriptions for Users and Groups

Use the **Notifications** page to subscribe one or more users or groups to notifications. You can subscribe users to notifications when you are editing user or group accounts, but the users and groups must be allowed to subscribe to the notification. For details, refer to Notification Subscriptions [page 296].

Note: Users or groups with External product access cannot be subscribed to notifications on this page, but you can specify that they always receive certain notifications. To do so, edit the notification and select the **Subscribe** option for the External user or group.

Finding and Sorting Notifications

By default, notifications are sorted alphabetically by name and may be listed across multiple pages. System-provided notifications are initially prepended with the first letter of up to three words from the workflow name.

To navigate the list:

- Click the **Name** column headers sort notifications.
- Search for notifications by name.
- Use the arrows and number links at the bottom of the page.

Subscription Options

The following options are available on the **Notifications** page when you are editing user or group accounts:

- **Include a Link to the Item**

  For user accounts, select this check box to include a link to the item in e-mail notifications that use the `$IF(VIEWLINK)` e-mail template tag. For details, refer to Notification Tags [page 445].

- **Name**

  Lists the available notifications available.

- **Users and Groups**

  The user or group accounts you are editing are listed. Select the check box for each notification to subscribe to users or groups.

  Note: Users who are members of multiple groups subscribed to a notification receive only one e-mail message per notification per cycle.

User Channel Settings

Use the **Channels** page to enter a user's recipient ID. The recipient ID is used to send notifications directly to the user. For details, refer to About Channels [page 395].

Entering Channel Parameters

To add a recipient ID for a particular channel:

1. Select a channel in the **Name** drop-down list.
2. Enter the recipient ID in the **Value** field. For example, in order to send Bill notifications through a user channel like Gtalk, enter his Gmail e-mail address here.
3. Click **Save** to save your changes.

The user is now associated with a recipient ID that can receive notifications via the selected channel.

User Password Settings

The **Passwords** page enables you to override system password settings specified in SBM System Administrator. You can override settings for individual users or a set of users.

If you are modifying multiple accounts, click **Compare** to view the different settings for each account. For guidance, refer to Comparing and Changing User and Group Accounts [page 146].

Password overrides apply for on-premise customers using SBM authentication or LDAP authentication first, and then SBM. In the latter case, user passwords must match in SBM and LDAP.

On-demand customers can also override password options.

To override password options for users, clear the **Use System Settings** check box, and then set the following options as needed:

- **Expiration**
  - **Password Expires**

    Select to enable validity settings, and then select the number of days for which passwords are valid.
  - **Password Does Not Expire**

    Select to prevent passwords from expiring. This setting also enables users to log into the system without a password.
  - **Cannot Be Changed**

    When you prevent passwords from expiring, you can select this option to prohibit users from changing their passwords.
- **Validity**
  - **Password Valid for n Days**

    Specify, in days, how long passwords are valid and after which users must create new passwords. The default expiration is one day, and the accepted range is one to 999 days.
  - **Password Expires In**

    Indicates the number of days before the user's password expires.

- **Reset**

  Click this button to reset the timer used to calculate expiration. For example, if the password expiration period is set to 60 days, you can click this button after 55 days to reset the expiration period.

- **Requirements**
  - **No Minimum Length**

    Selected by default, this option does not set length restrictions on passwords. Passwords can have a maximum of 36 characters, however.

  - **Minimum Length of n Characters**

    Select to require users to create passwords with a minimum number of characters.

  - **No Special Characters Required**

    Selected by default, this option does not require users to include special characters in their passwords.

  - **Require**

    Select to require users to include a specified number of special characters in their password. Special characters include punctuation marks, the percent sign, and currency symbols.

  - **No Historical Password Validation**

    Selected by default, this option does not require users to create a sequence of unique passwords. Users cannot use the same password when other settings on this page require them to change their password, however.

  - **Cannot Match Last n Passwords**

    Select this option to require users to create a specific number of unique passwords.

  - **Must Include a Number**

    Select this option to require at least one number in passwords.

  - **Must Include an Uppercase Letter**

    Select this option to require at least one uppercase letter in passwords.

  - **Must Include a Lowercase Letter**

    Select this option to require at least one lowercase letter in passwords.

    Note: Depending on the version of SBM you are using, the last two options may not apply and should not be selected for best results. For example, if you are using the Japanese version, do not select the **Must Include an Uppercase Letter** or **Must Include a Lowercase Letter** check boxes.

User Reference Settings

Use the **References** page to transfer application settings from one user to another. For details, refer to Transferring Application Settings to Another User [page 151].

The following settings are available on the **References** page:

- **Replace User**

  Click this button select a user to whom all of the settings on the **References** page will be transferred. For details, refer to Transferring Settings to a Single User [page 152].

  Note: To transfer settings to more than one user, double click each setting and modify it as needed. For details, refer to Transferring Settings to Multiple Users [page 152].

- **Field Selections**

  Lists fields for which the user is a selection, along with the workflows where the selection is used.

- **Field Defaults**
  Lists the fields for which the user is selected as a default value in a *User* or *Multi-User* field, along with:

  - **Workflow Name**

    Listed if the default value is set for a workflow.

  - **Project Name**

    List if the default value is set for a project.

  - **Hierarchy**

    Indicates the project hierarchy at which the default value was defined.

  - **Transition**

    Listed if the default value is defined for a transition.

- **Field Dependencies**
  Lists the fields and selections for which the user is defined in a dependency.

  - **Project Name**

    Lists the name of the project for which the dependency is defined.

  - **Independent Field Name**

    Indicates the independent field for the dependency.

  - **Independent Selection Name**

    Indicates the independent field selection for which the user is defined.

  - **Independent Field Name**

    Indicates the dependent field.

  - **Independent Default Name**

Indicates the default value for the independent field, if one is specified.

- **Notifications**

  Lists the notifications to which the user is subscribed, along with the application name, notification name, and notification action.

- **Groups**

  Lists the groups to which the user is assigned. Deleted groups are indicated in the status.

- **Roles**

  Lists the roles to which a user is assigned, along with the project and project path for which the assignment was made.

For details about delegating each of these application settings, refer to Transferring Application Settings to Another User [page 151].

Tip: Use the paging arrows at the bottom of each section to scroll through long lists. You can also search for fields, projects, notifications, roles, and groups by name.

Select User Page

Use the **Select User** page to search for and select a user to whom application settings should be transferred.

All users available to an administrator are listed.

CAUTION:

Because the setting transfer is irreversible, use care when selecting a user for this feature.

For details, refer to:

- Transferring Application Settings to Another User [page 151]
- User Reference Settings [page 165]

Replace User Log Page

A log is generated each time you use the Replace User feature to transfer all application settings to another user and includes the following information:

- User whose settings were replaced.
- User to whom settings were transferred.
- Date and time replacement was started.
- User who performed the replacement.
- Group transfers.
- Role transfers.

- Field selection, default value, and dependency transfers.
- Notification subscription transfers.

The log is overwritten after each replacement. To save log information, click the **Copy Log to Clipboard** button, and then paste the log information into a separate document.

Delegation of Items View

Use the **Delegation of Items** page to manage out-of-office settings. For details, refer to Delegating Primary Items to Another User [page 153].

The following settings are available:

- **Add**

  Click to add off-of-office entries.

- **Details**

  Select an entries in the list, and then click to edit it.

You can view the following information for each delegation:

- **Status**
  Indicates one of the following for the delegation period:
  - **Scheduled**

    Has not yet begun.

  - **Active**

    Is in progress.

- **Start**

  Indicates the start date and time for each entry.

- **End**

  Indicates the end date and time for each entry.

- **Delegate To**

  Indicates the user to whom primary items are delegated. This user must have privileges to own items in the delegation project.

- **Project**

  Indicates the project for which items are delegated. If you select a parent project, items in sub-projects are delegated as well.

- **Include Sub-projects**

  Indicates where items in sub-projects will also be delegated.

- **Application Name**

  Indicates the application for which items are delegated.

- **Created By**

Indicates the user who created the out-of-office entry.

Delegation Settings

Use this page to define setting for out-of-office entries. For details, refer to Delegating Primary Items to Another User [page 153].

- **Start Date**

  Select a start date and time for the out-of-office entry. You cannot modify start dates for active entries.

- **End Date**

  Select an end date and time for the entry.

  Note: Hours are in 24-hour format, with 00:00:00 representing midnight. Times are based on the system time zone of the user creating the out-of-office entry.

- **Delegate To**

  Click **Find** to search for a user to whom items will be delegated for the specified time period. This user must have privileges to own items in the delegation project, so you must first select a project.

  Click **Clear** to remove a user from the **Delegate To** box.

- **Delegate items in sub-projects too**

  Select this check box to delegate items in the selected project and all of its sub-projects.

- **Project**

  Search for or navigate to the project that contains primary items to delegate to the selected user.

About Roles

Roles are created in SBM Composer as part of an process app, which can comprise multiple applications. Roles can span the applications within the process app and serve two functions:

- Roles are a named collection of privileges. The privileges secure user actions and data access. For example, a role named User could be a collection of privileges suitable for someone to whom items are assigned but who has no administrative tasks. Someone with that role could be restricted from executing some transitions and from viewing fields in certain sections.

- Roles are a means to populate selection lists for *User*, *Multi-User*, and *Multi-Group* fields. You associate roles with these fields in SBM Composer, then assign users and groups to the roles in SBM Application Administrator.

Roles are distinct from groups, which are named collections of users. Administrators can use groups to identify a set of users based on criteria other than job function. A group could be created for a particular project, for example, or for a division within the company. You can assign roles to a group.

Users and groups are associated with roles for particular projects in Application Administrator.

Note: When groups or users are copied, role assignments are copied with them. Also, when groups or users are imported through LDAP using a template group or user, the role assignments associated with the template are copied to the new group or user.

Key Benefits

- Organizes privilege sets by function rather than by users.
- Provides consistency in privilege assignments based on function, such as "manager" or "service technician."
- Enables you to populate user-type fields at design time.

Working With Roles

SBM Application Administrator offers multiple methods for assigning users and groups to roles:

- **To manage role assignments in multiple applications** – Open the main **Roles** view from the **Administrator Portal**. For details, refer to Assigning Roles Across Applications [page 169].
- **To manage role assignments for specific projects** – Edit a project, and then select the **Roles** tab. For details, refer to Assigning Roles for Specific Projects [page 170].
- **To manage role assignments for groups in one or more projects** – Edit one or more groups, and then select the **Roles** tab. For details, refer to Assigning Groups to Roles [page 171].
- **To manage role assignments for users in one or more projects** – Edit one or more user accounts, and then select the **Roles** tab. For details, refer to Assigning Users to Roles [page 171].

By default, a group or user inherits the role assignment specified for the parent project. You can override this inheritance by enabling a user or group for a role in a child project; the role is then assigned to that user or group for the current project regardless of the selections made for parent projects.

Note: To ease role maintenance, consider assigning roles at a parent project. This ensures role assignments are inherited throughout the project hierarchy.

Assigning Roles Across Applications

Prerequisites:

Create roles for an application in SBM Composer, assign privileges to those roles, and then deploy the application.

The main **Roles** view enables you to quickly assign roles to users and groups for projects in multiple applications. For example, from one view, you can assign one set of users to

an "IT Technician" role in an IT Help Desk application and another set of users to an "Employees" role in a Time-off Request application.

To assign users and groups to roles for different applications:

1. From the **Administrator Portal**, select the **Roles** icon.
2. Use one of the following methods to find the project for which you want to associate roles to users and groups:
   - Navigate to the project from the list of applications on the left, following the steps in Navigating Projects [page 31].
   - Search for the project.
3. Select the project in the bottom pane and a role in the top pane, and then:
   - Click **User Assignment** to assign users to the role.
   - Click **Group Assignment** to assign groups to the role.
4. Navigate to or search for the user or group to assign to the role, and then:
   - Click **Enable** to enable the user or group for role.
   - Click **Inherit** to return to the inherited status, which is "disabled" if the role was not assigned for a parent project.

   Tip: You can select multiple users or groups in the list and assign them to the role at once. You can also filter the list of users and groups by status (Enabled or Disabled).
5. Save your changes.

Assigning Roles for Specific Projects

Prerequisites:

Create roles for an application in SBM Composer, assign privileges to those roles, and then deploy the application.

Use the **Roles** page in the **Projects** view to assign users and groups to roles for specific projects.

To assign users or groups to projects:

1. Edit a project, following the steps in Adding and Editing Projects [page 33].
2. Select the **Roles** tab.
3. Select a role, and then:
   - Click **User Assignment** to assign users to the role.
   - Click **Group Assignment** to assign groups to the role.
4. Navigate to or search for the user or group to assign to the role, and then:

- Click **Enable** to enable the user or group for role.
- Click **Inherit** to remove role status overrides for the project you are editing.

Tip: To see existing role assignments, filter the list of users and groups by status (Enabled or Disabled).

5. Save your changes.

Assigning Groups to Roles

Prerequisites:

Create roles for an application in SBM Composer, assign privileges to those roles, and then deploy the application.

Use the **Roles** page in the **Groups** view to make role assignments for one or more groups. You can assign roles for these groups in multiple projects.

For example, you can edit the Managers, Employees, and IT Technicians groups and assign each group to different roles in different projects as appropriate.

To assign groups to roles in projects:

1. From the **Administrator Portal**, select the **Groups** icon.
2. Select one or more groups in the list, and then click **Details**.

Note: If you are adding a group, click **Add Group**.

3. Select the **Roles** tab.
4. Navigate to or for search for a project in the **Projects** area, and then select the project.
5. In the bottom pane, select a role, and then select the check box under each group to enable the role for the group. If a role is already enabled for a group, clear the check box to return to the role's inherited status.
6. Repeat for each project, as needed. As you change role assignments, they are listed in the **Changes** area. This enables you to save your changes for multiple projects at one time rather than incrementally for each project.
7. Save your changes.

Assigning Users to Roles

Prerequisites:

Create roles for an application in SBM Composer, assign privileges to those roles, and then deploy the application.

Use the **Roles** page in the **Users** view to make role assignments for one or more users. You can assign roles for these users in multiple projects.

To assign users to roles in projects:

1. From the **Administrator Portal**, select the **Users** icon.
2. Select one or more users in the list, and then click **Details**.

   Note: If you are adding a user, click **Add User**.

3. Select the **Roles** tab.
4. Navigate to or for search for a project in the **Projects** area, and then select the project.
5. In the bottom pane, select a role, and then select the check box under each user to enable the role for the user. If a role is already enabled for a user, clear the check box to return to the role's inherited status.
6. Repeat for each project, as needed. As you change role assignments, they are listed in the **Changes** area. This enables you to save your changes for multiple projects at one time rather than incrementally for each project.
7. Save your changes.

About Group Accounts

Groups simplify user management by organizing sets of users. You can then assign these groups to roles, which are a set of application privileges. You can also subscribe user sets to notifications, apply an initial set of user preferences, and assign non-role-related privileges to group members.

Groups also simplify the process for populating *User*, *Multi-User*, and *Multi-Group* fields. After you assign a group to a role, the members of that group are valid values for these field types if the role was associated to the field in SBM Composer. After you create group accounts, you may want to review the selections for the *User*, *Multi-User*, and *Multi-Group* fields in your system. For details, refer to Values for User, Multi-User, and Multi-Group Fields [page 92].

Key Benefits

- Organizes sets of users.
- Enables you to assign sets of users to roles rather than one user at a time.
- Allows you to subscribe multiple users to notifications at one time.

Working With Groups

The following sections provide guidance for managing group accounts:

- Adding Groups [page 173]
- Comparing and Changing User and Group Accounts [page 146]

- Copying Groups [page 173]
- Deleting Groups [page 174]
- Applying Preferences to Groups [page 174]
- Groups for On-Demand Customers [page 176]
- About Privileges [page 180]

Adding Groups

Groups enable you to organize sets of users so that you can easily assign roles and notification subscriptions to multiple users at once. Groups also provide an easy way to maintain your system. Rather than make changes to multiple users, for example, groups enable you to make a single change, which is then made for each member of the group.

To add a group:

1. From the **Administrator Portal**, do one of the following:
   - Hover over the **Groups** icon, and then click the plus sign.
   - Click **Groups** icon, and then click **Add**.
2. Provide a name for the group, along with a product-access level. For details, refer to Product-Access Types [page 143].
3. Save your changes.
4. Select the **Roles** tab, and then assign groups to roles as explained in Assigning Groups to Roles [page 171].
5. Select the **Membership** tab, and then assign users to the group as explained in Membership Settings for Users and Groups [page 160].
6. Select the **Privileges** tab, and then assign privileges to the group for each page.

   Note: For best results, use roles to assign all application-related privileges to groups. Privileges on the **System** page and administration privileges can only be granted to users or groups, with groups being the preferred mechanism.
7. Select the **Notifications** tab, and then subscribe group members to notifications as explained in Notification Subscriptions for Users and Groups [page 162]
8. Save your changes.

Copying Groups

Copy group accounts to quickly and easily create groups with identical privilege sets, role assignments, preferences, and notification subscriptions. You can then tailor the group as needed.

To copy a group account:

1. From the **Administrator Portal**, select the **Groups** icon.

2. Search for or navigate to the group you want to copy, and then click **Copy**.
3. Provide a unique name for the group, and if desired, description in the **Memo** box.
4. Modify role assignments, privileges, notification subscriptions, preference, and membership as needed.
5. Save your changes.

Deleting Groups

To protect historical information, groups can be deleted and restored as needed. When you delete a group, all role, membership, privilege, and notification subscriptions are removed for members of the group.

To delete a group:

1. From the **Administrator Portal**, select the **Groups** icon.
2. Search for or navigate to the group you want to delete.
3. Click **Delete**.

Restoring Deleted Groups

When you restore a deleted group, all role, membership, privilege, and notification subscriptions are restored for members of the group.

To restore a deleted group:

1. From the **Administrator Portal**, select the **Groups** icon.
2. Select the **Show Deleted Groups** check box.
3. Search for or navigate to the deleted group you want to restore.
4. Click **Restore**.

Applying Preferences to Groups

Use the **Group Preferences** page to apply user preferences to group members. You can:

- Choose to apply only certain preferences to group members, leaving others intact.
- Exclude preference changes for specific users.
- Apply preferences to one or more groups.

When applying preferences to groups, be aware that:

- Preferences are not automatically applied to new members you add to existing groups. For details, refer to Applying Preferences to New Group Members [page 175].
- Users who have privileges to modify their user profile can overwrite preferences you set for them. Likewise, changes you make to preferences overwrite changes made by users or earlier changes applied to a different group.

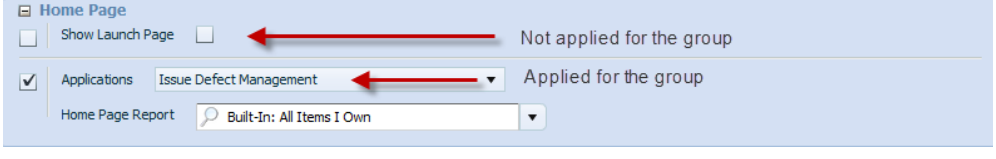
- Privileges may determine if preferences apply to group members. For example, if a member of a group does not have privileges to see a report set as the home page for the group, the preference is ignored for that member.

To set preferences for groups:

1. From the **Administrator** portal, select the **Groups** icon.
2. Select one or more groups, and then click **Details**.
3. Select the **Group Preferences** tab.
4. Select the tab that contains the preferences you want to change. Choices are:
   - Content
   - Display
   - Sections
   - Date/Time & Locale
   - Work Center

   For details on each preference, refer to About Preferences [page 242].
5. Apply preferences to the group by changing a setting or by selecting the check box next to each setting you want to change.

   Tip: Use the check boxes at the far left of each setting to determine if it was applied for the group.

6. Click **Save**.
7. A dialog box opens, showing you the list of users that are impacted by your change. To exclude specific users from the change, move them to the **Excluded Users** list.
8. Click **OK**.

Applying Preferences to New Group Members

To apply group preferences to new group members:

1. Edit the group.
2. Add new members to a group, and then save your changes.
3. Select the **Group Preferences** tab.
4. Optionally, adjust preferences for the group.
5. Click **Save**.

6. On the **Apply to Group Members** dialog box, verify that your new members are listed.
7. Click **OK** to save preferences for the full list of members, or move members to the **Excluded Users** list, and then click **OK**.

Groups for On-Demand Customers

The following groups are provided automatically for on-demand customers:

- Administrators
- Designers
- Users
- Submitters

These groups are configured with the privileges listed in the tables below. You can assign members to these groups, but you cannot modify other settings. Additional privileges can be assigned through roles in SBM Composer or by creating custom groups.

System Privileges				
Privilege	**Administrators**	**Designers**	**Users**	**Submitters**
Modify User Profile Settings	✔	✔	✔	✔
Log on as Another User	✔			
Remote Administration	✔	✔		
Create/Edit/ Delete Multi-Table Reports	✔	✔	✔	

Administrative Privileges		
Privilege	**Administrators**	**Designers**
Global Administration	✔	✔
Add/Edit/ Delete Users	✔	

Administrative Privileges		
Privilege	**Administrators**	**Designers**
Add/Edit Tables	✔	✔
Delete Tables	✔	
Add/Edit/ Delete Projects	✔	✔
Assign Roles	✔	✔
Edit General Properties	✔	✔
Edit Workflow	✔	✔
Edit Transitions	✔	✔
Manageable Groups	Administrators Designers Users Submitters	Designers Users Submitters
Deploy Process Apps to this Host	✔	✔
Delete Process Apps for this Host	✔	✔
Deploy to this Host from SBM Composer	✔	✔
Export Process Apps from this Host	✔	✔
Promote to this Host	✔	✔

Administrative Privileges		
Privilege	**Administrators**	**Designers**
Create, Edit and Delete Process App Endpoints for this Host	✔	✔
Create, Edit and Delete Process App Privileges	✔	

Group Settings

The following sections discuss group account settings:

- Groups View Settings [page 178]
- General Group Settings [page 179]
- Role Settings for Users and Groups [page 160]
- Membership Settings for Users and Groups [page 160]
- About Privileges [page 180]
- About Preferences [page 242]
- Notification Subscriptions for Users and Groups [page 162]

Groups View Settings

The **Groups** view lists the groups you have privileges to administer. Use this view to search for groups and to add, edit, copy, and delete user accounts.

Finding and Sorting Groups in the List

By default, groups are sorted alphabetically by name. Depending on the number of groups in your system, you may need to navigate the list. To do so:

- Click the column headers to sort fields by group name, status, product-access type, or memo.
- Search for groups by name.
- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.
- Select the **Show Deleted Groups** check box to add deleted groups to the list.

Tip: To select groups on multiple pages, use the CTRL or SHIFT keys to select groups on one page, and then use the navigation buttons at the bottom of each page to move to other pages. Use the CTRL or SHIFT keys to select groups on these pages. A count of selected groups is available at the bottom of the **Groups** view.

Groups View Options

The following options enable you to work with groups in the list:

- **Add**

  Click to add a group. For details, refer to Adding Groups [page 173].

- **Details**

  Select one or more groups, and then click to edit the group. For details, refer to Comparing and Changing User and Group Accounts [page 146].

- **Delete**

  Select one group, and then click to delete the group.

  Tip: When a group is deleted, it is not really deleted from the database. You can restore and rename a deleted account rather than add a new one.

- **Restore**

  This button is enabled when the **Show Deleted Groups** check box and a deleted group is selected. Click **Restore** to restore the deleted group.

- **Copy Group**

  Select one group, and then click to copy the group. For details, refer to Copying Groups [page 173].

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

General Group Settings

The following options are available on the **General** page when you add or edit a group account.

When you edit multiple group accounts, the **General** page opens to the Product Access section for all selected groups. Click **Compare** to view general information for all groups,

or click each group's name to view and change information and options for that group. For details, refer to Comparing and Changing User and Group Accounts [page 146].

- **Name**

  Provide a name of up to 64 unicode characters.

- **Memo**

  Provide an optional description for the group account. This information appears in the **Memo** column on the **Groups** view.

- **Product Access**

  You must assign a product-access type to the group. The product-access type of the group determines which users can be members of the group. For details, refer to Product-Access Types [page 143].

- **Add New External Users Automatically**

  For groups with External User access, select this check box to automatically add external users to the group. Only one group with External User access can be specified as the "automatic" group. For details, refer to Managing External Users [page 149].

About Privileges

User privileges determine which information and features are available to users, and the product-access level assigned to users and groups determines which privileges they can be assigned. The tables in the following sections indicate which privileges are available for each product-access level.

For details on product-access levels, refer to Product-Access Types [page 143].

For details on specific privileges and their related product-access levels, refer to:

- Privilege Inheritance Rules for Roles and Groups [page 180]
- System Privileges [page 181]
- Folder Privileges [page 189]
- Item Privileges [page 191]
- Field Privileges [page 203]
- Attachment Privileges [page 208]
- Note Privileges [page 213]
- Report Privileges [page 218]
- Table Privileges [page 224]
- Privilege Behavior for System Tables [page 241]

Privilege Inheritance Rules for Roles and Groups

Roles and groups offer a convenient way to grant privileges to multiple users at one time.

Privileges can also be granted to users in addition to those granted by their role or group membership, if needed. A user's total privilege set include all individual privileges plus all the privileges given to each role and group to which the user is assigned.

In general, all application privileges should be assigned through roles created in SBM Composer. System privileges for users and administrative privileges should be granted to groups, and users should be assigned to those groups.

Viewing Privilege Inheritance

To ease the process of granting privileges to users, privileges can be inherited through roles, groups, and projects. Folder privileges can also be inherited through the folder hierarchy established in SBM System Administrator.

Privileges that are inherited from a role, group, project, or folder are disabled. To determine how a disabled privilege was granted, hover over the check box to the right of the privilege name to view text indicating the role, group, parent item, or folder from which the privilege is inherited.

System Privileges

System privileges apply to features that support applications but are not specific to applications. Examples include granting the user or group the ability to modify their user profile settings or log in to the system as another user. The following table describes each system privilege and the product-access types for which it applies.

CAUTION:

Granting the Remote Administration privilege to those with Regular User product access grants administrative access to all applications and system-level settings. Because of this, use caution when granting the Remote Administration privilege to users. To control administrators' access, grant them Managed Administration product access, the Remote Administration system privilege, and the appropriate set of Managed Administration privileges for their responsibilities. For details, refer to Chapter 6: Managing Administrators [page 255].

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔			**Modify User Profile Settings** – Allows users to modify their user profile settings. Users who are not granted this privilege can modify their profile as follows: • **SBM User Workspace** **General** tab settings, including out-of-office delegation. • **Work Center** General **General**, **My Projects**, and **Feeds** tab settings.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Logon as Another User** – Allows users to log on to SBM User Workspace, SBM Application Administrator, and SBM Application Repository as another user without knowing that user's password. For best results, only grant this privilege to administrators who may need to view other user accounts for testing or troubleshooting purposes. When logged on as another user, administrators can perform all actions as the user they are logged in as. Any changes made to items in the SBM User Workspace as another user are recorded in the **Change History** section for each item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Remote Administration** – Allows users to connect to SBM System Administrator remotely and to SBM Application Administrator and Application Repository. When granted to users with Regular User product access, this privilege grants full administrative access to the system. For details, refer to Types of Administrators [page 255].  **Note:** Administrators cannot remove this privilege from their own account.
✔			✔	**Logon from SourceBridge** – Allows access to various version control integrations that can be used to associate source control actions with primary items and record version control history. This privilege also enables users to create, run, modify, and delete **Version Control Actions** reports.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔	✔	**View Public Problems & Resolutions** – Allows users to view problems and resolutions marked for public viewing in Knowledge Base folders they have privileges to view. For details on this privilege, refer to Privilege Behavior for System Tables [page 241].
✔	✔	✔		**View Your Contact Information** – Allows users to view their personal contact information in fields in the **Standard Fields** section of their *Contact* record and on their user profile card. For details on this privilege, refer to Privilege Behavior for System Tables [page 241].

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**Edit Your Contact Information** – Allows users to modify their personal contact information in fields in the **Standard Fields** section of their *Contact* record. Users must also be granted the **View Your Contact Information.** For details on this privilege, refer to Privilege Behavior for System Tables [page 241].
✔			✔	**Assign Contact External User Access** – Allows users to assign contacts external access to the system. For example, a customer support representative can assign a customer External access to the system from a Contacts table record. Users must also be granted privileges to view items in the system *Contacts* table. This privilege is granted on the **Tables** page. This privilege pertains only to system *Contacts* table records that are associated with user accounts. This setting is located on the **General** tab when you add or edit a user account.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**Run System Reports** – Allows users to run System reports. System reports allow users to view various aspects of the system configuration. They cannot be customized or deleted. There are nine system reports: Active Users, Group Membership, Item Locks, Current User Activity, Privileges, Project Fields, Users, Users Change History, and Workflow Fields.
✔			✔	**Create/Modify Pass-Through SQL Queries** – Allows users to create and modify advanced SQL reports that use pass-through SQL queries. In addition to this privilege, users must be granted the **Create/Modify Advanced SQL Queries** privilege for at least one project or auxiliary table. This privilege is located on the **Report** and **Table** privilege pages.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Create/Edit/Delete Multi-Table Reports** – Allows users to create, edit, and delete **Multi-Table** reports and to create reports from the **Global Search** feature. Users can only run **Multi-Table** reports and save **Global Searches** as reports in tables/ projects for which they have privileges to run reports.
✔				**Select Calendar for Hours of Operation** – Allows users to specify a calendar in their user preferences to calculate when notification escalations are sent. This ensures that notification escalations are only generated during the hours defined in the calendar. For details, refer to About Calendars [page 390].
✔			✔	**Connect using the API** – Allows users to connect to SBM using the C++ API. To obtain documentation about the SBM API, visit http://www.serena.com/support.
✔				**CC Scheduled Reports to Other Users** – Allows users to CC scheduled reports to other users and groups.

Folder Privileges

Folder privileges apply to public and Knowledge Base folders, which are created in SBM System Administrator. The following table describes each folder privilege and the product-access types for which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔	✔	**View Items in Folder** – Allows users to view items and URLs in the selected folder. For Knowledge Base folders that do not allow anonymous access, users must also be granted the "View Public Problems & Resolutions" privilege on the **System – Privileges** page to view public items or privileges to view items in the *Problems or Resolutions* table to view public and internal items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**Add Items to Folder** – Allows users to add items and URLs to the selected folder. This privilege also enables users to edit URLs added to the selected folder. The **Add Items to Folder** privilege also enables users to select the folder as a selection for *Folder* fields used in primary or auxiliary tables.
✔			✔	**Remove Items from Folder** – Allows users to remove items and URLs contained in the selected folder.

Item Privileges

Item privileges apply to primary items in the selected project. By default, the Base Project is selected. You can set privileges at the Base Project level and the privileges are inherited in any further derived projects. Ideally, however, privileges should be set for parent projects at the application level. To grant a unique set of privileges to a selected sub-project, clear the **Inherit All Parent Project's Privileges** check box.

Note: If you apply privileges to multiple projects while you are editing user or group accounts, your changes are added to the **Changes Log** in the upper right pane. You can then save your changes for multiple projects at one time rather than incrementally for each project.

The following information applies to item privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- The "Transition All Items," "Transition Item If Owner," "Transition Item If Secondary Owner", and "Transition Item If Submitter" privileges apply to all transitions in the selected project. To learn about restricting individual transitions, refer to Restricting Transitions [page 82].
- Users are available as e-mail recipients in the **Send E-mail** dialog box for items they have privileges to view. Groups who are assigned the "View All Items" privilege are available as e-mail recipients in the **Send E-mail** dialog box.
- Users can send e-mail messages from primary items they can view. For those messages to be attached to the item, however, users must be granted "Add Note" privileges.

The following table describes each item privilege and the product-access types for which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**Submit New Items** – Allows users to submit new items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Submit on Behalf of Another User** – Allows users to submit new items on behalf of other users.
✔				**Own Items** – Allows users to own or be assigned items.
✔	✔			**Own Items if Submitter** – Allows users to own items they submitted.
✔				**Delete Items** – Allows users to delete items.
✔				**View All Items** – Allows users to view all items.
✔				**View Item If Owner** – Allows users to view items they primarily own.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**View Item If Secondary Owner** – Allows users to view items they secondarily own.
✔	✔	✔		**View Item If Submitter** – Allows users to view items they submitted.
✔	✔	✔	✔	**View Item if Contact** – Allows users to view items if they are selected in the *Contacts* field. For details on this privilege, refer to Privilege Behavior for System Tables [page 241].

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔	✔	**View Item if Contact's Company** – Allows users to view items of other contacts within the same company. For details on this privilege, refer to Privilege Behavior for System Tables [page 241].

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**View All Archived Items** – Allows users to view items contained in Archive tables through the SBM User Workspace. Users can search for archived items in any Archive tables using the **Advanced Search** feature. Archive tables are only available to users on the **Advanced Search** page if this privilege has been granted and items have been archived.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**Restore Item from Archive** – This privilege, along with the **View All Archived Items** privilege, allows users to restore archived items through the SBM User Workspace. Once the archived items are found, if the user has this privilege, a button appears allowing the user to restore the item from the Archive table to the active or original table.
✔				**Update All Items** – Allows users to update all items.
✔	✔			**Update Item If Owner** – Allows users to update items they primarily own.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Update Item If Secondary Owner** – Allows users to update items the secondarily own.
✔	✔			**Update Item If Submitter** – Allows users to update items they submitted.
✔				**Transition All Items** – Allows users to transition all items.
✔	✔			**Transition Item If Owner** – Allows users to transition items they primarily own.
✔				**Transition Item If Secondary Owner** – Allows users to transition items they secondarily own.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔			**Transition Item If Submitter** – Allows users to transition items they submitted.
✔				**Update Submitter** – Allows users to update the *Submitter* system field if the **Update Submitter** option is selected on a transition.
✔				**Mass Update Items** – Allows users to mass update items.
✔	✔	✔		**View Workflow Graphically** – Allows users to view the workflow assigned to items by clicking the **Workflow** icon located next to the Actions drop-down list on the **Item Details** pane.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View State Change History** – Allows users to view the state change history in the **Item Details** pane for items in the selected project and enables users to create **State Change** reports.
✔	✔	✔		**View Change History** – Allows users to view the change history in the **Item Details** pane for items in the selected project. This privilege also enables users to create **Change History** reports and to view Time Capture options on state forms.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**View Principal and Subtasks** – Allows users to view the **Subtasks** section. The **Subtasks** check box must also be selected in the user's preferences for users to view the **Subtasks** section. The **Subtasks** section only appears on forms if an item is a subtask of another item or has one or more subtasks associated with it and users have privileges to view at least one of the subtask items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Link Subtasks** – Allows users to establish a principal/ subtask relationship by linking subtasks to an existing principal item. Users can add subtasks to any item they have privileges to view.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Link/Unlink Principal** – Allows users to establish a principal/ subtask relationship by linking a principal item to existing items, making them subtasks of the principal item. This privilege also allows users to break the relationship between a principal item and its subtasks. Users can link and unlink principal tasks for any items they have privileges to view.
✔			✔	**Manage Version Control History** – Allows users to add, modify, and delete file associations to the Version Control History section.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**View Status of Notification** – Enables users to view the status of notifications for all users in the Item Notifications tab of an item. A recipient search box appears for users that have this privilege.

Field Privileges

This set of privileges determines which fields users can view and update on forms in the selected project.

In SBM Composer, each field is assigned to a privilege section, which is used to group fields for display or to limit user accessibility to certain fields. When quick forms are used, field privilege sections are used to control security and field layout. When custom forms are used, field privilege sections are used to control security only.

Note: Section labels can be modified at a global level in SBM System Administrator and for each table in SBM Composer. Custom labels are listed in the **Field** privileges page when appropriate.

The following information applies to field privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- Fields in the **Standard Fields** section are always visible to users who have privileges to view items for a particular project. These users can update fields in the **Standard Fields** section on applicable transitions if they have privileges to submit, update, or transition items for a particular project.
- Update privileges enable users and groups to view and update fields on Submit, Update, or Transition forms.
- View privileges enable users to view fields on all forms.

- You can combine view and update privileges as needed. For example, if you grant the "Update User Fields" privilege and the "View Manager Fields on Update" privilege, users can update fields in the **User Fields** section but only view fields in the **Manager** section when they use the Update transition.
- The *Item ID* field is always visible to users who have privileges to view an item, regardless of the section in which this field is placed.

The following table describes each field privilege and the product-access types for which it applies. All field privileges apply to on-premise and on-demand customers.

Note: If you apply privileges to multiple projects while you are editing user or group accounts, your changes are added to the **Changes Log** in the upper right pane. You can then save your changes for multiple projects at one time rather than incrementally for each project.

Regular User, Managed Administrator, and Script/ API	Occasional	External	Privilege Description
✔	✔	✔	**View User Fields** – Allows users to view all fields assigned to the *User Fields* section.
✔	✔		**View Advanced Fields** – Allows users to view fields assigned to the *Advanced Fields* section.
✔	✔		**View Manager Fields** – Allows users to view fields assigned to the *Manager Fields* section.
✔	✔		**View System Fields** – Allows users to view fields contained in the *System Fields* section.

Regular User, Managed Administrator, and Script/ API	Occasional	External	Privilege Description
✔			**Update User Fields** – Allows users to modify fields assigned to the *User Fields* section.
✔			**Update Advanced Fields** – Allows users to modify fields assigned to the *Advanced Fields* section.
✔			**Update Manager Fields** – Allows users to modify fields assigned to the *Manager Fields* section.
✔			**Update System Fields** – Allows users to modify fields assigned to the *System Fields* section.
✔			**View Hidden Fields in Detail Reports** – Allows users to view in Detail reports fields that have been moved to the *Hidden Fields* section. The **Hidden Fields (Details reports only)** option must also be selected in the user's profile.

Regular User, Managed Administrator, and Script/ API	Occasional	External	Privilege Description
✔	✔	✔	**View User Fields on Submit** – Allows users to view all fields assigned to the *User Fields* section when they submit items.
✔	✔		**View Advanced Fields on Submit** – Allows users to view all fields assigned to the *Advanced Fields* section when they submit items.
✔	✔		**View Manager Fields on Submit** – Allows users to view all fields assigned to the *Manager Fields* section when they submit items.
✔	✔		**View System Fields on Submit** – Allows users to view all fields assigned to the *System Fields* section when they submit items.
✔	✔		**View User Fields on Transition** – Allows users to view all fields assigned to the *User Fields* section when they transition items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	Privilege Description
✔	✔		**View Advanced Fields on Transition** – Allows users to view all fields assigned to the *Advanced Fields* section of Transition forms when they transition items.
✔	✔		**View Manager Fields on Transition** – Allows users to view all fields assigned to the *Manager Fields* section when they transition items.
✔	✔		**View System Fields on Transition** – Allows users to view all fields assigned to the *System Fields* section when they transition items.
✔	✔		**View User Fields on Update** – Allows users to view all fields assigned to the *User Fields* section when they update items.
✔	✔		**View Advanced Fields on Update** – Allows users to view all fields assigned to the *Advanced Fields* section when they update items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	Privilege Description
✔	✔		**View Manager Fields on Update** Allows users to view all fields assigned to the *Manager Fields* section when they update items.
✔	✔		**View System Fields on Update** – Allows users to view all fields assigned to the *System Fields* section when they update items.

Attachment Privileges

This set of privileges determines if users or group members can view, add, edit, and delete attachments to items in the selected project. An attachment can be a URL, a link to a file, or a link from one item to another.

You can also allow users to specify individual attachments to items as "unrestricted," meaning that anyone with privileges to view the item can also view any of its attachments that are designated as unrestricted. By default, all attachments are restricted based on privileges granted to users.

The following information applies to attachment privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- Users who do not have privileges to view an item's attachments cannot view file attachments and images that are added to *Text* fields, notes, and e-mail messages using the Rich Text Editor.
- Users who are assigned a "view" attachment privilege can also send e-mail messages from attachments they can view. E-mail messages sent from attachments are only attached to the item from which they are sent if the user has "add" note privileges. In addition, you must also select the **Insert E-mail as Note** system setting in SBM System Administrator before e-mail messages to items are attached to items.
- Unrestricted item links can be viewed by users who have privileges to view the linked item. Restricted item links can be viewed by users who have privileges to view the linked item and privileges to view attachments on the item containing the item link. If users create a two-way item link, the unrestricted/restricted status of the item link

in the destination project is the same as the source item link if they have privileges to set this status in the receiving project. If they do not have privileges to set this status in the receiving project, the status of the item link in the destination project is determined by default settings specified on the **Attachments** tab of the **Settings** dialog box in SBM System Administrator.

- Labels for the Attachment section can be customized and may be reflected in privilege names.

Note: If you apply privileges to multiple projects while you are editing user or group accounts, your changes are added to the **Changes Log** in the upper right pane. You can then save your changes for multiple projects at one time rather than incrementally for each project.

The following table describes each attachment privilege and the product-access types to which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View Attachments on Any Item** – Allows users to view attachments to any item.
✔				**View Attachments If Owner** – Allows users to view attachments to items that they primarily or secondarily own.
✔	✔	✔		**View Attachments If Submitter** –Allows users to view attachments to an items they submitted.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View Attachments You Authored** –Allows users to view attachments they authored.
✔	✔	✔		**Add Attachments to Any Item** – Allows users to add attachments to any item.
✔	✔			**Add Attachments If Owner** – Allows users to add attachments to items that they primarily or secondarily own.
✔	✔			**Add Attachments If Submitter** – Allows users to add attachments to items they submitted.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔	✔	**Add Attachments to Item if Contact** – Allows users to add attachments to items if they are the contact for the items.
✔				**Edit Attachments on Any Item** – Allows users to edit attachments on any item.
✔	✔			**Edit Attachments if Owner** – Allows users to edit attachments to an item that they primarily or secondarily own.
✔	✔			**Edit Attachments if Submitter** – Allows users to edit attachments to items they submitted.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**Edit Attachments You Authored** – Allows users to edit attachments they authored.
✔	✔	✔		**Set Unrestricted Status of Attachments** – Allows users to set individual attachments to an item as unrestricted. This enables users who have privileges to view the item to which the file, URL, or item link is attached to also view the attachment even if they have no attachment view privileges.
✔				**Delete Attachments on Any Item** – Allows users to delete attachments from any item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Attachments If Owner** – Allows users to delete attachments from items that they primarily or secondarily own.
✔				**Delete Attachments If Submitter** – Allows users to delete attachments from any item they submitted.
✔				**Delete Attachments You Authored** – Allows users to delete attachments from any item if they authored the attachments.

Note Privileges

This set of privileges determines if the user or group member is allowed to view, add, edit, and delete notes to items for the selected project. A note is a *Text* field provided for adding notes pertaining to a primary or auxiliary item. E-mail messages sent from items are also categorized as notes.

In addition, you can allow users to specify individual notes and e-mail messages attached to items as "unrestricted," meaning that anyone with privileges to view the item can also view any of its notes and e-mail messages that are designated as unrestricted. By default, all attachments are restricted based on privileges granted to users.

The following information applies to Note privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- Users who are assigned a "view" note privilege can also send e-mail messages from notes they can view. E-mail messages sent from notes are only attached to the item from which they are sent if the user has "add" note privileges. In addition, you must also select the **Insert E-mail as Note** system setting in SBM System Administrator before e-mail messages to items are attached to items. *(On-premise only.)*
- Users can send e-mail messages from primary and auxiliary items they have privileges to view. For those messages to be attached to the item, however, they must be granted "add" note privileges.
- Labels for the Notes section can be customized and may be reflected on the **Note** privileges page.

Note: If you apply privileges to multiple projects while you are editing user or group accounts, your changes are added to the **Changes Log** in the upper right pane. You can then save your changes for multiple projects at one time rather than incrementally for each project.

The following table describes each note privilege and the product-access types for which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View Notes on Any Item** – Allows users to view notes in any item.
✔				**View Notes If Owner** – Allows users to view notes in any item that they primarily or secondarily own.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View Notes If Submitter** – Allows users to view notes in any item they submitted.
✔	✔	✔		**View Notes You Authored** – Allows users to view notes they authored in an item.
✔	✔	✔		**Add Notes to Any Item** – Allows users to add notes to any item.
✔	✔			**Add Notes If Owner** – Allows users to add notes to any item that they primarily or secondarily own.
✔	✔			**Add Notes If Submitter** – This privilege allows users to add notes to any item they submitted.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔	✔	**Add Notes to Item if Contact** – Allows users to add notes to items if they are the contact for the items.
✔				**Edit Notes on Any Item** – Allows users to edit notes on any item.
✔	✔			**Edit Notes If Owner** – Allows users to edit notes on items that they primarily or secondarily own.
✔	✔			**Edit Notes If Submitter** –Allows users to edit notes on items they submitted.
✔	✔	✔		**Edit Notes You Authored** – Allows users to edit notes they authored in an item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**Set Unrestricted Access of Notes/e-mail** – Allows users to set individual notes and e-mail messages attached to an item as unrestricted. This enables users who have privileges to view the item to which the note or e-mail message is attached to also view the note or e-mail message even if they have no note view privileges.
✔				**Delete Notes on Any Item** – Allows users to delete notes from any item.
✔				**Delete Notes If Owner** – Allows users to delete notes from items that they primarily or secondarily own.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Notes If Submitter** – Allows users to delete notes from items they submitted.
✔				**Delete Notes You Authored** – Allows users to delete notes from items they authored in the item.

Report Privileges

This set of privileges determines if the user or group member is allowed to create, modify, run, and delete reports for specific privilege categories for the selected project. You can also grant user privileges to create, modify, run, and delete reports on auxiliary tables. For details, refer to Table Privileges [page 224].

By default, reports have the following privilege categories:

- **Private** – This privilege category enables individual users to manage reports they create. Only the user who creates a private report can access, modify, or delete private reports and only if this user is granted "Manage Private Reports" privileges.
- **Guest** - All users or groups assigned specific Report privileges under the Guest privilege category can perform the appropriate report actions for guest-level reports only. This privilege set also enables users to view and create public feeds in Work Center.
- **User** – All users or groups assigned specific Report privileges under the User privilege category can perform the appropriate report actions for user-level reports only.
- **Manager** – All users or groups assigned specific Report privileges under the Manager privilege category can perform the appropriate report actions for manager-level reports only.

The following information applies to report privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.

- Report privilege category labels can be modified in SBM System Administrator. Custom labels are listed in the **Report** privileges page when appropriate. *(On-premise only.)*
- Users who are not granted the **Create/Modify Advanced SQL Queries** privilege can run reports that contain advanced SQL queries if they have run privileges for the report type. For example, users with privileges to run manager-level reports in the selected project can run manager-level reports that contain advanced SQL queries.
- To allow users to modify, run, and delete guest-level, user-level, and manager-level reports they created, grant them the **Manage Public Reports You Authored** privilege located on the **Privileges – Report** page and the **Privileges – Table** page.

Note: If you apply privileges to multiple projects while you are editing user or group accounts, your changes are added to the **Changes Log** in the upper right pane. You can then save your changes for multiple projects at one time rather than incrementally for each project.

The following table describes each report privilege and the product-access types for which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Manage Private Reports** – Allows users to create reports that only they can access, run, modify, and delete.
✔				**Create Guest-Level Reports** – Allows users to create reports with guest-level access and public feeds in Work Center.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Create User-Level Reports** – Allows users to create reports with user-level access.
✔				**Create Manager-Level Reports** – Allows users to create reports with manager-level access.
✔				**Modify Guest-Level Reports** – Allows users to modify any guest-level report.
✔				**Modify User-Level Reports** – Allows users to modify any user-level report.
✔				**Modify Manager-Level Reports** – Allows users to modify any manager-level report.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**Run Guest-Level Reports** – Allows users to run any guest-level report or feed in Work Center. Also enables non-external users to receive links through e-mail to reports they can run.
✔				**Run User-Level Reports** – Allows users to run any user-level report. Also enables users to receive links through e-mail to reports they can run.
✔				**Run Manager-Level Reports** – Allows users to run any manager-level report. Also enables users to receive links through e-mail to reports they can run.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Guest-Level Reports** – Allows users to delete any guest-level report.
✔				**Delete User-Level Reports** – Allows users to delete any user-level report.
✔				**Delete Manager-Level Reports** – Allows users to delete any manager-level report.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Manage Public Reports You Authored** – Allows users to modify, run, and delete guest-level, user-level, and manager-level reports they created. This privilege enables users to create reports that other users can run, but prevents them from editing public reports that other users have created. For optimal use of this privilege, do not assign this privilege along with other privileges to modify guest, manager, and user reports.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**Create/ Modify Advanced SQL Queries** – Allows users to create and modify reports that contain advanced SQL queries as search specifications. Users who are granted this privilege can create and modify Advanced SQL reports that do not use pass-through SQL. To use pass-through SQL in reports, users must be granted this privilege and the **Create/ Modify Pass-Through SQL Queries** privilege located on the **System** privileges page.

Table Privileges

This set of privileges applies to auxiliary tables and determines if users or group members can submit, update, view, and delete information or create, modify, and run reports for the specified tables. Privileges must be assigned to individual tables.

The following information applies to table privileges:

- Privileges apply to the selected auxiliary table. For information about how privileges apply to system auxiliary tables, refer to Privilege Behavior for System Tables [page 241].
- In SBM Composer, each field is assigned to a privilege section, which is used to group fields for display or to limit user accessibility to certain fields. When quick forms are used, field privilege sections are used to control security and field layout. When custom forms are used, field privilege sections are used to control security only.
- An attachment can be a URL, a link to a file, or a link from one item to another. A note is a *Text* field provided for adding notes pertaining to the item. E-mail messages sent from primary and auxiliary items are also categorized as notes.
- Users who do not have privileges to view an item's attachments cannot view file attachments and images that are added to *Text* fields, notes, and e-mail messages using the Rich Text Editor.
- Users who are assigned a "view" note privilege can also send e-mail messages from notes they can view. E-mail messages sent from notes are only attached to the item from which they are sent if the user has "add" note privileges. In addition, you must also select the **Insert E-mail as Note** system setting in SBM System Administrator before e-mail messages to items are attached to items. *(On-premise only.)*
- Unrestricted item links can be viewed by users who have privileges to view the linked item. Restricted item links can be viewed by users who have privileges to view the linked item and privileges to view attachments on the item containing the item link.
- Users are available as e-mail recipients in the Send E-mail dialog box for items they have privileges to view. Groups who are assigned the "View All Items" privilege are available as e-mail recipients in the **Send E-mail** dialog box.

  Users can send e-mail messages from auxiliary items they can view. For those messages to be attached to the item, however, users must be granted "Add Note" privileges.
- Labels for fields sections, item details, and report privilege categories can be customized and may be reflected on the **Tables** privileges page.

Privileges for System Tables

On-premise customers automatically receive several system auxiliary tables which provide unique features, particularly for users with External User and Occasional User product access. Users with these limited access types can only be granted privileges in specific tables, and these privileges work in conjunction with other privileges.

For example, external users must be granted the View Your Contact Information privilege to see their Contact record. You can then grant the View User Fields privilege for the Contacts table so they can see fields in that section in their Contact record. Granting only the View User Fields privilege to external users for the Contacts table has no effect without also granting the View Your Contact Information privilege.

The following table describes privilege relationships for users with External User and Regular user product access.

Privileges	Applicable System Table	Description	Related Privileges
View User Fields View Attachments on Any Item View Notes on Any Item	Contacts Problems Resolutions	Allows users with External User and Occasional User access to view fields in the User Fields section, notes and attachments in: • Public records in the Problems and Resolutions tables • Their own Contact record	• Grant privileges to view items in specific Knowledge Base folders that do not allow anonymous access. (Folders page) • View Public Problems and Resolutions (System page) • View Your Contact Information (System page)

Table Privilege List

The following table describes each auxiliary table privilege and the product-access types for which it applies.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Submit** – Allows users to submit new items.
✔				**Update** – Allows users to update items.
✔				**Delete** – Allows users to delete items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔			**View** – Allows users to view table items in report and search results and by clicking the relational table icon next to the field on forms.
✔	✔	✔		**View User Fields** – Allows users to view all fields assigned to the **User Fields** section. Refer to Privilege Behavior for System Tables [page 241] before assigning this privilege to users with External User or Occasional User product access.
✔	✔			**View Advanced Fields** – Allows users to view all fields assigned to the **Advanced Fields** section.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔			**View Manager Fields** – Allows users to view all fields assigned to the **Manager Fields** section.
✔	✔			**View System Fields** – Allows users to view all fields assigned to the **System Fields** section.
✔				**Update User Fields** – Allows users to modify fields assigned to the **User Fields** section.
✔				**Update Advanced Fields** – Allows users to modify fields assigned to the **Advanced Fields** section.
✔				**Update Manager Fields** – Allows users to modify fields assigned to the **Manager Fields** section.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Update System Fields** – Allows users to modify fields assigned to the **System Fields** section.
✔				**View Hidden Fields in Details Reports** – Allows users to view in Detail reports fields that have been moved to the **Hidden Fields** section.
✔				**View User Fields on Submit** – Allows users to view all fields assigned to the **User Fields** section upon submitting an item.
✔				**View Advanced Fields on Submit** – Allows users to view all fields assigned to the **Advanced Fields** section upon submitting an item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**View Manager Fields on Submit** – Allows users to view all fields assigned to the **Manager Fields** section upon submitting an item.
✔				**View System Fields on Submit** – Allows users to view all fields assigned to the **System Fields** section upon submitting an item.
✔				**View User Fields on Update** – Allows users to view all fields assigned to the **User Fields** section when they update items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**View Advanced Fields on Update** – Allows users to view all fields assigned to the **Advanced Fields** section when they update items.
✔				**View Manager Fields on Update** – Allows users to view all fields assigned to the **Manager Fields** section when they update items.
✔				**View System Fields on Update** – Allows users to view all fields assigned to the **System Fields** section when they update items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔	✔		**View Attachments on Any Item** – Allows users to view attachments to all items. Refer to Privilege Behavior for System Tables [page 241] before assigning this privilege to users with External User or Occasional User product access.
✔				**View Attachments You Authored** – Allows users to view attachments they created to items.
✔				**Add Attachments to Any Item** – Allows users to add attachments to any item.
✔				**Edit Attachments on Any Item** – Allows users to edit any attachments to items.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Edit Attachments You Authored** – Allows users to edit attachments they authored.
✔				**Set Unrestricted Status of Attachments** – Allows users to set individual attachments as "unrestricted". This enables users who have privileges to view the item to which the file, URL, or item link is attached to also view the attachment even if they have no attachment view privileges.
✔				**Delete Attachments on Any Item** – Allows users to delete attachments from any item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Attachments You Authored** – Allows users to delete attachments they authored.
✔	✔	✔		**View Notes on Any Item** – Allows users to view notes on all items. Refer to Privilege Behavior for System Tables [page 241] before assigning this privilege to users with External User or Occasional User product access.
✔				**View Notes You Authored** – Allows users to view notes they created.
✔				**Add Notes to Any Item** – Allows users to add notes to any item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Edit Notes on Any Item** – Allows users to edit any notes in items.
✔				**Edit Notes You Authored** – Allows users to edit notes they authored.
✔				**Set Unrestricted Status of Notes/E-mail** – Allows users to set individual notes and e-mail messages attached to a table item as "unrestricted. This enables users who have privileges to view the item to which the note or e-mail message is attached to also view the note or e-mail message even if they have no note view privileges.
✔				**Delete Notes on Any Item** – Allows users to delete notes from any item.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Notes You Authored** – Allows users to delete notes they authored.
✔	✔			**View Change History** – Allows users to view the **Change History** for items. This privilege also enables users to create **Change History** reports for the selected table.
✔				**Manage Private Reports** – Allows users to create reports that only they can run, modify, and delete.
✔				**Create Guest-Level Reports** – Allows users to create reports with guest-level access.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Create User-Level Reports** – Allows users to create reports with user-level access.
✔				**Create Manager-Level Reports** – Allows users to create reports with manager-level access.
✔				**Modify Guest-Level Reports** – Allows users to modify any guest-level report.
✔				**Modify User-Level Reports** – Allows users to modify any user-level report.
✔				**Modify Manager-Level Reports** – Allows users to modify any manager-level report.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔	✔			**Run Guest-Level Reports** – Allows users to run any guest-level report.
✔				**Run User-Level Reports** – Allows users to run any user-level report.
✔				**Run Manager-Level Reports** – Allows users to run any manager-level report.
✔				**Delete Guest-Level Reports** Allows users to delete any guest-level report.
✔				**Delete User-Level Reports** – Allows users to delete any user-level report.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔				**Delete Manager-Level Reports** – Allows users to delete any manager-level report.
✔				**Access Public Reports You Authored** – Allows users to modify, run, and delete guest-level, user-level, and manager-level reports they created.

Regular User, Managed Administrator, and Script/ API	Occasional	External	On-premise Only	Privilege Description
✔			✔	**Create/ Modify Advanced SQL Queries** – Allows users to create and modify reports that contain advanced SQL queries as search specifications. Users who are granted this privilege can create and modify Advanced SQL reports that do not use pass-through SQL. To use pass-through SQL for reports, users must be granted this privilege and the Create/ Modify Pass-Through SQL Queries privilege located on the **System** privileges page.
✔				**Mass Update Items** – Allows users to update and delete multiple items in the selected table.

Privilege Behavior for System Tables

On-premise customers automatically receive several system auxiliary tables which provide unique features, particularly for users with External User and Occasional User product access. Users with these limited access types can only be granted privileges in specific system tables, and these privileges work in conjunction with other privileges.

For example, external users must be granted the "View Your Contact Information" privilege to see their record in the system *Contacts* table. You can then grant the "View User Fields" privilege for the *Contacts* table so they can see fields in that section in their *Contact* record. Granting only the "View User Fields" privilege to external users for the *Contacts* table has no effect without also granting the "View Your Contact Information" privilege.

In addition, privileges for the system *Contacts* table pertain only to records that are associated with user accounts. This setting is located on the **General** tab when you add or edit a user account.

The following table describes privilege behavior related to system auxiliary tables.

Note: The system behavior discussed in this topic applies only to the *Contacts*, *Companies*, *Problems*, and *Resolutions* tables that are created by the Create Database Wizard. If you create your own tables called *Contacts* or use the *Problems* primary table provided with Serena Service Manager, for example, the system behavior does not apply.

Privilege and Location	Applicable Tables	Notes
View Public Problems and Resolutions (System tab)	Problems Resolutions	Must also grant users privileges to view items in specific Knowledge Base folders that do not allow anonymous access. These privileges are granted on the Folders tab.
View Your Contact Information (System tab)	Contacts	Allows users to view their records in the *Contacts* table if that record has been associated with the user's account.
Edit Your Contact Information (System tab)	Contacts	Allows users to modify their records in the *Contacts* table if that record has been associated with the user's account.

Privilege and Location	Applicable Tables	Notes
View User Fields (Tables tab)	Contacts Problems Resolutions	Users must also be granted the "View Your Contact Information" privilege before these privilege take effect for the *Contacts* table. Users must also be granted the "View Public Problems and Resolutions" privilege before these privileges take effect for the *Problems* and *Resolutions* tables.
View Attachments on Any Item (Tables tab)	Contacts Problems Resolutions	
View Notes on Any Item (Tables tab)	Contacts Problems Resolutions	
View Item If Contact (Item tab)	Any Primary Table	Relational fields based on the system *Contacts* and *Companies* tables must be added to the application for which privileges are being granted. When granted these privileges, users can see items if they are selected in the *Contacts* fields or if the company associated with their *Contacts* record is selected in the *Company* field.
View Item If Contact's Company (Item tab)	Any Primary Table	

About Preferences

You can apply an initial set of preferences to users or groups. These preferences apply to Serena Work Center, the SBM User Workspace, or both.

You can apply preferences for:

- **A single user**

  This works best when you only need to set preferences for a new user or to assist a single user with this task.

- **A set of users**

  This works best when you only need to set preferences for a small number of users who may not be members of the same group.

- **A group**

  This works best when you want to apply privileges to all members of one or more groups. This is the easiest way to apply privileges to a large number of users at the same time. For details, refer to Applying Preferences to Groups [page 174].

When you apply preferences to multiple users or groups, settings that differ between multiple user accounts are highlighted in red when **All** is selected on the toolbar. You can

change the settings for all users, or you can select each user on the toolbar and make changes for the selected user only. For guidance, refer to Comparing and Changing User and Group Accounts [page 146].

Consider the following information when setting preferences for users and groups:

- Users who have privileges to modify their user profile can overwrite preferences you set for them. Likewise, changes you make to preferences overwrite changes made by users.
- Users with External product access cannot modify their user profile settings, so all changes for these users must be made in SBM Application Administrator.
- User accounts with API/Script product access are granted a set of required preferences. You should not modify preferences for accounts with this access type.

For details on each setting, refer to:

- Content Preferences [page 243]
- Display Preferences [page 245]
- Section Preferences [page 247]
- Date/Time and Locale Preferences [page 248]
- Work Center Settings [page 249]

Content Preferences

Use the **Content** page to set the initial home page, preferred application, and quick links for users. These options apply only to the SBM User Workspace.

Note: When you set preferences for groups, group members may not have privileges in all applications or reports in the list. In this case, changes do not apply to those users.

- **Home Page Options**
  - **Show Launch Page**

    Select this check box to open the **Task** page when users log in to the SBM User Workspace or select any application tab. Clear this check box to open the home page report specified for each application. By default, the **Task** page is the home page for new users.

  - **Applications**

    Select an application from the list to set the home page report and quick links for that application, and then save your changes. Repeat this process for each application in the list.

  - **Home Page Report**

    Enables you to set the home page report for each application. Search for or select reports, including built-in, System, and custom reports. To select a different home page report for each application, select an application from the **Application** list, and then select the report from the **Home Page Report** list. If you are selecting a home page report for the user's preferred application and you

have not enabled the **Launch** page for this user, the report runs when the user logs on to the SBM User Workspace, clicks the **Home** button, or selects the **Application** tab for the preferred application.

- **Application Options**
  - **Preferred Application**

    Select the application that determines which **Application** tab is selected by default.

  - **Tabs to Display**

    Sets the number of **Application** tabs that are displayed on the **Application** toolbar. Applications that exceed this limit are listed on the **More** tab.

  - **Application Tab Order**

    To order Application tabs on the Application toolbar in the SBM User Workspace, select an application, and then click the **Up** and **Down** buttons.

- **Quick Link Options**

  You can create an initial set of quick links for users, who can then add or remove quick links later. Quick links apply only to the SBM User Workspace.

  These options are not available when you are setting preferences for group accounts.

  To add a quick link, type a name in the **Link Name** box, and then select one of the following options:

  - **Execute Report**

    Click the list arrow to select from reports the user has privileges to run in any application or auxiliary table, as well as built-in reports and System reports. You can also search for reports by title.

  - **Submit Into**

    Lists the projects the user has privileges to submit into based on the application selected in the **Application** list located in the **Home Page** section. Select a project from the list to open a **Submit** form for that project each time the user selects the quick link. You can also search for a project by name.

  - **Advanced Lookup**

    Contains the primary table associated with the application selected in the **Application** list located in the **Home Page** section as well as auxiliary tables the user has privileges to access. Select a table from the list to open the **Advanced Lookup Tool** for that table each time the user selects the quick link.

  - **URL**

    With URL selected form the list, type a Web address in the **URL** box, and then click **Create Link**. Optionally, provide a link for the name.

  To remove a quick link, select it in the list, and then click the **Remove** icon ().

Display Preferences

Use the **Display** page to set preferences for the number of items returned for search and report results, the accessible interface, and more.

If you are modifying multiple accounts, click **Compare** to view the different settings for each account. For guidance, refer to Comparing and Changing User and Group Accounts [page 146].

Option	Description	Applies To
Auto Folder Items	Select this check box to automatically place links to items in the system favorites folders, which include the Inbox, Submitted Items, Transitioned Items, and Updated Items folders. Clearing this check box does not remove links to items already contained in the folders but prevents new item links from being created. Users may improve system performance by clearing the **Auto Folder Items** check box.  **Note:** This option is only available if the **Allow Auto Folder Items** check box has been selected on the **Database** tab of the **Settings** dialog box in SBM System Administrator.	SBM User Workspace
Version Control History	Select this check box to show version control history associated with primary items in the **Item Details** pane. This option applies to primary items that use a version control integration, such as SourceBridge or VersionBridge. Users can view the names of the files associated with an item, the date and time in which files were checked in and out, the process app user who performed the action or file association, and the associated comment. Depending on the version control tool, the file revision number may also be listed. *(On-premise customers only.)*	SBM User Workspace
Auto Requery	Select this check box to automatically update results for Listing report, including those viewed in the Editable Grid, or items in Knowledge Base folders (on-premise). This option applies when you update an item so that it no longer fits the criteria of the report, and then select **Back to Results**. For example, if the report lists active items, and you close one of the items in the report, the results lists is updated automatically when you return to it. If this option is not selected, the report list is not updated; instead the results will remain the same as when originally run. To manually refresh results, click the **Requery** link or rerun the report. For Knowledge Base folders, the update occurs when an item is added or removed from a folder.	SBM User Workspace

Option	Description	Applies To
Use Accessible Interface	This option condenses SBM features into a text-rich, vertical format. The Accessible interface is appropriate for handheld device users and users who rely on assistive technologies.	SBM User Workspace
Items Per Page	This option determines the maximum number of items that appear per page. Note that displaying a large number of items could impact performance.  **Note:** The **Items Per Page** setting on the **Settings - Display** tab in SBM System Administrator controls the maximum number of items users can display on each page in the SBM User Workspace. Users can specify a lower number of items, but they cannot exceed the number of items allowed by the system.	Serena Work Center and SBM User Workspace
Advanced Lookup Defaults	This option sets the default menu choice for the *Active/Inactive* field on certain search features, such as the **Advanced Search** page, the the **Advanced Lookup Tool**, and the **Relational Field Value Lookup** form in the SBM User Workspace. This option also sets the default choice for the *Active/Inactive* field in the Auxiliary Data feature. Users can choose to view inactive items, active items, or all items. Users can change the default selection as needed.	SBM User Workspace

Deprecated Settings

 **Note:** The preferences will be removed from Application Administrator in a future release. These options will still be available to end users, however.

Option	Description	Applies To
Single Frame View	Select this check box to display the **Item List** pane in a single frame for report results, search results, and folder contents. When users click an item link, the **Item Details** pane opens and replaces the **Item List** pane. If this option is not selected, both panes appear in a two-frame view, with the **Item List** pane appearing on top and the **Item Details** pane on the bottom. This option is selected by default for new user accounts.	SBM User Workspace

Option	Description	Applies To
Auto Spell Check	Select this check box to automatically check spelling for *Text* fields in the SBM User Workspace. The system checks spelling in forms, note attachments, and e-mail titles when users exit a form or dialog box. Users may improve system performance by clearing the **Auto Spell Check** check box.  **Note:** The Spell Check feature is only available in the SBM User Workspace and only for legacy (non-modern) themes. Spell check is not available if HTML5 features have been enabled for your system. In this case, the native browser spell check feature can be used to verify spelling for most text-entry fields. Note that Internet Explorer 9 (IE9) users may need to first download and enable a spell-check plug-in. Spell check is also not available if the default locale for the SBM Application Engine is set to Japanese. If the default locale has not been set, then the Spell Check feature is not available if the SBM Application Engine is installed on a Japanese operating system.	SBM User Workspace/ legacy (non-modern) themes only
Top View	Display state change history information at the top of the **Item Details** pane on quick forms.	Serena Work Center and SBM User Workspace
Bottom View	Display state change history information at the bottom of the **Item Details** pane on quick forms.	Serena Work Center and SBM User Workspace

Section Preferences

Use the **Sections** page to sort notes and change history and enable or disable the State History view. These options apply to Serena Work Center and the SBM User Workspace.

If you are modifying multiple accounts, click **Compare** to view the different settings for each account. For guidance, refer to Comparing and Changing User and Group Accounts [page 146].

- **Notes**
  The following preferences control how notes and e-mail messages attached to items are displayed in the **Notes** section:
  - **Sort new first**

    Sort notes and e-mail messages by displaying the most recent date first.
  - **All**

View all notes and e-mail messages attached to an item.

- **None**

  Prevent notes and e-mail messages attached to an item from being displayed.

- **Last**

  View a specific number of notes attached to an item. For example, if you enter the number 5, the five most recent notes are displayed.

- **Change History**
  The following preferences control how the history of changes to items, particularly changes made to each field and to an item's attachments, subtasks, and principal tasks, appear in the **Change History** section. The **Change History** preference may also detemine if the Time Capture view is available to users on state forms.

  - **Sort new first**

    Sort entries in the **Change History** section by the most recent changes first.

  - **All**

    View all change history entries for an item in the **Change History** section.

  - **None**

    Turn off the display of the **Change History** section.

  - **Last**

    View a specific number of change history entries. For example, if you enter the number 5, the five most recent change history entries are displayed.

    Note: Users must have privileges to view change history for specific projects and auxiliary tables. If users do not have change history privileges, changes to these options have no effect.

- **State History View**

  Select **View On** to enable the State History view. Select **View Off** to disable the State History view. Users must have privileges to view the State History for this change to take effect. Also, users can choose to display State History at the top or bottom of item forms.

Date/Time and Locale Preferences

Use the Date/Time & Locale page to set users' preferred date/time format, time zone, locale, and business calendar. These options apply to the Serena Work Center and SBM User Workspace.

If you are modifying multiple accounts, click **Compare** to view the different settings for each account. For guidance, refer to Comparing and Changing User and Group Accounts [page 146].

- **Date Format**
  Choose one of the following date display options:

  - mm/dd/yyyy

- mm/dd/yyyy (24-hour clock)
- dd/mm/yyyy
- dd/mm/yyyy (24-hour clock)
- dd.mm.yyyy
- dd.mm.yyyy (24-hour clock)
- yyyy-mm-dd
- yyyy-mm-dd (24-hour clock)
- **Use Date/Time Format From Locale** – Select this option to display dates and times based on the selected locale.

- **Time Zone**

  The system time zone is enclosed in brackets, such as <GMT -7:00 America/Denver>. Select a different time zone as needed. By default, the system time zone specified by your administrator is selected.

- **Calendar for Hours of Operation**

  Calendars are defined in SBM Application Administrator. Users who have been granted the **Select Calendar for Hours of Operation** system privilege can select a calendar in their user preferences. Calendars are used to:

  - Calculate when notification escalations are sent. This ensures that notification escalations are generated only during the hours defined in the calendar. For example, if your organization operates from 9 a.m. to 5 p.m., Monday through Friday, notification escalations are sent only during these hours. The 24 Hour Calendar is selected by default, which means notification escalations are sent 24 hours a day, seven days a week.
  - Calculate the distribution of Time Capture entries for users who do not have resource records with calendar assignments.

- **Locale**

  By default, the system locale is selected. Select a different locale as needed.

Work Center Settings

Use the **Work Center** page to pin up to five applications and application groups to users' Work Center toolbars.

You can:

- Apply settings at a global level. These default settings are automatically applied to newly created users, but you can apply them manually to users and group members.
- Apply settings to one or more users.
- Apply settings to one or more groups.

Users can modify the applications you pin for them, unless you select the **Locked** check box for specific applications.

- **Get Default Settings**

  If you are pinning applications for users and groups, click this button to use the global settings. For details, refer to Pinning Application Groups [page 331].

- **Available Application Groups**

  Select or search for applications, then double-click or use the arrows to move selected groups to the list of pinned applications.

- **Pinned Application Groups**

  Shows the list of pinned applications. You can pin up to 5 applications. Use the arrows to reorder applications. Select the **Locked** check box to prevent the user from unpinning the application.

- **Show Home Icon**

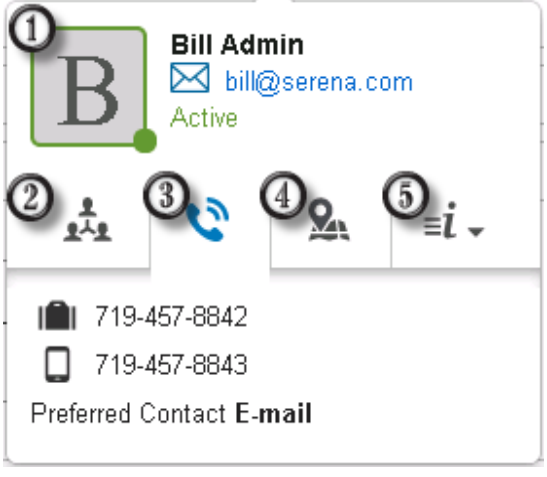
  By default, the **Home** icon is available for all users. **Home** provides a global context for dashboards and views. Clear this check box to remove the **Home** icon from the Work Center toolbar.

About the User Profile Card

The user profile card displays important information about a user to other users in the system. When a user clicks another user's name in one of the end-user interfaces, the profile card appears and displays select user attributes such as the user's title, contact information, and location.

Important: The user profile card is a modern browser feature that requires HTML5. You must select the **Enable HTML5 Features** option on the **General** tab for the Base Project in order to display the card when a user's name is clicked.

Each user profile card consists of five sections:



1. **Main**

   Typically displays the user's avatar, full name, title, and e-mail address. In addition:

- The first character of the user's name is displayed if the user has not selected an avatar.
- Hovering your mouse over the avatar displays the user's last activity.
- The color of the border around the avatar indicates if the user has accessed the system recently. Green indicates recent activity; if the user has not accessed the system recently, the color is orange.

2. **Organization**

   Typically displays attributes related to your organization, such as the name of the user's manager.

3. **Contact**
   Typically displays attributes related to contact information, including phone numbers and the user's preferred contact method.

   Note: Contact attributes are displayed on the user profile card according to the "view" privileges on the Contacts table. This means that users without privilege to view a given field section cannot view fields that are assigned to that privilege section, and the attributes that are associated with those fields are not displayed on the user profile card.

4. **Location**

   Typically displays attributes related to the user's location, such as the user's physical location and local time.

5. **Information**

   Typically displays informational attributes, such as the user's department, skills, and teams.

Key Benefits

- Displays information about a user to other users in the system.
- Provides contact information for users in the system.
- Enables users who are working on common items to easily interact with one another.

The user attributes that appear on every user's card are managed on the **User Profile Card** page in Application Administrator. For details, refer to Customizing the User Profile Card [page 251].

Customizing the User Profile Card

The **User Profile Card** page lists every user attribute in the system. You can also search for an attribute on the page by name. The **Type** column indicates which type of record is associated with the attribute. Each attribute belongs to either a user, resource, or a contact record.

Users and administrators can set these attributes by:

- Manually editing attributes on user, resource, and contact records.
- Importing and updating users and contacts from spreadsheets.

- Importing and updating users and contacts from LDAP.

Any administrator with access to Application Administrator can customize which attributes should appear on each user's profile card. Use the drop-down boxes in the **Section** column to designate which section of the card should display the attribute. Select **(None)** if the attribute should not be displayed.

Tip: Some attributes are limited to certain sections (you cannot display the **Full Name** in the **Location** section, for example.)

If an attribute is empty, the attribute does not appear on the card. For example, if Bill does not have a **Title** attribute defined on his user account, the **Title** attribute does not appear on his user profile card.

Journal and Memo fields are not available for display on the user profile card. All other field types are applicable.

Frequently Asked Questions About User Management

- **What is the difference between roles and groups?**

  Roles provide a way to organize a set of application privileges, while groups provide a way to organize a set of user accounts. In general, you should create roles in SBM Composer to organize privilege sets for your applications. Then, create groups in Application Administrator to organize sets of users, and enable roles for those groups.

- **If I delete a user's account, is data related to that user still available?**

  Users can continue to view data pertaining to deleted users, such as Change History records and data provided by these users, but be aware that some areas of your system may need to be modified when you delete user accounts. For details, refer to Deleting User Accounts [page 148].

- **Can I modify multiple user accounts at the same time?**

  Yes, you can select multiple user accounts and modify settings for all selected users. You can also modify multiple group accounts at once. For details, refer to Comparing and Changing User and Group Accounts [page 146].

  You can also use the Import Users feature to update basic account information, such as product-access type, phone numbers, and e-mail addresses. For details, refer to About User Import [page 350].

- **How do I set a home page report for users?**

  For the User Workspace, modify user preferences for one or more users or groups to set an initial home page, determine which application opens when users log in, and set the tab order. For details, refer to Content Preferences [page 243].

  For Serena Work Center, users view reports in Dashboard views. You can add report widgets to the system My Dashboard view for Home, applications, and application groups. For details, refer to Managing System Views [page 333].

- **How do I grant limited administrative access to the system?**

Assign Remote Administration product access to the user, and then assign administrative privileges to specific applications, users, groups, and more. This enables you to easily delegate administrative tasks among different users while maintaining security of your overall system. For details, refer to Chapter 6: Managing Administrators [page 255].

Chapter 6: Managing Administrators

The following topics describe how to manage administrators in Application Administrator.

About Administrator Management

SBM offers various types of administrative levels. These levels enable you to distribute administration tasks while maintaining control of your system.

Types of Administrators

The following types of administrators are available:

- **System Administrators [page 255]**

  These administrators have full access to the system in on-premise environments.

- **Managed Administrators [page 256]**

  These administrators are responsible for portions of a system, such as specific applications, projects, and users.

- **Global Managed Administrators [page 257]**

  These administrators manage other managed administrators, but generally have fewer responsibilities than system administrators. For on-demand systems, global managed administrators have full capabilities for their systems.

System Administrators

In on-premise systems, system administrators typically perform installation, upgrade, and system configuration tasks. They typically can modify any application in the system, perform deployment and promotion activities for all runtime environments, and control the access of all users in the system.

For best results, on-premise systems should have at least one primary system administrator with the product access and privileges listed below.

Note: When you use the **Create Database Wizard** in SBM System Administrator to establish your SBM database, you must specify an account for a primary system administrator. This administrator is given Regular User product access and the Remote Administration privilege. You can then log in to SBM Application Administrator and grant additional privileges to this account.

- **ODBC Access** - Some administrative tasks can only be performed when an administrator uses ODBC to connect to SBM System Administrator. This access level requires an ODBC System DSN on the administrator's computer pointing to the proper data source and access to the database. For details, refer to the *SBM System Administrator Guide*.

- **Product-access Level** — Grant Regular User product access to system administrators, along with the Remote Administration system privilege.

  CAUTION:

  This combination offers full administrative access to your system. Because of this, use caution when granting the Remote Administration privilege to users.

- **User Privileges** — For best results, grant all user privileges to the system administrator. Without specific application-level privileges, system administrators can administer applications, but they cannot use these applications in user interfaces, such as Serena Work Center and SBM User Workspace. For details, refer to About Privileges [page 180].

- **Repository Privileges** - For best results, grant all repository privileges to the primary system administrator. For details, refer to the *SBM Application Repository Guide*.

Managed Administrators

Managed administrators are typically granted access to specific applications. For example, you may want someone who can add projects or create notifications for a specific application, but not for every application in your system.

Managed administrators should be granted privileges depending on the tasks they will perform. For example:

Application Configuration Tasks - Managed administrators who will only modify applications from SBM Application Administrator should be granted the following access and privileges:

- **Managed Administration Product Access**

- **Remote Administration user privilege** - Allows managed administrators to connect to SBM Application Administrator, to the SBM System Administrator (using remote administration), and to SBM Application Repository.

- **Application-specific privileges** - Managed administrators should be granted project, workflow, field, group, and table privileges specific to the applications they manage. For details, refer to Administrative Privileges [page 259].

  Tip: Do not grant the **Global Administration** privilege to managed administrators. This privilege is located on the **Administration - System** page.

Design, Deployment, and Configuration Tasks - Managed administrators who will design process apps and applications in SBM Composer, deploy them to the SBM Application Engine, and configure them in SBM Application Administrator need the following access and privileges:

- **Managed Administration Product Access**

- **Remote Administration user privilege** - Allows managed administrators to connect to SBM Application Administrator, to the SBM System Administrator (using remote administration), and to SBM Application Repository.
- **Application and Deployment Privileges** - Managed administrators should be granted the privileges described in Privileges Required for Application Configuration, Deployment, and Promotion [page 257]. Managed administrators who will perform promotion activities should be granted promotion-related privileges.
- **Repository privileges** - Managed administrators need repository privileges for specific process app tasks. For details, refer to the *SBM Application Repository Guide*.

Global Managed Administrators

Global managed administrators are responsible for certain portions of an SBM system. They are able to manage other administrators and have extended deployment and environment capabilities.

Global managed administrators should be granted the same privileges as managed administrators, along with the **Global Administration** privilege. The **Global Administration** privilege works in conjunction with other administrative privileges, such as Edit Users and administrative privileges over specific groups.

The **Global Administration** privilege also allows administrators with applicable deployment privileges to add applications to an environment. Administrators must also have applicable privileges granted on the **Administration - Deployment** page.

They can also clear the Common Log history in SBM Application Repository.

Additionally, global administrators in on-premise systems can:

- In SBM Application Repository, delete environments on any host when connected to the database that is the primary host for your system.
- Modify settings on the **System Settings** dialog box in SBM System Administrator.
- Import and update users and contacts into this system using the **LDAP Setup and Tools** dialog box in SBM System Administrator. Administrators must be granted the **Alter Server Settings** privilege to specify LDAP server connection and search filter parameters.
- Configure SourceBridge user setting overrides in SBM System Administrator.

Privileges Required for Application Configuration, Deployment, and Promotion

The following privileges must be granted to managed administrators before they can log into SBM Application Repository or deploy process apps to an environment and configure the applications in the process app after deployment. Privileges must be granted for each environment in which managed administrators will configure applications and deploy and promote process apps.

When administrators first publish or deploy a process app from SBM Composer, they are granted repository privileges to that process app in Application Repository. If administrators need to view, edit, publish, or deploy with a process app they did not initially publish or deploy, they must be manually granted repository privileges in Application Repository. Repository privileges are separate from the privileges below, which

enable managed administrators to deploy, promote, and configure applications in a specific environment.

Note: On-demand customers are automatically granted many of the following privileges through provided groups. For details, refer to Groups for On-Demand Customers [page 176].

Deployment and Promotion Privileges

The following table describes privileges required before managed administrators can log into Application Repository, and deploy, "get," and promote process apps.

Privilege	Privilege Location	Notes
Remote Administration	User - System page	Enables administrators to log into Application Repository.
Add Tables	Administration - System page	Administrators who will deploy new process apps to this host need this privilege. Administrators who have the Global Administration privilege do not need this privilege.
Edit Tables	Administration - System page	Administrators who will deploy existing process apps to this host need this privilege. Managed administrators also need to be granted privileges to specific applications they will deploy. These privileges are granted on the **Administration - Tables** page. Administrators who have the Global Administration privilege do not need this privilege.
Deploy Process Apps to This Host	Administration - Deployment page	Administrators who will deploy process apps to this host need this privilege.
Deploy to This Host From SBM Composer	Administration - Deployment page	Required only if the managed administrator will deploy from SBM Composer.
Export Process Apps From This Host	Administration - Deployment page	This privilege should be granted only to administrators who will perform the "Get Process Apps" task from Application Repository.
Promote to This Host	Administration - Deployment page	This privilege should be granted only to administrators who will promote process apps to this host database. Administrators must also have the "Deploy Process Apps to This Host" privilege.

Application Configuration Privileges

The following table describes the minimum set of privileges required before managed administrators can configure deployed applications in SBM Application Administrator.

Privilege	Privilege Location
Edit Workflows	Administration - Workflows page
Edit Transitions	Administration - Workflows page
Add Projects	Administration - Projects page
Edit Projects	Administration - Projects page
Assign Roles	Administration - Projects page
Override Ordering for Default Fields	Administration - Fields page
Edit Fields	Administration - Fields page
Tables	Administration - Tables page

Administrative Privileges

Administrative privileges enable you to control access to various parts of your system. Users must have Managed Administration product access assigned to them before they can be granted administrative privileges described in the following sections.

- System Administration Privileges [page 259]
- Project Administration Privileges [page 262]
- Workflow Administration Privileges [page 263]
- Field Administration Privileges [page 264]
- Group Administration Privileges [page 264]
- Table Administration Privileges [page 265]
- Deployment Privileges [page 265]

System Administration Privileges

System privileges are applied globally to each environment. The following table provides a list and description of the system administration privileges.

Privilege	Description	On-premise Only
Global Administration	Select this check box to grant managed global administrator access to the user. This enables the administrator to manage other administrators and perform other advanced administrative tasks. For details, refer to Global Managed Administrators [page 257]. The Global Administration privilege works in conjunction with other administrative privileges, such as Edit Users and administrative privileges over specific groups.  **Note:** Administrators cannot remove this privilege from their own accounts.	
Add Users	Allows administrators to add users and import users from a spreadsheet in Application Administrator.	
Edit Users	Allows administrators to edit users and to update user accounts from a spreadsheet using the Import Users feature in Application Administrator.	
Delete Users	Allows administrators to delete users.	
Add Groups	Allows administrators to add groups.	
Edit Groups	Allows administrators to edit groups.	
Delete Groups	Allows administrators to delete groups.	
Set "Logon as Another User"	Allows administrators to grant the **Logon as Another User** system privilege to users and groups they manage.	

Privilege	Description	On-premise Only
Set "Remote Administration"	Allows administrators to set up remote administration for users and groups they manage.	
Set "Logon from SourceBridge"	Allows administrators to grant the **Logon from SourceBridge** privilege to users and groups they manage.	✔
Set "Connect using the API"	Allows administrators to grant the **Connect using the API** privilege to users and groups they manage.	
Add Folders	Allows administrators to add Public and Knowledge Base folders in SBM System Administrator.	✔
Edit Folders	Allows administrators to edit folders in SBM System Administrator. This privilege also controls the administrator's ability to move folders in the folder hierarchy.	✔
Delete Folders	Allows administrators to delete folders in SBM System Administrator.	✔
Assign Folder Privileges	Allows administrators to grant the **Assign Folder Privileges** privilege to users and groups they manage.	✔
Add Notifications	Allows administrators to add notifications and rules for workflows they have privileges to administer.	
Edit Notifications	Allows administrators to edit notifications and edit or override rules for workflows they have privileges to administer.	

Privilege	Description	On-premise Only
Delete Notifications	Allows administrators to delete notifications and rules for workflows they have privileges to administer.	
Add Tables	Allows administrators to add primary and auxiliary tables that are deployed as part of process apps.	
Edit Tables	Allows administrators to redeploy process apps and their associated tables.	
Delete Tables	Reserved for future use.	
Alter Database Settings	Allows administrators to modify settings on the **Database** tab of the **Settings** dialog box in SBM System Administrator.	✔
Alter Server Settings	Allows administrators to modify the following settings in SBM System Administrator: • **Server** tab of the **Settings** dialog box • **General** tab of the **LDAP Setup & Tools** dialog box • **License Options** dialog box	✔
Associate Web Services/ Scripts with Notifications	Determines if Run Web Service and Run Script are available as action choices for notifications for the administrator.	✔ (Scripts only)
Associate Scripts with Self-Registration Form	Allows administrators to associate scripts with the **Self-Registration** form in SBM System Administrator.	✔

Project Administration Privileges

Project privileges enable managed administrators to administer projects.

The following information applies to project privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- Privileges are inherited through the project hierarchy, which allows you to set privileges once, rather than for each individual project. The **Inherit All Parent Project's Privileges** check box is selected by default; therefore, to grant a set of privileges for a particular project, clear the check box.

The following table provides a list and description of all project administration privileges.

Note: All project administration privileges apply to on-premise and on-demand customers.

Privilege	Description
Add Project	Allows administrators to add projects.
Edit Project	Allows administrators to edit, move, and reorder projects.
Delete Project	Allows administrators to delete projects.
Assign Privileges	Allows administrators to assign project-based privileges for groups or users for the selected project. As a prerequisite, the administrator must have the **Add Users** or the **Edit Users** system administration privilege.
Assign Roles	Allows administrators to assign users to roles for specific projects.
Edit General Properties	Allows administrators to modify **General** properties for selected projects.

Workflow Administration Privileges

The following information applies to workflow privileges:

- All selections apply to the selected workflow and inherited workflows unless inheritance is removed.
- Privileges are inherited through the workflow hierarchy, which allows you to set privileges once, rather than for each individual workflow. The **Inherit All Parent Workflow's Privileges** check box is selected by default; therefore, to grant a set of privileges for a particular workflow, clear the check box.

The following table provides a list and description of all the workflow administration privileges.

Note: All workflow administration privileges apply to on-premise and on-demand customers.

Privilege	Description
Edit Workflow	Allows administrators to edit workflows to add, edit, and delete selections for *User*, *Multi-User*, and *Multi-Group* fields and set default values for those fields. This privilege also allows administrators to manage notifications if they have been granted the **Add Notifications**, **Edit Notifications**, and **Delete Notifications** privileges located on the **Administration - System** page.
Edit Transitions	Allows administrators to view and modify transition restriction settings in projects assigned to the selected workflow.

Field Administration Privileges

Field privileges enable administrators to edit properties for specific fields for projects.

The following information applies to field privileges:

- All selections apply to the selected project and inherited projects unless inheritance is removed.
- Privileges are inherited through the project hierarchy, which allows you to set privileges once, rather than for each individual project. The **Inherit All Parent Project's Privileges** check box is selected by default; therefore, to grant a set of privileges for a particular project, clear the check box.

The following table provides a list and description of all the field administration privileges.

Note: All field administration privileges apply to on-premise and on-demand customers.

Privilege	Description
Override Ordering for Default Fields	Allows administrators to override field ordering for the selected project.
Edit Fields	Allows administrators to edit the selected field for the project. All fields in the primary table associated with the project are listed, except those that are in the Not Used fields section or that have been deleted.

Group Administration Privileges

Group privileges enable you to control which groups administrators can manage. All groups in the system are listed; select the groups that administrators can manage.

Use group privileges to limit administrative capabilities to a set of users by granting a managed administrator privileges to specific groups, and then assigning users to that group. This determines which users an administrator can control. For example, create a group called "IT Service Techs" and add three users to this group. Edit Bill Managed Administrator's account, and then select "IT Service Techs" on the **Administrator -**

Groups page. When Bill logs in to SBM Application Administrator, he can only administer the three users added to the "IT Service Techs" group.

Managed administrators can only edit the accounts of users added to groups selected on the **Groups** privileges page. This includes the ability to update these accounts using the Import Users feature.

Table Administration Privileges

Table privileges enable you to control which tables a managed administrator can administer in SBM System Administrator. All tables in the system are listed; select the table to grant administrative access to that table.

Deployment Privileges

Deployment privileges control deployment and promotion activities, such as creating environments in Application Repository, deploying process apps, and promoting applications to another SBM environment.

Tip: For guidance on granting deployment privileges, refer to Privileges Required for Application Configuration, Deployment, and Promotion [page 257].

Repository privileges control process app activities performed in Application Repository and SBM Composer, such as checking process apps in or out of the repository, and editing, publishing and deploying process apps. For details, refer to the *SBM Application Repository Guide*.

The following table provides a list and description of all deployment privileges.

Privilege	Description	On-premise Only
Create, Edit, and Delete Environments for This Host	Enables administrators to manage environments for this host in Application Repository.	✔
Deploy Process Apps to This Host	Enables administrators to deploy process apps and the applications they contain to this host.	
Delete Process Apps for This Host	Enables administrators to delete process apps that have been deployed to this host.	

Privilege	Description	On-premise Only
Deploy to This host From SBM Composer	Enables administrators to deploy process apps and their applications to this host from SBM Composer. All target servers and endpoints must be mapped, and on-premise customers must configure the environment for this host to allow deployments from SBM Composer. These settings are applied in Application Repository.	
Export Process Apps from This Host	Enables administrators to perform the "Get Process App From SBM Application Engine" task from Application Repository.	
Promote to This Host	*On-premise*: Enables administrators to promote process apps from another host to this host. Also enables administrators to promote individual application entities, such as reports and user accounts, that are contained in a process app. *On-demand*: Enables administrators to import solution files into Application Repository and promote them to the SBM Application Engine.  **Note:** Administrators must also have the "Deploy Process Apps to This Host" privilege.	
Create, Edit, and Delete Process App Endpoints for This Host	Enables administrators to manage process app endpoints for this host in Application Repository and SBM Composer.	

Privilege	Description	On-premise Only
Create, Edit, and Delete Process App Privileges	Enables administrators to set process app and application privileges in Application Repository. These privileges control access to process apps and applications in Application Repository and SBM Composer. This privilege must be set for administrators in the primary host for your SBM installation.	

Frequently Asked Questions About Managing Administrators

- **How do I create a primary system administrator?**

  In new on-premise systems, a primary system administrator is created using the **Create Database Wizard** in SBM System Administrator. This administrator can then log in to SBM Application Administrator and create additional administrators.

  To do so, add or edit a user account, and then grant Remote Administration product access to the user. Select the **Administration** tab, and then select administrative privileges as needed. For details on the different types of administrators and guidelines for setting them up, refer to Types of Administrators [page 255].

- **How do I grant administrative control over a set of users?**

  You can limit administrative capabilities to a set of users by granting a managed administrator privileges to specific groups, and then assigning users to that group. This determines which users an administrator can control. For example, create a group called "IT Service Techs" and add three users to this group. Edit Bill Managed Administrator's account, and then select "IT Service Techs" on the **Administrator - Groups** page. When Bill logs into SBM Application Administrator, he can only administer the three users added to the "IT Service Techs" group.

- **What happens if I forget my password, and I am the only administrator?**

  On-premise customers can open SBM System Administrator and run the **Reset Administrative Access Wizard**. This wizard can only be run when SBM System Administrator is connected to the database through an ODBC connection. For details, refer to the *SBM System Administrator Guide*.

  On-demand administrators who forget their password should contact customer support.

Chapter 7: Managing Notifications

The following topics describe how to administer notifications in Application Administrator.

About Notifications

Notifications provide a way to inform users when changes occur in the system. For example, you can create notifications that send an e-mail message to users when they are assigned an item or when an item is submitted.

Notifications are executed when certain events occur or conditions change in the system. Rules determine when notifications should be generated.

You can increase the importance of notifications by setting escalation parameters that repeat a notification, send an escalation notification if an action has not occurred within a specified time period, or delay a notification based on the value in a *Date/Time* fields. For details and examples, refer to About Escalations [page 271].

Notifications can also be used to automatically call Web service functions or run SBM AppScripts. This allows for a simple way to integrate with external applications, enabling you to easily import or export data when changes occur in SBM.

Notifications also provide automation for adding item links to and removing items from folders. For example, you can automatically add item links to an SBM Knowledge Base folder when support personnel add information to a specific field.

Key Benefits

- Push information to users as key data changes in the system.
- Notify managers if employees fail to act on items in a specified timeframe.
- Ensure items are not forgotten.

How Notifications Work

As users submit, update, and transition items in the system, the Notification Server processes notifications defined for workflows and auxiliary tables. Rules determine when notifications are generated.

Rules are evaluated during each Notification Server cycle, and when a rule becomes true, a notification is generated.

Common rule examples are:

- "I become the owner of an item" - This rule sends a notification to a user who is assigned an item.
- "Any item is closed" - This rule sends a notification to subscribers when items become inactive.
- "An item has not been acted upon since last week" - This rule sends a notification when an item has not changed state this week.

The most common use of notifications is to generate e-mail messages. For each notification, you can specify which users always receive an e-mail and which users can choose to subscribe or unsubscribe to the notification. You can customize the e-mail templates that are sent for each notification by including certain field data, notes and attachments related to a particular item, and a link to the item.

Users can also view their notifications in Serena Work Center.

Inheritance Guidelines

Notifications are created for workflows. Each notification applies to all projects assigned to a workflow and its sub-workflows, also referred to as child workflows. If you change the rule selection for a notification at a child workflow level, that selection applies to all workflows assigned to the child's parent.

Rules created in a parent workflow are inherited in any sub-workflows, but rules contained in sub-workflows can be overridden.

For example, at a parent workflow, you can create this rule:

"Any Item Changes State AND Customer Reported Is Equal to Yes."

You can override this rule for a sub-workflow as follows:

"Any Item Changes State AND Customer Reported Is Equal To No."

Changes made to the rule in the sub-workflow do not impact the rule in the parent workflow.

Editing a rule at the sub-workflow level overrides the rule's inherited properties. Any modifications you make apply to the selected workflow only.

Provided Notifications

To ease the process of implementing new process apps, a default set of notifications and notification rules are provided for each parent workflow in your application. The notifications and supporting rules are added after the first deployment of a new process app or on subsequent deployments after new parent workflows have been added.

The names of each notification and rule are prepended with the first letter of up to three words from the workflow name. For example, a workflow named "Software Development Workflow" would result in a SDW prefix for the provided notifications and rules. (If prefixes already exist in your system, subsequent prefixes are numbered, such as SDW1.) You can remove or modify this prefix as needed. The singular item name for your application is included in the name to indicate the type of item to which the notification refers.

By default, members of all groups in your system are allowed to subscribe to the provided notifications. You can modify these settings on the **Subscriptions** page for each notification. For details, refer to Notification Subscriptions [page 296].

The following notifications are provided for each workflow in a 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]

Tip: You can modify or delete the provided notifications and rules if you do not want to use them.

About Escalations

Escalations enable you to increase the importance of notifications by:

- Delaying notifications based on values in *Date/Time* fields.
- Sending an escalation notification if action has not occurred on an item within a specified time period.
- Repeating a notification.

Termination rules determine when escalation stops or does not occur. For example, you can create a rule for "Item Is Assigned." If an item is assigned before the rest of the escalation criteria becomes true, the escalation is not set.

To ensure that escalations are only sent during working times, you can specify a calendar that defines your organization's hours of operations. For example, if your organization operates from 9 a.m. to 5 p.m., Monday through Friday, escalations are only sent during these hours. For details on calendars, refer to About Calendars [page 390].

Delaying Notifications

Delay parameters enable you to send a notification based on the value of a *Date/Time* field. Rules determine when the timer begins for delayed notifications, which are fired after the specified delay.

Unlike other types of escalations, delayed notifications are triggered by a specified time value rather than a change to an item.

For example, when you send items to a "Review" state and specify a deadline of two weeks to complete the review, you can send a notification after one week to remind reviewers of their pending deadline. In this case, the rule for the notification would be "Items Sent to Review State" and the delay parameters would be "Due Date Is Less Than 1 Week."

For details on using delayed notifications, refer to Creating Delayed Notifications [page 278].

Sending Escalation Notifications Based on Inaction

Escalations allow one notification to send another notification based on an elapsed amount of time. A *Termination* rule stops an escalation from occurring.

For example, an e-mail notification is sent to an employee when an item is submitted into the system. If the employee does not act on the item within three days, an escalation notification is sent to the employee's manager.

For details, refer to Creating Escalation Notifications [page 280].

Repeating Notifications

Notifications can be sent repeatedly until a condition is met. The notification continues to be sent until the selected Termination rule is true. For example, you can set up a standard notification that sends an e-mail reminder to users every two days after they become the owner of a primary item. A Termination rule can be specified that stops sending the notification after the owner transitions the item to a new state.

For details, refer to Creating Repeating Notifications [page 279].

Combining Escalation Parameters

You can combine escalation parameters as needed. For example:

- You can send a notification to a service technician when an item has been assigned. You can repeat this notification day until the item is closed, and send an escalation notification to managers after three days.
- You can delay a notification for three days after the *When* rule becomes true, and then repeat this notification every two days until an item is closed.

Note: When you combine escalations based on inaction and repeating notifications, an Escalation notification is sent when the *Termination* rule is not met and the specified time interval for escalation has elapsed. If the *Termination* rule is true, the notification is no longer sent. The repeating notification is not sent after escalation has occurred.

About Rules and Conditions

Rules are the foundation of notifications because they determine when notifications are generated. There are two types of rules:

- **When Rules** - Determine when a notification will be generated. Before a notification can be generated, the set of conditions that make up the notification's rule must become true.
- **Termination Rules** - Determine when escalations should no longer be sent.

All rules consist of one or more conditions. Conditions are typically based on changes to field values, such as:

- "State Changes to Assigned"
- "Submit Date Changes"
- "Owner Changes From Current User"
- "Severity Changes to Critical"

You can also group conditions together to form more complex rules:

- "Any Item is Submitted AND Item Type Is Equal to Hardware Request AND Purchase Amount Is Greater Than 1,000"
- "State Changes to Closed AND (Manager Changes From Joe Manager OR Manager Changes From Samatha Manager)"

Common conditions for Termination rules are:

- "State Changes to Assigned"
- "Resolution Changes to Complete"
- "Attachment Is Added"

At the beginning of each Notification Server cycle, which is defined in the SBM Configurator, all changes to items that have occurred since the last cycle are evaluated against notification rules. Notifications are generated for each rule that became "true" in that cycle.

For details, refer to:

- Creating Rules [page 277]
- The Rules View [page 309]
- Condition Settings [page 311]

Conditions Guidelines

Consider the following information when you create conditions:

- When a *Sub-Relational* field is selected as the object, notifications are fired when the field's value is changed in an item using the workflow for which the rule is defined. For example, if your Issues workflow contains a relational field to the *Incidents* table and a *Sub-Relational* field to the *Company* field within that table, you can create a notification that fires when the selection in the issue changes the value of the *Incident Company* field.
- The (Current User) value is available for *User*, *Multi-User*, and *Multi-Group* field types. (Current User) enables you to create a rule that sends a notification to the current user selected for a field if that user has privileges to view an item and is subscribed to the notification. For example, the condition "Manager Is Equal To (Current User)" causes a notification to be sent to a particular user when that user is selected in the *Manager* field. For *Multi-User* fields, each selected user receives a notification. For *Multi-Group* fields, members of each selected group receive a notification.

  The following examples illustrate how you can use the (Current User) value in standard notifications. In these cases, Joe, Laura, and Samir have privileges to view, own, and submit items into a project. Newton only has privileges to submit items into the same project. All users are subscribed to receive e-mail notifications using the following rules:

  - State changes AND Owner is (Current User): Laura owns an item and its state changes. Only Laura receives an e-mail notification.

- State changes AND Submitter is not (Current User): Joe submits an item. Laura and Samir receive an e-mail notification when the item's state changes, but Joe does not.
- State changes AND Submitter is (Current User): Newton submits an item. Joe, Laura, and Samir do not receive a notification when the item changes state. Newton also does not receive a notification because he does not have privileges to view the item he submitted.

You can also use the (Current User) value to send escalation notifications to the correct users. For example, you can send an escalation notification to the owner of an item that has not been acted on in three days. In this case, the rule for the escalation notification should include the condition "Owner Is Equal To (Current User)." This rule ensures that the escalation is sent only to the owner of an item that has not been acted on in three days.

- You can use *Date/Time* keywords, such as *startof_last week*, as values for *Date/Time* fields. These keyword values are recalculated each time a condition is evaluated.
- Disabled selections for *Single Selection*, *Multi-Selection*, *Multi-User*, and *Multi-Group* fields are available and can be used to build rules. This enables you to build rules for a workflow when projects using that workflow have disabled field selections.
- You can create notifications that execute when work items are added to or removed from a backlog in Serena Work Center. You can also generate notifications when the priority changes for an item in a backlog. Rule conditions must be created for each backlog.

About Scheduled Report Notifications

A new scheduled report notification is created for each report that is scheduled to run at a specific time. Note that you cannot add scheduled report notifications in Application Administrator; you can only edit them after they have been created.

Tip: Each scheduled report that appears in Application Administrator includes the name of the user that created it. Use the list of scheduled reports to monitor the number of the scheduled reports that your users create.

You can edit scheduled report notifications to customize the name, description, and e-mail template that is used for each scheduled report e-mail.

In the **Notifications** view, filter your notifications by selecting **Scheduled Reports Only**, select the desired scheduled report notification, and then click **Details** to edit the e-mail template that is used for a particular user's scheduled report.

For more information about working with scheduled report notifications, see Scheduled Report Notification Settings [page 307].

Working With Notifications

The following sections explain how to create rules and different types of notifications.

- Creating Standard Notifications [page 275]
- Creating Rules [page 277]
- Creating Delayed Notifications [page 278]

Creating Standard Notifications

Prerequisites:

- The Notification Server must be configured and running. On-premise customers can do this in SBM Configurator. The Notification Server is configured automatically for on-demand customers.
- To receive e-mail notifications, users must have a valid e-mail address included in their user profile.
- Users can only receive e-mail notifications for items they have privileges to view.

Standard notifications are generated when conditions specified in the *When* rule become true.

To add or edit a standard notification:

1. From the **Administrator Portal**, select the **Notifications** icon.
2. Do one of the following:
   - To manage notifications for applications, select the process app for which you want to manage notifications from the **Process Apps/Applications** list.
   - To manage notifications for auxiliary tables, select **Auxiliary Tables** at the bottom of the pane.
3. Select the workflow or auxiliary table to which the notification is related.
4. Click one of the following options:
   - **Add** - Click to add a notification.
   - **Details** - Select a notification for a workflow or auxiliary table, and then click to edit it.
5. Provide a unique name for the notification, using the guidelines in Best Practices for Notifications and Escalations [page 322].
6. Provide an optional description.
7. Select a **Link Type**. The link type that you select is appended to the item URL that appears in the notification as described in General Notification Settings [page 288].

8. Select one of the following actions for the notification, and then apply settings based on that action:

   - **No Action**

     Select this option to disable actions for the notification or escalation.

   - **Send Broadcast Channel**

     Select this option to send e-mail messages using one or more broadcast channels (which are not bound to a specific user). For example, after you create a broadcast channel in the Channels view, you can select the new channel in the notification, and specify a user account that limits the message details according to the user's privileges. For details, refer to Broadcast Channel Action Options [page 290].

   - **Send E-mail/User Channel**

     Select this option to send messages to users by e-mail and optionally, one or more user channels. This action sends an e-mail message to subscribed users, and enables you to specify the fields that should appear in e-mail messages. To send messages to users via a user channel as well, you must add one or more channels to the notification. For details about sending e-mail messages, refer to E-mail and User Channel Action Options [page 291] and E-mail Field Settings [page 297]. For details about sending messages via a user channel, see E-mail and User Channel Action Options [page 291].

   - **Add Items to Folders**

     Select this option to add item links to folders. For example, you can add item links to a team's folder when a member of the team becomes the owner of an item. For details, refer to Folder Action Options [page 292].

   - **Remove Items From Folders**

     Select this option to remove item links from folders. For example, if you use a notification to add item links to a team's folder when a member of the team becomes the owner of an item, you can use another notification to remove links from the folder when the team member is no longer responsible for the item. For details, refer to Folder Action Options [page 292].

   - **Raise Event**

     Select this option to execute an event as a specific user in connection with the item that triggered the notification. For example, you can have the system send an event to the Orchestration Engine, which can then execute an orchestration workflow when a notification rule becomes true. The change history will show that the changes were invoked by the user that you specified. For details, refer to Raise Event [page 292].

   - **Run Script**

     (On-premise only.) Select this option to run an SBM AppScript. Run an SBM AppScript imported into SBM Composer and deployed to this environment when a notification rule becomes true. The script is executed once for each user subscribed to the notification. Each time the script is executed, the shell property `Shell.User` is set to the user name. If no users are subscribed to the notification, the script is executed only once and the shell property Shell.User will

be blank. For details, refer to the *SBM AppScript Reference*. For details, refer to Script Action Options [page 292].

- **Run Transition**

  Select this option to perform a transition as a specific user against the item that triggered the notification. For example, when the item reaches a certain state, you can have the system perform a transition against the item when a notification rule becomes true. The change history will show that the transition was executed by the user that you specified. For details, refer to Run Transition [page 293].

- **Run Web Service**

  Select this option to call a Web service function. You must first import a Web service definition or WSDL, into SBM Composer, and deploy the associated application to this environment. For details, refer to Web Service Action Options [page 294].

9. Select a *When* rule that causes the notification to be sent. You can also click the plus (+) sign to create a new rule. For details, refer to About Rules and Conditions [page 272].
10. Save your changes.
11. Subscribe users to the notification. For details, refer to Notification Subscriptions [page 296].
12. For notifications that send e-mail, specify which fields should appear in the e-mail message. The `$FIELDS()` tag must be included in the template used by the notification. For details, refer to $FIELDS() [page 450].
13. Save your changes.

Creating Rules

Rules can be added at any level in the workflow hierarchy or for any auxiliary table. When you create rules for primary items, you can add a rule at the Base Workflow level so that it is inherited by any further derived workflows for that primary item, or application, type. You can then override the rule in sub-workflows.

Tip: For organizational purposes, it is often better to create a rule at the workflow level where the rule will be used.

Use the following steps for creating *When* rules, which determine when a notification will be generated, and *Termination* rules, which determine when escalations will stop being sent.

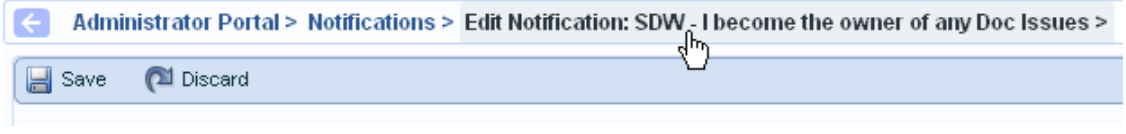
To create a rule:

1. From the **Administrator Portal**, select the **Notifications** icon.
2. Do one of the following:
   - Add or edit a notification for a workflow or auxiliary table, and then click the plus sign located to the right of the **When** list.

- Select the **Rules** button on the **Notifications view** toolbar, select a workflow or auxiliary table, and then click **Add**.

  Tip: To create a rule that can be used by all workflows in a process app, select **All Workflows** at the top of the **Process Apps/ Applications** list, and then click **Add**.

3. In the **Title** box, provide a name for the rule. For best results, the name should clearly state the rule's purpose, such as "Critical Item Is Closed."
4. In the conditions area, create one or more conditions that make up the rule. For example, "Severity Is Equal to Critical" and "State Changes to Closed" could be conditions for the "Critical Item Is Closed" rule. For guidance on defining conditions, refer to Condition Settings [page 311].
5. As each condition is defined, click **Add** to add it to the list. To reorder conditions, select one in the list and then move it up or down.
6. Add operators and parentheses to further refine the rule. For the example above, use the "And" operator to combine the two conditions.
7. Save your changes.
8. If you created the rule from within a notification, select the name in the breadcrumb links to return to the notification.



Creating Delayed Notifications

You can delay notifications based on the value of a *Date/Time* field rather than on a specific change in an item. These notifications can serve as reminders for users to act on items.

For example, you may want to send a notification to employees when the due date for a work item has passed. If the item has been closed before the due date, the notification is not sent. In this case, the timer for the delay is started when the work item is assigned to the user, the delay parameter is "Due Date Is Greater Than 1 Day," and the *Termination* rule is "Item Is Closed."

For details, refer to:

- About Escalations [page 271]
- Escalation Settings [page 294]

To create a delayed notification:

1. Create or edit the notification that you want to be delayed. (For guidance, refer to Creating Standard Notifications [page 275].)
2. Select the **Escalations** tab.

3. In the **Termination Rule** area, select or create a rule that stops the delay timer. In the example above, the *Termination rule* might be "Item Is Closed." For details, refer to About Rules and Conditions [page 272].
4. In the **Delay Parameters** section, select the **Delay** check box.
5. Set delay parameters as follows:
   - **Send when interval between** - Indicates the beginning of the delay period.
   - **Date/Time field** - Select the *Date/Time* field used to calculate the delay period. Note that only *Date/Time* fields set to store date and time values can be used. Those that store elapsed time and time of day values do not apply to delayed notifications.
   - **And current date becomes** - Select the delay interval in minutes, hours, days, and weeks.
6. Optionally, select a calendar from the list to calculate the delay interval. For example, you may not want weekends included in the delay period. If you select a calendar that reflects operational hours of Monday through Friday from 9 a.m. to 5 p.m, an 8-hour delay interval that begins at 2 p.m. Friday ends on Monday at 1 p.m. By default, a 24-hour calendar is selected. For details, refer to About Calendars [page 390].
7. Save your changes.
8. Select the **Subscriptions** tab, and then verify that the correct users are subscribed to the delayed notification.

Tip: Be sure to verify subscribers have permissions to view items on which the notification is based.

Creating Repeating Notifications

You can configure a notification so that it generates repeatedly until a *Termination* rule becomes true. For example, you can send a service technician an "I Am Assigned a Problem Ticket" every two days until the item is closed.

For details, refer to:

- About Escalations [page 271]
- Escalation Settings [page 294]

To create a repeating notification:

1. Create or edit the notification that you want to send repeatedly. (For guidance, refer to Creating Standard Notifications [page 275].)
2. Select the **Escalations** tab.
3. In the **Termination Rule** area, select or create a rule that stops the repeated notifications from generating. In the example above, the *Termination* rule might be "Item Is Closed." For details, refer to About Rules and Conditions [page 272].
4. In the **Repeat Action Parameters** section, select the **Repeat** check box.

5. In the **Every** area, specify the time interval for repeating the notification until the selected *Termination* rule becomes true.
6. Optionally, select a calendar from the list to calculate the repeat time interval. For example, you may not want to generate repeat notifications on weekends. If you select a calendar that reflects operational hours of Monday through Friday from 9 a.m. to 5 p.m, an 8-hour period that begins at 2 p.m. Friday repeats on Monday at 1 p.m. By default, a 24-hour calendar is selected. For details, refer to About Calendars [page 390].
7. Save your changes.
8. Select the **Subscriptions** tab, and then verify that the correct users are subscribed to the repeated notification.

Tip: Be sure to verify subscribers have permissions to view items on which the notification is based.

Creating Escalation Notifications

One notification can send another notification if action has not been taken on an item. The subsequent notification sent is referred to as an escalation notification.

For example, a critical ticket is assigned to a service technician and the "I Become the Owner of a Critical Service Ticket" notification is sent to the technician. The ticket is not resolved after three days, so a separate "Critical Issue Is Not Resolved" notification is sent to a manager. This separate notification is referred to as an escalation notification, but the escalation parameters are defined in the "I Become the Owner of a Critical Service Ticket" notification.

Escalation notifications are generated according to escalation parameters specified in an initiating notification. Therefore, escalation notifications must be created separately from their initiating notifications.

Ideally, you should create the escalation notification before you set escalation parameters in the initiating notification. You will select the escalation notification from the **Invoke** list when you define your escalation parameters.

For details, refer to:

- About Escalations [page 271]
- Escalation Settings [page 294]

To create an escalation notification:

1. Create the rule and escalation notification that will be sent when the escalation conditions become true. This process is the same as creating a standard notification, except you must select the **Escalation** check box on the **General** tab.
2. Save your changes to the escalation notification.
3. Create or edit the notification from which you want escalations to be sent. (For guidance, refer to Creating Standard Notifications [page 275].)
4. Select the **Escalations** tab.

5. In the **Termination Rule** area, select or create a rule that prevents the escalation notification from generating. In the example above, the *Termination rule* might be "Item Is Resolved." For details, refer to About Rules and Conditions [page 272].
6. In the **Escalation Parameters** section, select the **Escalation** check box.
7. In the **After** area, specify a time interval for escalation. For example, if you specify "3 days," and the *Termination* rule is not met and three days pass, an escalation is sent.
8. To apply a specific set of hours to the escalation period, select a calendar from the list. For details on using calendars, refer to About Calendars [page 390].
9. From the **Invoke** list, select the escalation notification you created in steps 1 through 3. In the example above, you would select "Critical Issue Is Not Resolved." (If you have not yet created this notification, click the plus sign.)

   Tip: Be sure to verify that users are subscribed to both this notification and the escalation notification selected in the **Invoke** list. Also, verify that subscribers have permissions to view the items on which the escalation is based.
10. Save your changes.

Finding Notifications and Rules

As time goes on, the number of notifications in your system may grow and it may be difficult to locate specific notifications or rules. SBM offers several ways to search for them.

Note: Notification searches are dependent on the workflow or auxiliary table related to the notification. You must first select the workflow or auxiliary table related to a notification before you can search for the notification by name. Searches are case-insensitive.

- **To find notifications in applications:**
  1. In the **Notifications** view, select the **Workflow Name** icon ( ) located next to the **Search** box.
  2. Type the name of the workflow, and then select it in the results list.
  3. Select the **Notification Name** icon ( ).
  4. Search for the notification by name.
  5. Select the notification in the results list, and then click **Details** to open and edit it.
- **To find notifications in auxiliary tables:**
  1. In the **Notifications** view, select **Auxiliary Tables** at the bottom of the left pane.
  2. Select the table that contains the notification.

3. With the table selected, search for the notification by name.
4. Select the notification in the results list, and then click **Details** to open and edit it.

- **To find rules from within a notification:**
  1. Select a notification, and then click **Details**.
  2. On the **General** page, search for a rule by name in the **When** box.
  3. Click the **Search** icon.
  4. Select a rule from the list.

     Note: Only rules applicable to the notification's workflow or table are returned.

- **To find rules from the Notifications view:**
  1. In the **Notifications** view, select **Rules**.
  2. To find rules for applications, select the **Workflow Name** icon () located next to the **Search** box.
  3. Type the name of the workflow, and then select it in the results list.

     Note: To search for a rule in an auxiliary table, first select the specific table.

  4. Select the **Rule Name** icon (), and then search for the rule by name.
  5. Select the rule in the results list, and then click **Details** to open and edit it.
- **To find which notifications use a specific rule:**
  1. In **Rules** view, search for the rule you need.
  2. Select the rule. The related notifications are listed in the bottom pane.
  3. Double-click a notification to open and edit it.
- **To find notifications sent as escalations:**

  One notification can send another notification if action has not been taken on an item. The subsequent notification sent is referred to as an escalation notification.

  When you select an escalation notification in the **Notifications** list, the orignial notification on which escalation is based is listed in the **Related Notifications** list.
- **To find notifications that do not have subscribers:**

  In the **Notifications** view with a list of notifications visible, change the **All** filter to **No Subscribers**.
- **To find rules that are not assigned to notifications:**

  In **Rules** view, change the **All** filter to **Not Used**.

Creating Notification E-mail Templates

SBM Application Administrator enables you to create and modify templates for notification e-mails. You can create text or HTML templates; a WYSIWYG editor is available for formatting HTML templates and quickly adding template tags to text and HTML templates.

You can use existing e-mail templates, modify these templates, or create new ones. By default, three templates are available:

- **default.txt** – A standard text template
- **default.html** - A standard HTML template
- **external.txt** - A text template intended for auto-reply notifications

You should use HTML templates if users will apply Rich Text formatting to *Text* fields that are included in notifications.

Note: Notification e-mail templates are stored in the SBM database and must be modified in SBM Application Administrator.

You can manage templates from the global Templates view (Global Mailbox View [page 439]) or for a specific notification. If you create a global template, you must assign the template to specific notifications.

To add or edit e-mail templates for notifications:

1. From the **Administrator Portal**, select the **Notifications** icon.
2. Edit a notification that sends e-mail messages as its action.
3. In the **E-mail Options** section, select an existing template from the list and click the edit icon to edit it, or click the plus sign to add a template. The **E-mail Template Editor** opens.
4. For new templates, provide a name for new template in the **Template Name** box.
5. Enter text, e-mail template tags, and HTML formatting (if applicable) into the editor, or click **Editor** to open a WYSIWYG editor.

   Tip: Click the **Template Tag** icon () to insert SBM-specific tags into the template. Click the **Fields** icon () to insert fields into the template. The field's values will be returned in the e-mail notification.
6. Save your changes.

Calling Web Services From Notifications

You can use notifications to call functions from external Web services to update SBM items or to send SBM data to third-party or custom applications that offer Web services.

For each notification, you can call a Web service function for notification rules based on primary and auxiliary items. You can map the function's input and output parameters to SBM fields.

Note: You can select a single function for each notification, but you can assign a function to multiple notifications.

Consider the following information:

- Support for development efforts with custom programs written using Web services is provided by Professional Services. Questions regarding Web services operations as documented are handled by Serena Customer Support.
- Web services must be imported into SBM Composer as part of a process app before they can be associated with a notification.
- Authentication for Web services is specified for the service's endpoint in Application Repository.
- SBM calls are synchronous. SBM waits for Web services calls to return, or for the specified time-out period to expire. If you need asynchronous calls, consider using orchestrations to call Web services. For details, refer to the *SBM Orchestration Guide*.
- Input data is passed to the Web service in UTF-8.
- Output data from the Web service is assumed to be in UTF-8.
- Managed administrators must have the **Associate Web Services/Scripts with Notifications** administration privilege to select the Run Web Service as an action choice for notifications.

Assigning Web Service Functions to Notifications

To call a Web service from a notification:

1. In SBM Composer, import a Web service into an application, and then publish and deploy the application's process app to the SBM Application Engine.
2. In SBM Application Administrator, select the **Notifications** icon on the **Administrator Portal**.
3. Create or edit a notification.
4. From the **Action** list, select **Run Web Service**.
5. From the **When** list, select the condition that must become true for the notification to execute.
6. In the Web Service area, click the **Select Function** button. The **Select Web Service Function** page opens.
7. Select the function to call for the notification, and then click **OK**.
8. Click the **Map Inputs/Outputs** button.
9. Map Web service parameters to fields or set fixed values. For guidance, refer to:

- Mapping Web Service Function Parameters to SBM Fields [page 302]
- Web Service Mapping Settings [page 300]
- Enumeration Mapping Settings [page 306]

10. Click **OK**.
11. In the **On Script/Web Service Failure** area, select the **Retry Every** check box, and then type the number of cycles that should elapse before the Notification Server retries the notification.
12. Select the **Quit After** check box, and then type a number in the **attempts** box to specify the number of times the Notification Server should attempt to execute the Web message. By default, the Notification Server will stop retrying the notification after one attempt.
13. Save your changes.

Notification Settings

The following sections discuss notification settings:

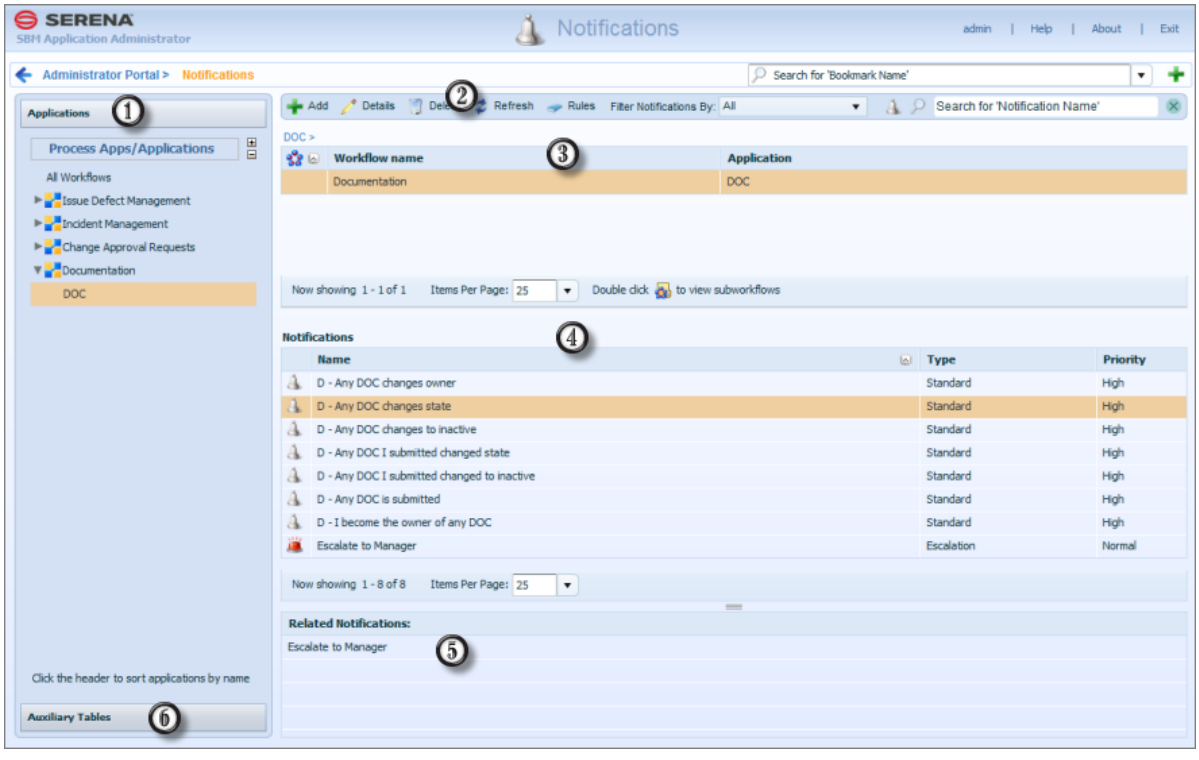
- The Notifications View [page 286]
- The Rules View [page 309]
- Escalation Settings [page 294]
- Notification Subscriptions [page 296]
- E-mail Field Settings [page 297]
- E-mail Responses [page 298]
- About the E-mail Template Editor [page 443]

The Notifications View

The **Notifications** view enables you to add, edit, and delete notifications. You can also open the **Rules** view.

To open the **Notifications** view, click the **Notifications** icon on the **Administrator Portal**.

The **Notifications** view has the following parts:



1. **Applications**
   To work with notifications based on primary tables, use this list to navigate through process apps and their corresponding applications. Expand and collapse the nodes to navigate through the tree. Click the **Process Apps/Applications** link to sort the list alphabetically. Select an application to open its associated workflows in the **Workflow** list.

   Note: To add a notification at the base workflow level, select **All Workflows** at the top of the **Process Apps/Applications** list, and then click **Add**. You must then select a rule that applies to a specific workflow.

2. **Notifications Toolbar**

   - **Add**

     Select a workflow or auxiliary table, and then click to add a notification. For details, refer to Creating Standard Notifications [page 275].

   - **Details**

     Select a workflow or auxiliary table, and a notification, and then click to edit the notification.

- **Delete**

  Select a workflow or an auxiliary table, select one or more notifications, and then click **Delete**.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Rules**

  Click to open the **Rules** view and manage *When* rules used by notifications and *Termination* rules used by escalations. For details, refer to The Rules View [page 309].

- **Filter Notification By**
  List all notifications for a selected workflow or auxiliary table, limit the list to those which have no subscribers, or return only scheduled report notifications.

  Tip: A new scheduled report notification is created for each report that your users schedule. You can edit these notifications to customize the e-mail template that is used for each scheduled report e-mail. Filter your notifications by selecting **Scheduled Reports Only**, select the desired notification, and then click **Details** to edit the e-mail template that is used for a particular user's scheduled report.

- **Search**

  Select the **Search** icon to search for workflows or notifications by name. For tips on searching for notifications, refer to Finding Notifications and Rules [page 281].

3. **Workflow List**

   When you select an application, this pane lists the workflows associated with that application. Click the column headers to sort the list by workflow name. Select a workflow to view its associated notifications.

4. **Notifications List**

   Lists the notifications associated with the selected workflow or auxiliary table. Click the column headers to sort the list by notification name, type, or priority.

5. **Related Notifications**

   When you select an escalation notification in the **Notifications** list, the original notification on which escalation is based is listed in the **Related Notifications** list. For example, a notification is generated when a critical item is submitted. An escalation is sent if the critical item has not been assigned within two days. When you select this escalation in the **Notifications** list, the original "Critical Item Has Been Submitted" notification is listed in the **Related Notifications** list.

6. **Auxiliary Tables**

   To work with notifications based on auxiliary tables, click **Auxiliary Tables**, and then select a table.

7. **Notification System Settings**

Enables on-demand customers to apply notification settings for their SBM instance. On-premise customers apply these settings in the SBM Configurator. For details, refer to Notification System Settings (On-demand Only) [page 308]

Tip:

Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

General Notification Settings

The following options are available on the **General** page when you add or edit a notification or escalation:

- General Settings [page 288]
- Broadcast Channel Action Options [page 290]
- E-mail and User Channel Action Options [page 291]
- Folder Action Options [page 292]
- Raise Event [page 292]
- Script Action Options [page 292]
- Run Transition [page 293]
- Web Service Action Options [page 294]

For details about working with scheduled report notifications, see Scheduled Report Notification Settings [page 307].

General Settings

- **Escalation**

  Select this check box if the notification will be sent as an escalation notification. In other words, the notification will be selected from the **Invoke** list on the **Escalation** tab for a standard notification. For details, refer to Creating Escalation Notifications [page 280].

- **Name**

  Indicates the unique name for the notification, which appears in the e-mail message if the `$NOTIFICATION()` e-mail template tag is included in the template used by the notification. For details, refer to $NOTIFICATION() [page 456].

- **Description**

  Optional descriptive information about the notification.

- **Action**

  Indicates one of the following actions taken by the notification when its rule conditions become true:

  - **No Action**

Select this option to disable actions for the notification or escalation.

- **Send Broadcast Channel**

  Select this option to send e-mail messages using one or more broadcast channels (which are not bound to a specific user). For example, after you create a broadcast channel in the Channels view, you can select the new channel in the notification, and specify a user account that limits the message details according to the user's privileges. For details, refer to Broadcast Channel Action Options [page 290].

- **Send E-mail/User Channel**

  Select this option to send messages to users by e-mail and optionally, one or more user channels. This action sends an e-mail message to subscribed users, and enables you to specify the fields that should appear in e-mail messages. To send messages to users via a user channel as well, you must add one or more channels to the notification. For details about sending e-mail messages, refer to E-mail and User Channel Action Options [page 291] and E-mail Field Settings [page 297]. For details about sending messages via a user channel, see E-mail and User Channel Action Options [page 291].

- **Add Items to Folders**

  Select this option to add item links to folders. For example, you can add item links to a team's folder when a member of the team becomes the owner of an item. For details, refer to Folder Action Options [page 292].

- **Remove Items From Folders**

  Select this option to remove item links from folders. For example, if you use a notification to add item links to a team's folder when a member of the team becomes the owner of an item, you can use another notification to remove links from the folder when the team member is no longer responsible for the item. For details, refer to Folder Action Options [page 292].

- **Raise Event**

  Select this option to execute an event as a specific user in connection with the item that triggered the notification. For example, you can have the system send an event to the Orchestration Engine, which can then execute an orchestration workflow when a notification rule becomes true. The change history will show that the changes were invoked by the user that you specified. For details, refer to Raise Event [page 292].

- **Run Script**

  (On-premise only.) Select this option to run an SBM AppScript. Run an SBM AppScript imported into SBM Composer and deployed to this environment when a notification rule becomes true. The script is executed once for each user subscribed to the notification. Each time the script is executed, the shell property `Shell.User` is set to the user name. If no users are subscribed to the notification, the script is executed only once and the shell property Shell.User will be blank. For details, refer to the *SBM AppScript Reference*. For details, refer to Script Action Options [page 292].

- **Run Transition**

Select this option to perform a transition as a specific user against the item that triggered the notification. For example, when the item reaches a certain state, you can have the system perform a transition against the item when a notification rule becomes true. The change history will show that the transition was executed by the user that you specified. For details, refer to Run Transition [page 293].

- **Run Web Service**

  Select this option to call a Web service function. You must first import a Web service definition or WSDL, into SBM Composer, and deploy the associated application to this environment. For details, refer to Web Service Action Options [page 294].

- **When**
  Select the rule that causes the notification to generate. For details, refer to About Rules and Conditions [page 272] and Creating Rules [page 277].

  Tip: To create a rule for the notification, click the plus sign. To edit the notification assigned to a rule, click the edit icon.

Broadcast Channel Action Options

When you select **Send Broadcast Channel** from the **Action** list, the following options are available:

- **Link Type**
  Indicates which interface should open when users click the item link in e-mail notifications. Choose one of the following options:

  - SBM User Workspace

    Opens to the SBM User Workspace. For example: `http://host/tmtrack/tmtrack.dll?View&I=9&T=1011`.

  - Serena Work Center

    Opens to the Serena Work Center. For example: `http://host/tmtrack/tmtrack.dll?shell=swc&View&I=9&T=1011`.

  The following link type is only available if you have Serena Service Manager installed:

  - **Request Center**

    Opens Serena Request Center. For example: `http://host/tmtrack/tmtrack.dll?shell=srp&View&I=9&T=1011`.

- **Priority**

  Select a priority for the notification message. The priority appears in the notification message depending on the selected broadcast channel.

- **Add New Channel**

  Click this button to add more broadcast channels for the notification message.

- **Channel**

Select or search for the broadcast channel that will be used for the notification message.

- **Message Template**
  Select an existing template from the list and click the edit icon to edit it, or click the plus sign to add a template. Click the trash can to delete a selected template. For details on modifying templates, refer to Creating Notification E-mail Templates [page 283].

  Note: Select an HTML template if users will apply Rich Text formatting to *Text* fields that are included in the notification.

- **User**

  Enter or search for a user account that will act as a template to limit the message details according to the user's privileges. For example, if the broadcast message should only show field information that Joe can view (according to his privileges), select Joe in the drop-down list.

E-mail and User Channel Action Options

When you select **Send E-mail/User Channel** from the **Action** list, the following options are available:

- **Link Type**
  Indicates which interface should open when users click the item link in e-mail notifications. Choose one of the following options:

  - SBM User Workspace

    Opens to the SBM User Workspace. For example: `http://host/tmtrack/tmtrack.dll?View&I=9&T=1011`.

  - Serena Work Center

    Opens to the Serena Work Center. For example: `http://host/tmtrack/tmtrack.dll?shell=swc&View&I=9&T=1011`.

  The following link type is only available if you have Serena Service Manager installed:

  - **Request Center**

    Opens Serena Request Center. For example: `http://host/tmtrack/tmtrack.dll?shell=srp&View&I=9&T=1011`.

- **Related Notifications**

  Lists notifications used by the e-mail template.

- **Priority**

  Select a priority for the notification e-mail message. Depending on the recipient's e-mail client and the type of e-mail server used by your system, the priority appears in the e-mail notification. The appearance of the selected priority depends on the receiving e-mail client; for example, in in some mail clients, "Highest" and "High" priority selections appear as an exclamation point. In others, the selected priority appears as text.

- **Add New Channel**

  Click this button to add one or more user channels for the notification message.

- **Channel**

  Select the channel for the notification message. The default channel is [Send E-mail].

- **Message Template**
  Select an existing template from the list and click the edit icon to edit it, or click the plus sign to add a template. Click the trash can to delete a selected template. For details on modifying templates, refer to Creating Notification E-mail Templates [page 283].

  Note: For each notification, you choose a text or HTML e-mail template, but you cannot choose both formats for a single notification.

Folder Action Options

When you select **Add Item To Folder** or **Remove Item From Folder** from the **Action** list, you must choose a system Favorite, Public, or Knowledge Base folder from the **Destination Folder** list. Public and Knowledge Base folders are created in SBM System Administrator. Folders must be configured to allow items to be added to them and users need privileges to view items in the folders to see the item links.

Raise Event

When you select **Raise Event** from the **Action** list, the following options are available:

- **Event to Execute**

  Select an existing event that will be executed when the rule becomes true. For example, you could select an event that fires an orchestration that updates the item via the UpdateItem Web service call, and then creates one or more copies of the item.

- **Execution Context**

  Select a user or a *User* field that defines the execution context. For example, you can either search for a user that has privilege to perform the orchestration, or you can select a *User* field in the orchestration that contains the privileged user. The actions that are performed when the rule becomes true will be executed in the context of the user that is provided in either case.

Script Action Options

When you select **Run Script** from the **Action** list, the following options are available:

- **Script to Execute**

  (On-premise only.) SBM AppScripts deployed to your environment are available. Ensure that the SBM AppScript you select is valid for the selected notification rule.

- **Retry Every n Cycles**

  Specify the number of cycles that should elapse before the Notification Server retries the notification.

- **Quit After n Attempts**

With the **Retry Every n Cycles** check box selected, specify a number of attempts the Notification Server should retry to process the script or Web service. The Notification Server will stop attempting when the notification is successfully executed. By default, the Notification Server will stop retrying the notification after one attempt.

Run Transition

When you select **Run Transition** from the **Action** list, the following options are available:

- **Initial State**

  Select the state that the item must be in before the transition can execute. You can leave this field empty to perform the selected transition if it is applicable to the item at the time the rule becomes true. All transitions in the workflow appear if you leave **Initial State** empty.

  Tip: Click the **Show Workflow** button that appears when you select **Run Transition** to view a diagram of the workflow that is associated with the notification. You can use this diagram to help you select states and their available transitions.

- **Transition to Execute**

  Select the transition that should be executed when the item is in the selected state.

- **Execution Context**

  Select a user or a *User* field that defines the execution context (who performs the transition). For example, you can either search for a user that has privilege to perform the transition, or you can select a *User* field in the application that contains the privileged user. The transition that is performed when the rule becomes true will be executed in the context of the user that is provided in either case. The change history will show that the transition was executed by the specified user.

- **Field**

  Select a field from the application that should be updated during the transition. Read-only fields that you cannot update are marked with a green asterisk. Required fields are marked with a red asterisk.

  You can filter the list of fields by **Required Only** and **Read Only** attributes. For example, to return required fields that must have a valid value in order for the transition to succeed, select the **Required Only** check box. To view fields that are read only, select **Read Only**.

- **Value**
  Select or enter a value for the field. Click **Map** to set the value for the selected field. The field to be updated and the value that will be applies during the transition appear below. Continue selecting fields and mapping values until all the fields you want to update (and all the required fields) are mapped. Select a mapping and click **Unmap** to undo the mapping, or **Unmap All** to undo all your previous field value mappings.

  Note: Carefully review the changes that the transition will apply. For example, if you specify that a transition should update the Description field, all existing text in the Description field is replaced unless you have set the Append Only attribute on the field.

Web Service Action Options

When you select **Run Web Service** from the **Action** list, the following options are available:

- **Select Function**

  Click to select a Web service function that has been imported into SBM Composer and deployed to this environment.

- **Map Inputs/Outputs**

  Once you have a Web service function selected, click this button to map inputs and outputs. For details, refer to:

  - Mapping Web Service Function Parameters to SBM Fields [page 302]
  - Web Service Mapping Settings [page 300]
  - Enumeration Mapping Settings [page 306]

- **Retry Every n Cycles**

  Specify the number of cycles that should elapse before the Notification Server retries the notification.

- **Quit After n Attempts**

  With the **Retry Every n Cycles** check box selected, specify a number of attempts the Notification Server should retry to process the script or Web service. The Notification Server will stop attempting when the notification is successfully executed. By default, the Notification Server will stop retrying the notification after one attempt.

Escalation Settings

Escalations can be used to increase the importance of a notification. You can:

- Delay notifications based on values in *Date/Time* fields. For details, refer to Creating Delayed Notifications [page 278].
- Send notifications repeatedly until a *Termination* rule becomes true. For details, refer to Creating Repeating Notifications [page 279].
- Allow one notification to send a different notification based on defined rules, such as an item not being assigned to a service technician after three days. For details, refer to Creating Escalation Notifications [page 280].

The following settings are available on the **Escalations** page:

- **Termination Rule**

  Select the rule that prompts the Notification Server to stop sending repeat notifications, delayed notifications, and escalation messages. For details, refer to About Rules and Conditions [page 272].

  Tip: To create a termination rule, click the plus sign. To edit the rule assigned to the notification, click the edit icon.

- **Delay Parameters**

  Use these settings to specify an amount of time the notification should be delayed after the When rule becomes true.

  - **Delay**

    Select this check box to enable notification delay settings.

  - **Send when interval between...**
    Select a *Date/time* field, the value of which indicates the beginning of the delay period.

    Note: Only *Date/Time* fields set to store date and time values can be used. Those that store elapsed time and time of day values do not apply to delayed notifications.

  - **And current date becomes**

    Select the delay interval in minutes, hours, days, and weeks.

  - **Calendar**

    Select a calendar from the list to determine the time frame in which the delay is calculated. For example, you may want to stop the delay timer on weekends or holidays. By default, a 24-hour calendar is selected. For details on working with calendars, refer to About Calendars [page 390].

  - **Stop When**

    Indicates when the delay timer stops.

- **Repeat Action Parameters**

  Use these settings to send a notification repeatedly until the Termination rule becomes true.

  - **Repeat**

    Select this check box to enable repeat settings.

  - **Every...**

    Specify the amount of elapsed time in minutes, hours, days, and weeks before the notification is repeated.

  - **Calendar**

    Select a calendar from the list to calculate the time before a notification is repeated. For example, you may not want to generate repeat notifications on weekends. If you select a calendar that reflects operational hours of Monday through Friday from 9 a.m. to 5 p.m, an 8-hour period that begins at 2 p.m. Friday repeats on Monday at 1 p.m. By default, a 24-hour calendar is selected. For details on working with calendars, refer to About Calendars [page 390].

  - **Stop When**

    Indicates when the delay timer stops.

- **Escalation Paramters**

  Use these settings to send another notification after a specified amount of time.

- **Escalate**

  Select this check box to enable escalation parameters.

- **After**

  Specify a time interval for escalation. For example, if you specify "7 days," and the "Unless" Termination rule is not met and seven days pass, the notification selected in the **Invoke** list is sent.

- **Invoke**

  Select the notification that should be sent when the escalation parameters are valid. Click the plus sign to add a notification.

Notification Subscriptions

The **Subscriptions** page enables you to subscribe users and group members to notifications and escalations.

First, select the following options to filter the list:

- **Object Type**

  Select users or groups to change the list of potential subscribers to users or groups.

- **View External Users**

  Select this check box to add users and groups with external product access to the list.

- **View Occasional Users**

  Select this check box to add users and groups with occasional product access to the list.

- **Search**

  If the **Users** option is selected, search for users to subscribe to the notification. If the **Groups** groups option is selected, search for groups to subscribe members to the notification. Searches are case-insensitive.

Note: External users cannot subscribe to notifications themselves, so you must set their subscriptions.

Then, select the following options as they apply:

- **Channel**

  Select an associated channel. If you add one or more user channels to the notification, select a channel in the drop-down list and manage the subscriptions for that channel. You manage subscriptions for e-mail messages separately from messages that are sent through user channels.

- **Notify**

  Always deliver a notification to selected users or groups. Users or group members cannot unsubscribe from these notifications.

- **Allow to Subscribe**

Enables users or group members to subscribe to the notification in their user profile. Selected users and groups can also subscribe to Item Notifications, which are available in the **Actions** list for individual items.

- **Subscribe**
  Subscribes the selected users or groups to notifications. Users and group members can later unsubscribe from these notifications in their user profile.

  Note: If users were subscribed to a notification as part of their group membership, the name of the group is listed in the **Subscribe** column.

To manage notification subscriptions for several users at once:

- Use the **Set All** drop-down list to select all of the users in the **Notify**, **Allow to Subscribe**, or **Subscribe** columns.
- Use the **Clear All** drop-down list to clear all of the selected users in the **Notify**, **Allow to Subscribe**, or **Subscribe** columns.

E-mail Field Settings

The **Fields** page enables you to select the fields to display in an e-mail notification when the `$FIELDS()` tag is included in the selected e-mail template. For details on e-mail template tags, refer to E-mail Template Tags [page 444].

Note: The **Fields** page is only available when "Send E-mail" is selected from the **Action** list on the **General** page.

Field Settings for Notifications Based on Workflows

The following options are available on the **Fields** page for notifications based on workflows:

- **Privilege Section**

  Filter the list of fields in the grid by selecting a privilege section from the list.

- **Inherit Parent Field Selections**

  Select this check box to inherit from the parent workflow the list of fields that will appear in the e-mail notification. For notifications in sub-workflows, clear this check box to include a specific set of fields in the e-mail notification. When you modify field selections in a sub-workflow, inheritance is automatically broken. When you select this check box for notifications in parent workflows, all field check boxes are cleared, but you can add fields as needed.

- **Workflow Name**

  Select the workflow that pertains to the notification.

- **Search**

  Search for fields by name. Searches are case-insensitive.

- **Fields List**

Lists the fields, by section, available for the workflow upon which the notification's rule is based. Select the fields that should appear in the e-mail generated by the notification.

Note: Users receiving the notification must have privileges to view the fields. If they do not, the fields appear as asterisks in the e-mail message.

Field Settings for Notifications Based on Auxiliary Items

The following options are available on the **Fields** page for notifications based on auxiliary items:

- **Privilege Section**

  Filter the list of fields in the grid by selecting a privilege section from the list.

- **Search**

  Search for fields by name. Searches are case-insensitive.

- **Fields List**
  Lists the fields, by section, available for the table upon which the notification's rule is based. Select the fields that should appear in the e-mail generated by the notification.

  Note: Users receiving the notification must have privileges to view the fields. If they do not, the fields appear as asterisks in the e-mail message.

E-mail Responses

The **E-mail Responses** page enables you to configure response options for a notification. Response options can appear as links or buttons in a notification message, which enable the recipient to transition an item without requiring him or her to log in.

For example, you can create a notification that contains "Approve" or "Reject" links that a manager can use to quickly approve or reject a vacation request while it is in the Pending Approval state. The manager does not need to provide any login credentials to invoke these transitions. The manager simply approves or rejects the request directly from the notification message by clicking one of the response options. This launches a new browser window, and a confirmation message appears if the transition succeeds. If the item is no longer in an applicable state, a failure message appears.

Note the following important information:

- The **E-mail Responses** tab only appears in the **Notifications** view if the notification's action is set to **Send E-mail User Channel**.
- When the notification rule becomes true, the message is sent to the subscribed user. The recipient must have a valid e-mail address and privilege to transition the item.
- The response options invoke one or more available quick transitions in the item's workflow that are valid for the item's current state. The transitions that you use for responses must be quick transitions.
- The recipient is not required to log in to transition the item; instead, the responses each contain a unique expiring token that is embedded in the URL, which grants the recipient the ability to execute the quick transition. Because the user does not have

to log in, no license is used. This token cannot be reused in any way, and only grants the recipient the ability to perform the associated quick transition. If the recipient attempts to respond after the designated expiration time has passed, he or she must enter login credentials to access the item and perform the transition.

On-premise customers can configure the expiration time for the token in the Mail Servers tab in SBM Configurator. For details, refer to the *SBM Installation and Configuration Guide*. On-demand customers can configure this setting in the **Notification System Settings** tab in the **Notifications** view in Application Administrator.

To add a new response:

1. Select the **E-mail Responses** tab.
2. Click **Add new response**.
3. Enter a **Name** for the response. This name acts as an alias for the transition that will be executed. Take note of the name you provide; you will need to use it with the $EMAILRESPONSE() tag that you add to the Notification e-mail template.
4. Select the **Initial State**. This is the item's state from which the quick transitions are available.
5. Select a **Transition to Execute** for this response. This is the quick transition that maps to the response that you create. Only quick transitions that are applicable to the **Initial State** appear in the drop-down list.

   Tip: Click **Show Workflow** to view an image of the workflow. This is helpful if you want to view the state and its available transitions.
6. Click **Save** to save your changes.
7. Click **Add new response** to add another response option, if necessary.
8. After you define the responses, you must add the $EMAILRESPONSE() tag and the response options that you create to a new or existing Notification e-mail template, and select that template in the notification. For details, refer to Notification Tags [page 445].

Tip: You can customize the success or failure message template that appears in the browser. On the Application Engine server, navigate to *installationDirectory*\Serena\SBM\Application Engine\templates, edit the emailapproval template as necessary, and save your changes. Open SBM System Administrator and perform a **Put Files in Database** operation to save the modified template in the database. For more information on customizing templates, see the *SBM System Administrator Guide*.

Web Service Functions

The **Web Service Function** page lists all of the Web service definitions, or WSDLs, imported into SBM from SBM Composer. Each function contained in the WSDL is also shown. To view details about a selected function, click **Details**.

Note: After you select a function, click **OK** to return to the **Notifications - General** page, and then select the **Map Inputs/Outputs** button.

The following information is available for each function:

- **Function Name**

  Indicates the name of the selected function.

- **Service Name**

  Indicates the name of the WSDL.

- **Description**

  Provides the description defined in the WSDL.

- **Input/Output Parameters**

  Lists the inputs and outputs for the function.

For details on using Web services with notifications, refer to:

- Calling Web Services From Notifications [page 283]
- Mapping Web Service Function Parameters to SBM Fields [page 302]
- Web Service Mapping Settings [page 300]
- Enumeration Mapping Settings [page 306]

Web Service Mapping Settings

Use the **Map Web Service Function Parameters** page to map application fields to Web service inputs and outputs. You can choose to map only inputs or outputs, or to not map fields and execute a Web service without exchanging data between the Web service and SBM.

The following options are available on the **Map Web Service Function Parameters** page:

- **Inputs**

  Select this tab to map Web service inputs to SBM. When the Web service function is called, values in the mapped SBM fields are passed to the service.

- **Outputs**

  Select this tab to map Web service outputs to SBM fields. When the Web service function is called, values from the Web service are passed to mapped SBM fields.

- **Function Name**

  Indicates the name of the Web service function selected for the notification.

- **Service Name**

  Indicates the name of the WSDL.

- **Process App Fields**
  Lists the fields available for mapping based on the workflow or auxiliary table of the notification's *When* rule. You can map inputs and outputs to all fields, except those in the Deleted Fields and Not Used field sections.

  Note: You can map individual elements of Web service complex types to individual application fields. Complex types appear in a tree structure.

- **Web Service Inputs/Outputs**

  Lists the available inputs or outputs for the selected Web service function.

- **Map**

  Select an SBM field and a compatible Web service input or output, and then click **Map**. For guidance on mapping, refer to Input Data Mapping [page 302] and Output Data Mapping [page 304].

- **Unmap**

  Select a mapped field, and then click to unmap.

- **Unmap All**

  Click to unmap all mapped fields.

- **Configure Mapping**

  If you map compatible SBM fields to Web service enumerations, the **Configure Mapping** button is enabled. Click this button to map selections to enumeration types. For details, refer to Enumeration Mapping Settings [page 306].

- **Set Value**

  You can assign fixed values to Web service inputs for the following data types:

  - Text
  - Numeric
  - Boolean
  - Enumeration
  - Date/Time

  This enables you to control the data that is passed to the Web service, and to pass data other than values in SBM fields. You can specify a fixed value or map a field, but you cannot do both.

  To map fixed input values, select the data type from the **Web Service Inputs** list, select **Set Value**, and select:

  - **Value**
    Type a fixed input value. For Date/Time types, the value is expected to be in coordinated universal time (UTC). For example:

- 2007-04-28T12:30:00, which is interpreted as 12:30 p.m., April 28, 2007
- 2007-04-28, which is interpreted as April 28, 2007
- 2007-04-28T12:30:00Z, which explicitly specifies UTC
- 2007-04-28T12:30:00+6:00, which is a 6-hour offset from 12:30 p.m., April 28, 2007

- **Context Param**

  From the list, select one of the internal parameters to pass to the Web service. Choices are Login ID, Unique ID (Table ID:Item ID), Item ID, Table ID, or User ID.

Mapping Web Service Function Parameters to SBM Fields

The following sections provide guidance for mapping Web service inputs and outputs to SBM fields.

Input Data Mapping

The following table lists the allowable mapping between Web service inputs and SBM fields. When the Web service function is called, values in the mapped SBM fields are passed to the service.

The following considerations apply to mapping SBM fields to Web service inputs:

- When you map to *Text* fields set as Journal fields, all data from the field is passed to the Web service.
- *Summation* fields cannot be mapped to Web service inputs.

Unless otherwise noted, SBM field types are referenced in this table as follows:

- **Single selection-type fields** – Refers to *Single Selection*, *User*, and *Folder* fields, as well as the system *State* field and system *Project* field.
- **Multiple selection-type fields** – Refers to *Multi-Selection*, *Multi-Group*, *Multi-Relational*, and *Multi-User* fields.

Web Service Input Data Type	Allowable SBM Field Mapping	Notes
Boolean	Binary/ Trinary	For *Binary/Trinary* fields set as check boxes, "true" or "false" are mapped. Listbox and radio button labels are mapped.
Date/Time	Date/Time	*Date/Time* field values are converted to XML date/time format. Coordinated universal time (UTC) is assumed.

Web Service Input Data Type	Allowable SBM Field Mapping	Notes
Enumeration	Single selection-type fields	For details, refer to Enumeration Mapping Settings [page 306].
List Types	Multiple selection-type fields	For multiple selection-type fields, selected values are passed to the Web service as a comma-separated string.
Number (including floating point)	Binary/ Trinary Date/Time Numeric Single selection-type fields Single Relational Sub-Relational	For *Binary/Trinary* fields, 1 or 0 are passed to the Web service. For *Date/Time* fields, integers are interpreted as a modified julian date, which is the number of seconds since Jan. 1, 1970 in UTC. For *Numeric* fields, truncation could occur if the SBM field is set as a floating point and is mapped to a Web service integer input. For *Single Relational* fields, the TS_ID from the relational field table is passed to the input as the data value. For single selection-type fields, the TS_ID from the TS_SELECTIONS table is passed to the input as the data value. For *Sub-Relational* fields, SBM passes the database value of the field in the related item. If this value is text, SBM passes 0 to the Web service.

Web Service Input Data Type	Allowable SBM Field Mapping	Notes
Text	Binary/ Trinary Date/Time Single Relational Single selection-type fields Multiple selection-type fields Numeric Text Sub-Relational	For *Binary/Trinary* fields set as check boxes, "true" or "false" are mapped. Listbox and radio button labels are mapped. For *Date/Time* fields, strings must be in XML date/time format and are assumed to be in coordinated universal time (UTC). For single selection-type fields and *Single Relational* fields, the field display value is passed to the Web service as a string. For multiple selection-type fields, selected values are passed to the Web service as a comma-separated string. For *Numeric* and *Text* fields, the values are passed as text. For *Sub-Relational* fields, SBM passes the display value to the Web service.

Output Data Mapping

You can map Web service outputs to application fields based on the following information. When the function is called, data in fields mapped to the inputs is passed to the service; the Web service passes data back based on output field mappings.

Consider the following information when mapping Web service outputs to application fields:

- You can only map one application field to each Web service output.
- Depending on your workflow configuration, the Web service may overwrite default values for fields mapped to Web service outputs. Field dependencies may also be ignored. For example, if a Web service runs for a post-transition context, default field values that are specified for the transition are overwritten by values sent from the Web service.
- When mapping Web service outputs to selection-type fields, invalid values passed by the Web service are dropped. For example, if the Web service passes a value of "Defect" to the mapped Item Type field, that value is dropped if "Defect" is not a valid selection for that field. For best results, map fields that allow single selections, such as *User* and *Single Selection* fields, to Web service enumerations to ensure that values are properly mapped. For details, refer to Enumeration Mapping Settings [page 306].
- When you map to *Text* fields set as Journal fields, data from the Web service replaces existing text, even if you have the Append Only check box selected for the field.

- *Summation* and *Sub-Relational* fields cannot be mapped to Web service outputs.

Unless otherwise noted, SBM field types are referenced in the following table as:

- **Single selection-type fields** – Refers to *Single Selection*, *User*, and *Folder* fields, as well as the system State field and system Project field.
- **Multiple selection-type fields** – *Multi-Selection*, *Multi-Group*, *Multi-Relational*, and *Multi-User* fields.

Web Service Output Data Type	Allowable SBM Field Mapping	Notes
Boolean	Binary/ Trinary Numeric Text	For *Binary/Trinary* fields, True maps to 0; false maps to 1. Trinary field values are never returned by the Web service. For *Numeric* fields, 0 maps to 1; non-zero maps to 0. For *Text* fields, "True" or "False" values are returned by the Web service.
Date/time	Date/Time Text	For *Date/Time* fields, returned strings are assumed to be in coordinated universal time (UTC). For *Text* fields, the returned string is added in XML date/ time format.
Enumerations	Single selection-type fields Text	For single selection-type fields, enumeration types are matched to selection field values by name. If the Web service sends a value that is not valid for a mapped field, the value is dropped. For best results, map all enumerations to selection field values. For *Text* fields, the Web service enumeration type is added to the field as text.
List Types	Multiple selection-type fields Text	For multiple selection-type fields, each item in the list that matches a selection value is passed by the Web service. Items that do not match SBM selection values are dropped. Matching is by selection name. For *Text* fields, each item in the list is separated by a comma, and the entire list is added to the *Text* field.

Web Service Output Data Type	Allowable SBM Field Mapping	Notes
Number (including floating point)	Binary/ Trinary Date/Time Numeric Text Single Relational Single selection-type fields	For *Binary/Trinary* fields, "true" is mapped to the first value; "false" is mapped to the second value. The first and second values are specified on the **Options** page for the *Binary/Trinary* field. For *Date/Time* fields, integers are interpreted as a modified Julian date, which is the number of seconds since Jan. 1, 1970 in UTC. For *Numeric* fields, truncation could occur if the SBM field is set as a floating point and is mapped to a Web service integer output. For *Text* fields, the Web service numeric value is added to the field as text. For single selection-type fields and *Single Relational* fields, numbers are interpreted as the selection's TS_ID.
Text	Multiple selection-type fields Numeric Single selection-type fields Single Relational Text	For multiple selection-type fields, values must be passed as a comma-separated string. For single selection-type fields and *Single Relational* fields, data passed from the Web service must match the display value of the SBM selection. For *Numeric* fields, non-numeric values are passed as zero. For *Text* fields, exact text passed by the Web service is added to the SBM field.

Enumeration Mapping Settings

You can map Web service enumerations to the following SBM fields:

- Single Selection
- User
- Folder
- System State field
- System Project field

This enables you to control the data that is passed between the Web service and SBM and ensures that valid selections are passed to SBM items by the Web service.

Considerations for mapping enumeration types to selection field values:

- SBM automatically maps similar enumeration types and selection field values. Matches are based on text and are case insensitive. You can modify this mapping as needed.
- Unmapped outputs are set to "none."
- When the *State* and *Project* fields are mapped to Web service enumeration types and the fields contain duplicate values, the first named selection and enumeration pair that match are automatically mapped.
- You can map multiple outputs to a single input. For example, you can map multiple Web service output types to a single selection.
- You can map Web service enumeration types to disabled field selections. Data is passed as if the field selection were enabled.

Scheduled Report Notification Settings

The following options are available on the **General** page when you edit a scheduled report notification:

- General Settings [page 307]
- E-mail Options [page 307]

General Settings

- **Name**

  Indicates the unique name for the notification, which is used to uniquely identify a scheduled report by user name and and report name.

- **Description**

  Optional descriptive information about the notification.

E-mail Options

A new scheduled report notification is created for each report that your users schedule. All scheduled report e-mail notifications can use the same e-mail template, or you can customize the e-mail template for each scheduled report that your users create.

You can manage templates from the global Templates view (Global Mailbox View [page 439]) or for a specific scheduled report notification. If you create a global template, you must assign the template to specific scheduled report notification.

Important: The scheduled report e-mail templates are used to inform the recipient that report succeeded or failed to run. Therefore, all of the scheduled report e-mail template tags must be present in the e-mail template.

- **E-mail Template**

Select an existing template from the list and click the edit icon to edit it, or click the plus sign to add a template. Click the trash can to delete a selected template.

Note: You cannot delete the default scheduled report e-mail templates (`sr_scheduled_reports.txt` and `sr_scheduled_reports.htm`).

Note: For each notification, you choose a text or HTML e-mail template, but you cannot choose both formats for a single notification.

To add or edit e-mail templates for scheduled report notifications:

1. In the **E-mail Options** section, select an existing template from the list and click the edit icon to edit it, or click the plus sign to add a template. The **E-mail Template Editor** opens.
2. For new templates, provide a name for new template in the **Template Name** box.
3. Enter text, e-mail template tags, and HTML formatting (if applicable) into the editor, or click **Editor** to open a WYSIWYG editor.

   Tip: Click the **Template Tag** icon ( ) to insert SBM-specific tags into the template. Click the **Fields** icon ( ) to insert fields into the template. The field's values will be returned in the e-mail notification.
4. Save your changes.

Notification System Settings (On-demand Only)

Serena On-demand customers can modify the following options for their instance.

- **External server**

  Enter the external server name or address to include an HTTP link to items in the body of e-mail notifications. The $LINK() tag must also be included in the body of the notification e-mail template.

- **External server port** – Enter the port number for the external address. The port number appears in the external HTTP link that is included in the Notification Server e-mail messages if you provide an **External server** address.

- **E-mail Submission - Attach HTML E-mail as PDF**

  Select this check box to attach "text/html" formatted e-mails as PDF attachments to the item (in addition to the field mappings you define for the mailbox). This option is useful if incoming e-mails contain HTML and embedded images because text and image sequence are preserved.

- **Notification token expiration timeout**

  Set the default time for Expired Notification Tokens that are used in e-mail responses. For more information, refer to E-mail Responses [page 298].

For on-demand customers that have installed and configured Hybrid SSO, you can use the following settings to configure the link address that appears in your notifications.

Important: On-demand customers that are not using Hybrid SSO should not change these settings. These settings override the HTTP link that appears in notifications. The default address and port that is configured by Serena should be used unless you have installed and configured Hybrid SSO.

- **Web server**

  Enter the name or address of the Hybrid SSO server to include an HTTP link to items in the body of e-mail notifications. The $LINK() tag must also be included in the body of the notification e-mail template.

- **Web server port**

  Enter the Hybrid SSO server port number. The port number appears in the HTTP links that are included in the Notification Server e-mail messages. The default port value is 80.

- **E-mail Recorder - Attach HTML E-mail as PDF**

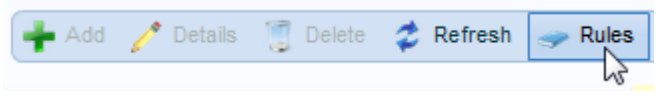
  Select this check box to attach "text/html" formatted e-mails as PDF attachments to the item. This option is useful if incoming e-mails contain HTML and embedded images because text and image sequence are preserved.

To edit options that are not check boxes, select a setting, and then click **Details** to enter a new **Value** in the **System Settings Editor** dialog box. Click **Apply** to save your changes.

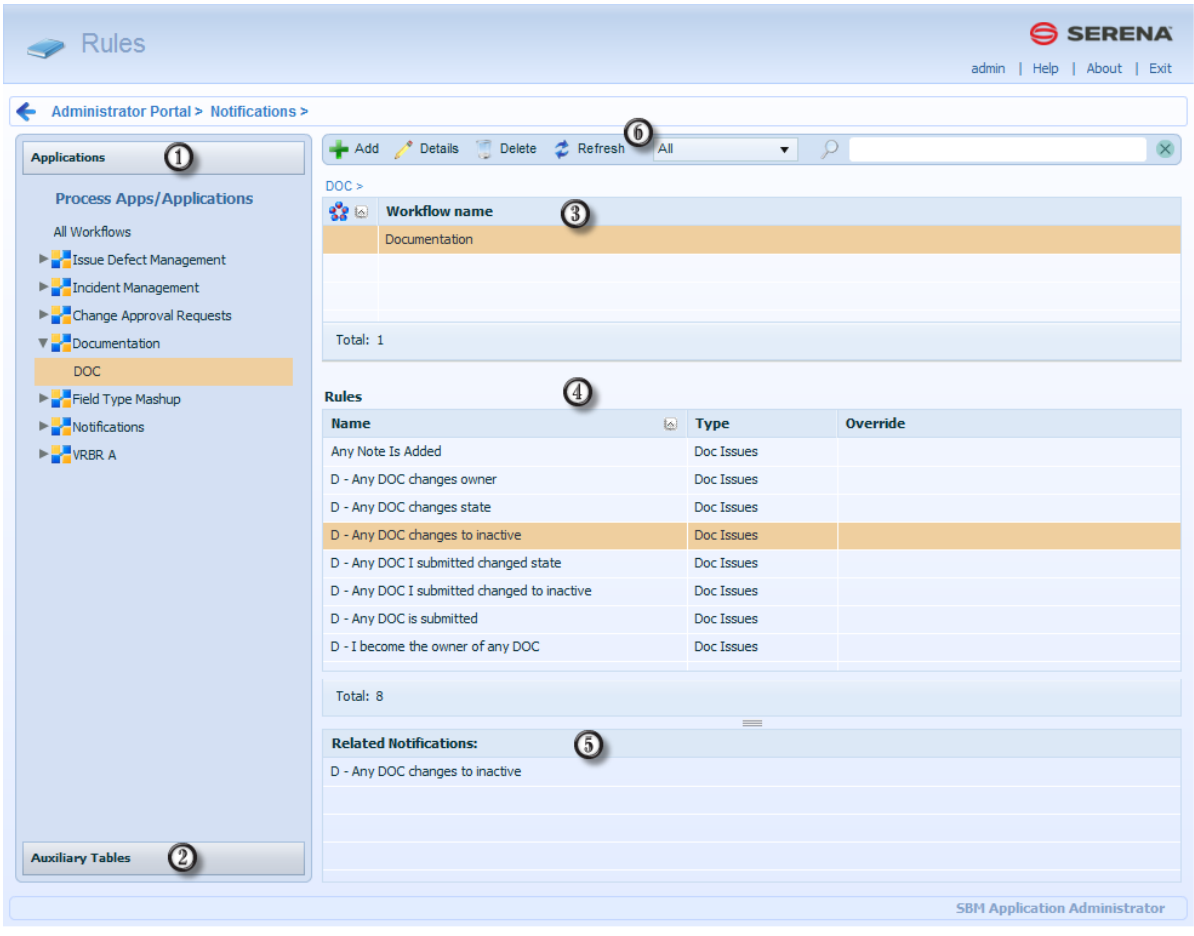
The Rules View

The **Rules** view enables you to add, edit, and delete *When* rules used by notifications and *Termination* rules used by escalations.

To open the **Rules** view, click the **Notifications** icon on the **Administrator Portal**, and then select **Rules**, as shown below.



The **Rules** view has the following parts:



1. **Applications**

   To work with rules based on primary tables, use the Applications list to navigate through process apps and their corresponding applications. Expand and collapse the nodes to navigate through the tree. Select an application to open its associated workflows in the **Workflow** list.

2. **Auxiliary Tables**

   To work with rules based on auxiliary tables, click **Auxiliary Tables**, and then select a table. All additions, modifications, or deletions of rules apply to the selected table.

3. **Workflow List**

   Lists the workflows associated with a selected application. Click the column headers to sort the list by workflow name. The Workflow list is only available for notifications based on primary tables, and all additions, modifications, or deletions of rules apply to the selected workflow.

4. **Rules List**

   Lists the rules associated with the selected workflow or auxiliary table. Click the column headers to sort the list by rule name.

5. **Related Notifications**

   Lists the notifications assigned to the selected rule. Double-click the notification to edit it.

6. **Rules Toolbar**

   - **Add**

     Select a workflow or auxiliary table, and then click to add a rule. For details, refer to Creating Rules [page 277].

   - **Details**

     Select a parent workflow or auxiliary table and a rule, and then click to edit the rule. Rules created in a parent workflow are inherited in any sub-workflows. You can edit a rule at the workflow level at which it was created.

   - **Override**

     Select a sub-workflow and a rule, and then click **Override** to override inherited rules. Overrides apply to the selected workflow only.

   - **Delete**
     You can delete rules as long as they are not being used by a notification. Select a workflow or an auxiliary table, and a rule, and then click **Delete**.

     Note: Rules pertaining to primary items can only be deleted in the workflow in which they were created. For example, rules created in a parent workflow and inherited by sub-workflows can only be deleted at the parent workflow level. The rule is then deleted in any sub-workflows as well.

   - **Refresh**

     Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

   - **Filter**

     List all rules for the selected workflow or auxiliary table, or limit the list to those that are not used by any notifications.

   - **Search**

     Search for a rule by name. Searches are case-insensitive. Results are listed by name and application type.

Tip:

Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Condition Settings

Use the **Conditions** page to define conditions for a rule. When the conditions become true based on changes in the system, a notification is generated.

The following settings are available on the **Conditions** page:

- **Title**

  Provide a name for the rule. The name should clearly indicate the rule's purpose so it can be used by multiple notifications, if applicable.

- **Workflow/Auxiliary Table**

  Indicates the workflow or auxiliary table for which the rule is defined.

- **Override**

  Rule modifications made at a child workflow level are considered overrides. In this case, you can modify conditions for the rule, but you cannot change the name or workflow assignment. For details, refer to Inheritance Guidelines [page 270].

- **Conditions**
  The following options are provided for defining conditions.

Option	Description	Example
Operator	Use to join two or more conditions together.	A rule becomes true when any item is closed *and* the resolution was a software change. Object = Any Item Comparison = Is Value = Closed **Operator = And** Object = Resolution Comparison = Is Equal To Value = Software Change
Open Parentheses	Use to set the precedence of conditions.	

Option	Description	Example
Object	Use to select which data will change to determine when the rule becomes true. Primary and auxiliary items are specified in the **Object** list as Any (primary or auxiliary item name), such as in Any issue or Any company. Most objects in the list are generated from the fields associated with the selected workflow or auxiliary table. The non-field object Attachment is included, however, to allow notifications to be sent when attachments are added to or deleted from an item, including attachments added to *Text* fields using the Rich Text Editor. Note that attachments include notes, e-mail messages, files, URLs, and item links. The "Any Paused/Unpaused Issue" operator is a non-field object that you can use to build rules for items that are paused or unpaused from Serena Demand Manager. Note that this operator is available even if you do not add the *Pause Status* system field to your primary table in SBM Composer. The "Transition" operator is a non-field object that you can use to send notifications when a certain transition occurs. For example, to send a notification when the Close transition occurs, select the "Transition" operator, the "Is" comparison, and the "Close" transition from the value drop-down list.	A rule becomes true when the estimated time to fix an issue is more than five days. *Estimated Time to Fix* is a field associated with the selected workflow and contains a date/time value. **Object = Est. Time to Fix** Comparison = Is Greater Than Value = 120:00:00 The date/time value stored in the *Estimated Time to Fix* field for the issue is compared with the value 120:00:00. If the date/time of the *Estimated Time to Fix* field is more than 120:00:00 hours, a notification is sent.
Comparison	Use to evaluate the selected object and selected value. Comparisons that appear in the list are determined by the type of field selected as the object. For details, refer to Condition Comparisons [page 315].	A rule becomes true when the priority of an incident changes to critical. Object = Priority **Comparison = Changes To** Value = Critical

Option	Description	Example
Value	Used to compare the selected object and the selected value. For most field types, a value is selected from the list. You must type the exact comparison value for *Text, Single Relational, Multi-Relational, Numeric,* and *Summation* fields, as well as *Sub-Relational* fields based on those field types. Text entered for comparison values must be case sensitive.	A rule might have the conditions that when the state of an item changes to resolved and the submitter of the item is a particular user, a notification is sent. Object = State Comparison = Changes To **Value = Resolved** Operator = And Object = Submitter Comparison = Is Equal To **Value = <Current User>**
Closed Parentheses	Use to set the precedence of conditions.	

- **Add**

  After specifying an object, comparison, and value for each condition, click **Add** to add it to the rule.

- **Move**

  Select a condition, and then click the **Move** options to reorder conditions as needed.

- **Modify**

  Select a condition, change the object, comparison, and value as needed, and then click **Modify**.

- **Remove**

  Select a condition, and then click to remove it from the list.

Condition Comparisons

The following table describes each of the available comparisons, lists the applicable field types, and provides an example of how to use each comparison.

Note: Unless noted in the following table, comparisons for *Sub-Relational* fields are based on sub-fields. For example, the applicable comparisons for a *Sub-Relational* field with a *Single Selection* as its sub-type are the same as those for *Single Selection* fields.

Comparison	Description	Field Types	Example
Added	Becomes true if the new value of an object contains the item selected in the **Value** list and the previous value did not.	Multi-Group, Multi-Selection, and Multi-User.	Object = Change in Version(s) **Comparison = Added** Value = V4.5 A notification is generated when the value **V4.5** is added to the *Change in Version(s)* field.
Added to Backlog	Becomes true when items are added to a specific backlog in Serena Work Center.	Any Item object (Primary items only)	Object = Any Work Item **Comparison = Added to backlog** Value = Sprint 1 Backlog A notification is generated when any work item is added to the Sprint 1 Backlog.
Changes	Becomes true when the selected object's value changes.	Binary/Trinary, Date/Time (except Elapsed Time), Folder, Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Numeric, Single-Relational, Single Selection, Text and User. Also Any Item, Note, and Attachment objects.	Object = Owner **Comparison = Changes** A notification is generated when the owner changes for an item.

Comparison	Description	Field Types	Example
Changes From	Becomes true when a new value for the object changes from the selected value.	Binary/Trinary, Folder, Multi-Relational, Single-Relational, Single Selection, Text, and User	Object = Engineer **Comparison = Changes From** Value = Laura Engineer A notification is generated when the value of the *Engineer* field changes from Laura Engineer to another value.
Changes From (None)	Becomes true when a field is given a value after it had no selected value.	Binary/Trinary, Folder, Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Numeric, Single Relational, Single Selection, Text, and User.	Object = Customer **Comparison = Changes From (None)** Value = ACME A notification is generated when the *Customer* field is given a value.
Changes To	Becomes true when a new value for the object changes to the selected value.	Binary/Trinary, Folder, Multi-Relational, Single-Relational, Single Selection, Text, and User	Object = Engineer **Comparison = Changes To** Value = Laura Engineer A notification is generated when the value of the *Engineer* field changes to Laura Engineer.

Comparison	Description	Field Types	Example
Changes to (None)	Becomes true when all values are removed from a field.	Binary/Trinary, Folder, Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Numeric, Single Relational, Single Selection, Text, and User.	Object = Targeted Release **Comparison = Changes To (None)** With this condition, a notification is generated when a value is removed from the *Target Release* field. This may indicate that a work item is no longer planned.
Changes to Paused	Becomes true when an item's *Pause Status* changes to Paused.	"Any Paused/ Unpaused Issue" object.	Object = Any Paused/ Unpaused Issue **Comparison = Changes To Paused** Value = Paused by Demand Manager A notification is generated when Serena Demand Manager changes the value of the *Pause Status* field on an item to Paused.

Comparison	Description	Field Types	Example
Changes to Unpaused	Becomes true when an item's *Pause Status* changes to Unpaused.	"Any Paused/ Unpaused Issue" object.	Object = Any Paused/ Unpaused Issue **Comparison = Changes To Unpaused** Value = Approved by Demand Manager OR Value = Rejected by Demand Manager A notification is generated when Serena Demand Manager changes the value of the *Pause Status* field on an item to Unpaused because the item is approved or rejected.
Contains	Becomes true if the current value of an object contains the selected value. This condition is evaluated for any records indicated as a change in the change history.	Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Single-Relational, and Text	Object = Description **Comparison = Contains** Value = XML A notification is generated when an item that contains the term "XML" in the *Description* field changes.

Comparison	Description	Field Types	Example
Is	Becomes true if the specified change is made to an item, or when the Transition operator is used, and the selected transition is executed.	Any Item, Note, and Attachment objects, and Transition objects	Object = Attachment **Comparison = Is** Value = Added A notification is generated when an attachment is added to an item. Or: Object = Transition **Comparison = Is** Value = Close A notification is generated when the close transition is executed.
Is (None)	Becomes true when the object has no specified value.	Binary/Trinary, Folder, Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Numeric, Single Relational, Single Selection, Text, and User	Object = Customer Priority **Comparison = Is (None)** A notification is generated when the *Customer Priority* field does not have a value.
Is Not (None)	Becomes true when the object is given a value.	Binary/Trinary, Folder, Multi-Group, Multi-Relational, Multi-Selection, Multi-User, Numeric, Single Relational, Single Selection, Text, and User	Object = Approver **Comparison = Is Not (None)** A notification is generated when a user is selected in the *Approver* field.

Comparison	Description	Field Types	Example
Is Equal To	Becomes true when the value of the object is equal to the selected value.	Binary/Trinary, Date/Time, Folder, Multi-Relational, Numeric, Single-Relational, Single Selection, Summation, Text, and User	Object = Issue Type **Comparison = Is Equal to** Value = Bug Report With this condition, a notification is generated when an item changes and the value in the *Issue Type* field is Bug Report.
Is Greater or Equal	Becomes true when the value of the object is greater than or equal to the selected value.	Numeric and Summation	Object = Price **Comparison = Is Greater or Equal** Value = 5.00 Anotification is generated when an item changes and the value in the *Price* field is greater than or equal to 5.00.
Is Greater Than	Becomes true when the value of the object is greater than the selected value.	Date/Time, Numeric, and Summation	Object = Submit Date **Comparison = Is Greater Than** Value = 10/1/2011 A notification is generated when an item changes and the Submit Date is greater than 10/1/2011.

Comparison	Description	Field Types	Example
Is Less or Equal	Becomes true when the value of the object is less than or equal to the selected value.	Numeric and Summation	Object = Price **Comparison = Is Less or Equal** Value = 5.00 A notification is generated when an item changes and the value in the *Price* field is less than or equal to 5.00.
Is Less Than	Becomes true when the value of the object is less than the selected value.	Date/Time, Numeric, and Summation	Object = Submit Date **Comparison = Is Less Than** Value = 10/1/2011 A notification is generated when an item changes and the Submit Date is earlier than 10/1/2011.
Priority changed in	Becomes true when the priority changes for any item in the specified backlog.	Any Item object (Primary items only)	Object = Any Object **Comparison = Priority changed in** Value = Backlog Sprint 1 A notification is the priority changes for any item in Backlog Sprint 1.

Comparison	Description	Field Types	Example
Removed	Becomes true if the specified value is removed from the field.	Multi-Group, Multi-Selection, and Multi-User	Object = Change in Version(s) **Comparison = Removed** Value = V4.5 A notification is generated when the value **V4.5** is removed from the *Change in Version(s)* field.
Removed from backlog	Becomes true when any item is removed from the specified backlog.	Any Item object (Primary items only)	Object = Any Item **Comparison = Removed from backlog** Value = Sprint 1 A notification is generated any item is removed from the Sprint 1 backlog.

Best Practices for Notifications and Escalations

Notification and Rule Names

- Notification and rule names must be unique across all applications and auxiliary tables.
- The notification name will appear in e-mails using templates with the `$NOTIFICATION()` template tag. For details, refer to $NOTIFICATION() [page 456].
- For newly deployed workflows, several notifications and rules are provided, and the names of each notification and rule are prepended with the first letter of up to three words from the workflow name. You can remove these prefixes as needed, but they do help organize your notifications and rules when an application has multiple workflows.
- If you have an escalation that is supposed to stop when an item is closed (moved to an inactive state), the termination rule could be ignored if two transitions are executed in close succession (such as **Resolve** and then **Close**) because the escalation is being created and closed in one notification cycle. In this scenario, consider adding a condition like **AND NOT Active/Inactive Is Equal to Inactive** to the end of your initial notification rule. This will cause the **Close** transition to be used as a terminator, thereby ensuring that the notification is not sent repeatedly.

E-mail Template Maintenance

To ease maintenance of e-mail templates, create a base e-mail template that includes the most of the tags you need for all of your notification e-mail messages. Use conditional tags in this base template to customize the generated information based on whether the notification relates to primary or auxiliary items, user privileges, and more. Use this base template as much as possible, reserving new e-mail templates for situations that cannot be handled by conditional tags and user settings. For details on e-mail template tags, refer to E-mail Template Tags [page 444].

Frequently Asked Questions About Notifications

- **Do users need special privileges to receive notifications?**

  Users must be able to view items to which notifications are related to receive e-mail notifications. For example, users who only have privileges to view items they submitted will not receive e-mail notifications related to items submitted by other users.

  Most users can manage their subscriptions in their user profile in either Work Center or the SBM User Workspace. The exceptions are users who are not granted privileges to modify their user profile and users with External product access.

- **What if a notification does not get sent as I expected?**

  First, verify the following in SBM Application Administrator:

  - Are other notifications being sent as expected?
  - Is the rule correctly defined? For example, make sure the rule does not contain a condition that excludes the expected recipient from receiving a notification, such as "Not Submitter Is Equal To (Current User)."
  - Is the user subscribed to the notification?
  - Does the user have a valid e-mail address specified in his or her user profile?
  - Does the user have privileges to view the item from which the notification is generated?

  If these steps do not solve the problem, contact an administrator who has access to the SBM Configurator and verify the following:

  - Is the Notification Server running?
  - Are there any errors in the log file, which can be opened from SBM Configurator?

- **How do I include information from items in e-mail notifications?**

  First, include the `$FIELDS()` tag to the e-mail template used by the notification, and then select the fields you want included on the **Fields** page for that notification. For details, refer to E-mail Field Settings [page 297] and Notification Tags [page 445].

- **Can users view notifications outside of their e-mail client?**

  Yes. Work Center offers the **My Notifications** feature, which enables users to see their notifications, mark them as read, and delete them. Search and filtering features

are provided. On-premise customers can use SBM Configurator to specify the number of days notifications are shown before they are purged.

- **How do I control which interface opens when users click an item link in an e-mail notification?**

  You can choose to open the SBM User Workspace or Work CenterSerena Work Center, for example. Select the applicable link type on the General tab for the notification. This option only applies to notifications that send broadcast channels or e-mail messages.

- **How do I send notifications based on time rather than on changes in the system?**

  Use delay parameters to send notifications based on values in a *Date/Time* field. For details, refer to Creating Delayed Notifications [page 278].

- **How do I prevent escalations from generating on holidays and weekends?**

  You can specify a business calendar as part of escalation parameters. Escalation time, such as delay and repeat periods, are calculated based on the calendar. For details, refer to About Calendars [page 390].

- **How do I add attachments to e-mail notifications?**

  Modify the e-mail template used by the notification and add the `$ATTACHMENT()` tag to include files attached to the primary or auxiliary item related to the notification. To include links to these attachments rather than the files themselves, use the `$FILEATTACHMENTLINKS()` tag. For details, refer to Notification Tags [page 445].

- **How do I include historical information about an item in an e-mail notification?**

  Use the `$CHANGEACTION()` template tag to return the action and user that caused the notification to be generated, along with the date and time the action occurred. Use the `$CHANGES()` template tag to return the change history for the item based on the action that caused the notification to be generated. For details, refer to Notification Tags [page 445].

- **How do I know if the Notification Server is configured and running?**

  The Notification Server is managed in the SBM Configurator. If you do not have access to the SBM Configurator, contact your system administrator.

- **Can users subscribe to notifications for individual items?**

  Yes. Item notifications allow users to receive e-mail notifications for individual primary and auxiliary items. For example, a user may be interested in following a particular item as it moves from state to state in the workflow. The user can subscribe to an "item changes state" notification and receive an e-mail message every time the item changes state in the workflow. To enable users to subscribe to individual notifications, make sure they are allowed to subscribe to the notifications, but are not actually subscribed to them. They can then select **Add Item Notification** from the **Actions** list on an item.

- **How do I generate notifications when notes are added to items?**

  Use the Rule object "Any Note" to send notifications when a note is added to or deleted from an item. To send a notification when a note changes, use the rule "Any Note Changes." To include the note in the e-mail notification that is generated, modify the template and include the `$NOTES()` tag. For details, refer to $NOTES() [page 455].

- **If users are in multiple groups that are subscribed to a notification, do they receive multiple messages?**

  No. Users will only receive one e-mail message per notification per cycle.

Chapter 8: Configuring Serena Work Center

This section is intended for administrators who will perform configuration tasks for Work Center.

About Work Center

Work Center is an end-user interface that brings the power of all of your SBM-powered solutions and applications to a single portal.

From a single entry point, users can:

- Use activity, backlog, calendar, and dashboard views to quickly access information pertinent to all applications or specific applications and applications groups.
- Submit new work items into projects assigned to any application, projects in a specific application, or their preferred projects.
- Search for items in all applications or in a specific application.
- Create feeds that populate data in views.
- Browse notifications that reflect changes in the system.

For more information about Work Center, refer to the *Serena Work Center Guide* located on the Documentation Center.

Administrative Tasks for Work Center

Administrative tasks include:

- Creating application groups so users can view easily information specific to the applications in each group. This task is performed in Application Administrator. Refer to Creating Application Groups [page 328].

- Pinning applications or application groups to the Work Center toolbar. This can be done for all new users or for specific groups and users. For details, refer to Pinning Application Groups [page 331].
- Customizing system views. This task is performed in Work Center. For details, refer to Managing System Views [page 333].
- Creating shared dashboards and views and pinning them to the navigation menus for users who share the view. Refer to Adding Views to User Menus [page 332].
- Designating *Single Selection* or *Numeric* fields that calculate estimated and actual time spent on items in Backlog views. Refer to Preparing for Backlogs [page 334].
- Creating resource teams so users can easily share views with different sets of users. For details, refer to About Resources [page 407].
- Changing the link type for e-mail notifications to Serena Work Center so that users are sent to Work Center when they click an item link in an e-mail notification. This task must be completed for each e-mail notification. For details, refer to General Settings [page 288].
- Running **Application Usage** reports. This report enable administrators to view the number of distinct times and application was accessed within a given date range. For details, refer to the *Serena Work Center Guide* located on the Documentation Center.

  Note: To use the **Application Usage** report, on-premise customers must ensure that SBM Logging Services is running in SBM Configurator.

- Adding end-user help text to projects to guide users as they search for projects when they want to submit new items. This task is performed on the **General** tab for each project in Application Administrator.
- Configuring search settings. For details, refer to Configuring the Global Search Feature [page 336].
- Modifying the default purge period (30 days) for the **Notifications** view. This task is performed in the SBM Configurator and is available for on-premise customers only. For details, refer to the *SBM Installation and Configuration Guide*.
- Modifying default branding and labeling. This task is performed in Work Center. Refer to Customizing Work Center Branding [page 335].

Creating Application Groups

An application group is a bundle of applications. A single application can be added to multiple application groups. You can organize the set of applications in each group by role, function, or any business need.

Application groups are pinned to the task bar in Serena Work Center, allowing users to easily access information related to the applications in the group. Users can perform this task themselves; you can also pin applications and application groups for all newly created users in your system or for specific users and groups. For details, refer to Pinning Application Groups [page 331].

Each application group has a set of system views that you can customize for users. For details, refer to Managing System Views [page 333].

There are two types of application groups: those provided for Serena solutions, such as Serena Release Manager and Serena Service Manager, and those that you create for your custom applications. You can hide applications from application groups provided by Serena, but you cannot add applications to them.

Note: Users must have privileges to view items in at least one application in a group before they can pin the group in Work Center.

To create an application group:

1. Launch SBM Application Administrator using this URL:
   `http://serverName/tmtrack/tmtrack.dll?StdPage&Template=newwebadmin/index.html`
2. From the **Administrator portal**, select Work Center, and then select **Application Groups**.
3. From the toolbar, click **Add**.
4. Provide information for the settings on the **General** tab, and then save your changes. For details on these settings, refer to Application Group General Settings [page 330].
5. Select the **Applications** tab, and then select the applications to include in the group. For details on these settings, refer to Application Selection Options [page 331].
6. Save your changes.

Application Group Settings

The following settings apply to application groups.

- Application Group View [page 329]
- Application Group General Settings [page 330]
- Application Selection Options [page 331]

Application Group View

The **Application Groups** view enables you to add, edit, and delete containers for multiple applications. For details about application groups, refer to Creating Application Groups [page 328].

To open the **Application Groups** view, click the **Projects** icon on the **Administrator Portal**, and then click **Application Groups**.

The following information is available for each application group. Click the column headers to sort the list.

- **Name**

  Shows the full name of the application group.

- **Short Name**

  Shows the display name of the application group.

- **Type**
  Shows one of two types:
  - **User**

    Custom application groups created for your installation.
  - **System**

    Application groups created for Serena solutions, such as Serena Release Manager and Serena Service Manager.
- **Status**

  Indicates whether the application group is enabled or disabled.
- **End-user Help Text**

  Shows the help text provided for the application group. Users see this text when they hover over the application group in Work Center.

For details on each of these settings, refer to Application Group General Settings [page 330].

Application Group General Settings

The following general settings are available for application groups:

- **Name**

  Provide a descriptive name for the application group. This name is shown Work Center users when the hover over an application group.
- **Short Name**

  Provide a display name of up to 16 characters that will be shown in Work Center.
- **Image Options**

  Images are shown to Work Center users when they pin application groups. Choose from a set of provided images or select your own image, as follows:
  - **Image URL**

    Indicates the URL for the selected image. To use a custom image, ensure that the image file is stored in a network location accessible to all users, and then paste the image URL in this box. For best results, use a square image no larger than 44x44 px stored as a .png file type.
  - **Select Image**

    Click this button to access a set of provided images, organized by category.
  - **Image Preview**

    Shows the selected image.
- **End-user Help Text**

  Provide guidance text that appears to users when they hover over the application group in Work Center. For example, you may want to list the applications that are included in the group or explain the purpose of the group.

- **Enabled**

  Selected for active application groups. Clear the check box to disable the application group.

For details about application groups, refer to Creating Application Groups [page 328].

Application Selection Options

Use the **Applications** page to select applications for an application group.

The following settings are available:

- **Name**

  Applications are listed by name.

- **Included**

  Available for "user" application groups. Select this check box for each application to include in the group. Clear the check box to remove an application from a group.

- **Hidden**

  Available for "system" application groups. Select this check box for applications you want to hide in the application group. Clear the check box to include the application.

- **Description**

  Shows the end-user help text provided for the application. Hover over the column to see the full text entry.

For details about application groups, refer to Creating Application Groups [page 328].

Pinning Application Groups

You can simplify the user start-up process by pinning applications and application groups to the Work Center toolbar.

You can pin applications at a global level to apply settings to newly created users. You can also choose to apply these default settings for existing users or groups or you can pin a different set of applications for users and groups.

Pinning a Default Set of Applications

To pin a default set of applications:

1. From the **Administrator** portal, select Work Center, and then select **Settings**.
2. Search for or select the applications or application groups you want to pin, then move them to the **Pinned Application Groups** column.
3. Select the **Locked** check box for applications that you do not want users to remove from their toolbar.
4. Clear the **Show Home Icon** if you do not want users to have access to the Home icon, which provides a global context for dashboards and views.
5. Save your changes.

Pinning Applications for Users and Groups

To pin application groups for specific users or groups:

1. From the **Administrator** portal, select the **Users** or **Groups** icon.
2. Select one or more users or groups, and then click **Details**.
3. Select the **User Preferences** tab, and then select Work Center.
4. Select **Get Default Settings** to apply the global set of applications, or select specific applications for the users or groups.
5. Select the **Locked** check box for applications that you do not want users to remove from their toolbar.
6. Clear the **Show Home Icon** if you do not want users to have access to the Home icon, which provides a global context for dashboards and views.
7. Save your changes.

Adding Views to User Menus

Administrators can create views, share them with users, and automatically add shared views to the navigation menu of users you share the view with.

Consider the following information when sharing and pinning views:

- You must have the Remote Administration privilege to automatically add shared views to users' navigation menus. Other administrators who co-own shared views can also perform this task.
- Users cannot remove menu items that are automatically added for them. To remove a menu item for a user, you must remove them from the view sharing list.
- Shared views are added to the menu for the application context where the view was created. If the view was created in the Home context, the view is added to the Home navigation menu. If the view was created for a specific application or application group, the view is pinned for that context. Users must pin the application or application group to their Work Center toolbar to see the view.

To automatically add shared views to menus:

1. In Work Center, create a dashboard or activity, backlog, or calendar view.
2. Select the **Sharing** tab.
3. Add users, groups, or resource teams to the **Selected** list.

   Tip: For best results, select groups or resource teams when you share views. This ensures that menu changes apply to users as you add or remove them from groups and teams.
4. Select the **Automatically pin view to menu** check box.
5. Save your changes.

Managing System Views

Work Center provides three system views for Home and for each application and application group. Users with the Remote Administration privilege can modify these system views.

Changes made to the system views impact all users. Users cannot remove widgets and feeds added to these system views, but they can add their own feeds and add and reorganize their own dashboard widgets.

The system views have the following default behavior:

- **My Dashboard**

  Shows tips for using the dashboard. You can replace these tips with widgets that contain reports, condensed activity views, or external Web pages.

  Tip: All users in your system will see the same content for Home, so choose content that applies to a broad set of user privileges.

- **My Activity**

  Shows the "All Items I Own (Primary)" system feed.

- **My Calendar**

  Has no default feeds. You can add public calendar feeds or leave this task to users, who can create and add their own calendar feeds.

Note: System views for Serena-provided solutions, such as Release Manager and Service Manager, may differ from that of system views for custom applications and application groups.

To modify a system view:

1. Select one of these:
   - To change a Home page view, click the Home icon.

   - To change an application view, click a pinned application icon on the toolbar.
2. Click the **Manage Views** ( ) icon in the navigation pane.
3. Select the view category (Dashboards, Activities, or Calendars), and then search for or navigate to the view you want to change.
4. Hover over the view, and then select the **Edit** icon.
5. Select the **System View** button.

   Note: You will only see this button if you have the Remote Administration privilege.

6. Modify the view as follows:

- For dashboards, change the name and description. Save your changes, then run the view to add widgets to the system view.
- For activity and calendar views, modify any setting.

7. Save your changes.

Preparing for Backlogs

Backlog views enable users to organize and prioritize work items based on backlog feed content. Backlog views and feeds are only available in Serena Work Center.

Backlogs are available to user without additional setup, but the following sections provide guidance on administrative changes that will enhance users' experience with backlog views and feeds.

Add Fields for Tracking Estimates and Actuals

To help users capture planning estimates and actual effort spent on each work item, add *Single Selection* fields with weights or *Numeric* fields to your workflow. Information from these fields is shown on the backlog list. "Estimates" are also used on progress reports and to calculate burn up and burn down charts.

Users can select these fields when they create feeds for backlog views. Since all *Single Selection* and *Numeric fields* are available when users create backlog feeds, use the field display name setting in SBM Composer to guide users on which fields provide the most benefit for backlog feeds.

For example, you can create two *Single Selection* fields:

Field Name	Value	Weights
Estimates	Small	50
	Medium	75
	Large	100
Actuals	Small	50
	Medium	75
	Large	100

Be aware that by default, "none" values are treated as 100. If you want "none" values to be treated as 0, change the value in the **Default weight for new values** setting to 0. This ensures that calculations are accurate for backlog items that have not been estimated or give "actuals" values.

Fields changes to support backlogs are made in SBM Composer.

Add Resource Teams for Easy Backlog Sharing

Resource teams enhance backlog use by enabling users to:

- Share backlog views with members of specific teams.
- Include resource teams in backlog feed criteria to limit the work items returned by the feed by specific teams.
- Used to show team statistics on progress reports.

For guidance on creating resource teams, refer to About Resources [page 407].

Create Notifications for Backlog Changes

To notify users of changes to items in backlogs, create notifications that fire when:

- Items are added to backlogs
- Items are removed from backlogs
- The priority changes for an item in a backlog

Use the "Any item" object to create rules pertaining to backlogs.

You can use a single rule for multiple notifications in a workflow, but you must create a separate condition statement for each backlog.

For details, refer to Creating Rules [page 277].

Viewing Logging Information

Log information about backlogs views and feeds can be found in the agile.txt file in this location on the Common Services server:

installationDirectory\Serena\SBM\Common\jboss405\server\default\log

Customizing Work Center Branding

You can change the logo, page title, and footer text for Work Center. You can also modify the Web page that opens when users click your logo. These changes can be made by any user with administrative access and are seen by all Work Center users.

The following settings are available on the **Branding Configuration** tab of the **Settings** page in Work Center. To open the **Settings** page, click the user icon in the upper right corner.

- **Header Title**

  Change the text that appears to the right of the logo and in the Web browser title bar. Use the toolbar to apply formatting.

  Note: The item ID and title are shown on the browser title bar when users open work items from reports, activity views, backlog views, and search results in a new tab. When users open reports in a new tab, the report title is shown as the browser title bar.

- **Image (URL)**

  Enter a URL to a logo file or image that is accessible to Work Center users. For example, do not enter an URL for a logo that is located in a restricted domain that is not accessible by all users.

- **Image Link**

  Enter the URL for a Web page that opens when users click the logo.

- **Footer Text**

  Add text that appears at the bottom of the interface. Use the toolbar to apply formatting.

Configuring the Global Search Feature

The powerful search feature in Work Center enables users to search for work items across all applications from a single place. Users can search for work items in all projects or filter the search to items in their preferred projects.

Search criteria is applied to most fields users have access to, with a few exceptions:

- For *Text* fields, the **Include field in Keyword searches** check box must be selected for the field in SBM Composer. This option is located on the field's **Options** tab.
- Data in *Date/Time*, *Numeric*, and *Summation* fields are not evaluated in search queries.

Privileges control the items returned by user searches and the information users see in each item.

On-premise customers can control certain system aspects of the Work Center global search feature, such as configuring polling interval that determines how often to poll the database to learn about new search strings and new related articles. The default is 3 minutes. These settings are modified in SBM Configurator. For details on system search settings, refer to the *SBM Installation and Configuration Guide*.

Chapter 9: Configuring Advanced Features

This section provides guidance on configuring features that require multiple steps in different interfaces. For example, to begin using the e-mail submission feature, you must configure mail client settings in SBM Configurator and prepare your workflow in SBM Composer in addition to the steps that you perform in Application Administrator.

Rich Text Editing

Users can apply basic formatting to text on many forms if Rich Text editing is enabled.

The Rich Text Editor is available to users for the following features:

- Text fields (Memo and Journal types)
- Notes
- E-mail messages sent from primary and auxiliary items

Along with standard formatting (bold, italics, bulleted lists, text color, and more), users can:

- Add attachments, images, and hyperlinks.
- Paste formatted text from Rich Text- or HTML-formatted documents.
- Edit the source for the text and directly add or modify HTML tags. If you choose to manually enter HTML, be aware that obviously "suspicious" ("dangerous") HTML is not rendered at runtime.

Administrators can also use the Rich Text Editor to format:

- Default values for *Text* fields
- Notification and e-mail submission templates
- End-user help text for application elements in SBM Composer and for projects in Application Administrator

Configuring Rich Text Capabilities

Rich Text features are controlled at a system level with the **Enable HTML5 Features** check box located on the **General** tab of the Base Project. This check box is enabled by default.

You can control users' ability to use the Rich Text Editor and the rendering of formatted text in individual elements as described in the following table:

Element	Control Setting	Default Behavior
Text fields (Memo and Journal only)	**Enable Rich Text** setting for each field. Set in SBM Composer.	Enabled for newly added fields.
Notes	**Render HTML in Notes** option. Set in SBM System Administrator.	Enabled for all notes. On-premise customers can disable this setting for their entire system.
E-mail messages	Always enabled. Use HTML templates to ensure content is rendered correctly.	See Selecting E-mail and Notification Templates [page 339].

The following sections provide guidance on enabling or disabling the Rich Text Editor and HTML rendering of text.

CAUTION:

If you disable Rich Text capabilities after formatted data has been added to fields, notes, and e-mail messages, the data may be garbled or unreadable. In this case, you must manually modify data to remove formatting tags.

Enabling the Rich Text Editor for Text Fields

The Rich Text Editor allows users to apply basic formatting to *Text* fields (Memo and Journal). This setting can only be applied in SBM Composer.

To enable the Rich Text Editor for individual fields:

1. In SBM Composer, open the process app that contains the fields for which you want to enable Rich Text editing.
2. In the App Explorer, select the **Data Design** filter, and then select the table that contains the fields.
3. Select a *Text* field, and then select the **Enable Rich Text** check box located on the **Options** tab.
4. Repeat step 3 for each *Text* field as needed.
5. Deploy the process app.

Note: If you enable Rich Text for a field, but HTML5 features are disabled for your system, users can manually type HTML tags into the field, and they will be rendered on State form.

Formatting Default Values for Text Fields

You can use the Rich Text Editor to apply formatting to default values for *Text* fields (Memo and Journal).

Default values can contain hyperlinks and links to images, but cannot contain images or file attachments.

To use the Rich Text Editor to format default values in SBM Composer, first select the **Enable HTML5 Features** check box located on the **Forms** page of the **Application** tab. The editor will be available for *Text* fields for which the **Enable Rich Text** check box is selected.

In SBM Application Administrator, you can apply formatting when you override default values for *Text* fields for projects and transitions if the **Enable Rich Text**check box is selected for the field.

Selecting E-mail and Notification Templates

To ensure that Rich Text formatting is correctly rendered in e-mail messages generated by the Notification Server, you must select HTML templates for notifications and for e-mails sent from items.

For notifications, e-mail templates are selected on the **General** page for each notification.

For e-mail messages sent by users as they work with items, templates are selected on the **Notification Server** tab of the **Mail Services** page in SBM Configurator. (An HTML template is selected for on-demand customers.)

Disabling Rich Text Capabilities for Your System

SBM's Rich Text capabilities require that users access the system with browsers that support HTML5. If users must access the system with an older browser, such as Internet Explorer 8 (IE8), you can disable Rich Text and other advanced HTML capabilities for your entire system.

For details, refer to Enabling System Settings From the Base Project [page 37].

Disabling Rich Text Capabilities for Notes

On-premise customers can disable the Rich Text Editor and HTML rendering of information in notes added to items.

To disable Rich Text and HTML capabilities for notes:

1. Open SBM System Administrator.
2. Select the **Settings** from the **Options** menu.
3. Select the **HTML** tab.
4. Clear the **Render HTML in Notes** check box.
5. Restart IIS.

The Social View

The **Social** view is an alternative view of primary items that enables users to collaborate more easily. For example, an item feed enables users to quickly and easily see who has contributed information to an item. Users can also easily post status entries, notes, and attachments.

You can also configure the **Social** view to:

- Enable users to see and contact "experts" who have worked on a item. For details, refer to Enabling the Experts Feature [page 341].
- Enable users to follow an item and be notified about changes to the item based on notifications you create and select for this feature. For details, refer to Enabling the "Follow" Feature [page 342].
- Disable the **Social** view. For details, refer to Disabling the Social View [page 342].

The **Social** view is enabled by default and can be opened by clicking the clicking the **Social** button on any primary item.

Note: The **Social** view is not available for users with Occasional User or External User product access.

Social View Application Dependencies

In general, the **Social** view provides an alternate view of the traditional **Details** view of a primary item. This section describes the relationships between application elements and the **Social** view.

- **Social View Updates**

  All data added to an item is available in the appropriate areas of the **Social** and **Item Details** views. For example, if a note is added to the **Social** view, users with appropriate privileges can see the note in the **Item Details** view.

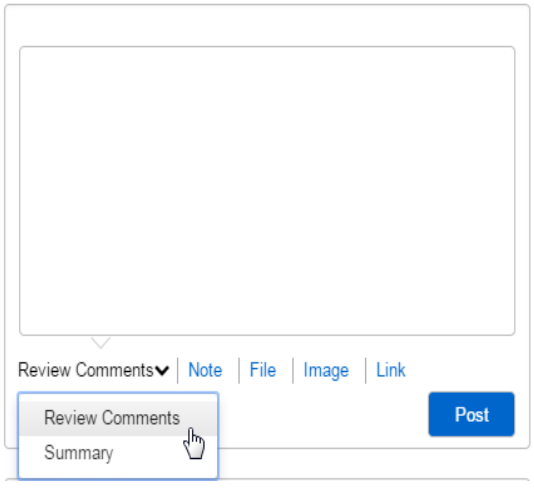
- **Privileges**

Privileges govern a user's ability to see items in the **Social** view. For example, users who do not have privileges to see change history for an item will not see change history entries in the Item Log.

- **Journal Log**

  The Journal Log is based on *Text* fields set as Journal fields and an Update transition. The first enabled update transition named "Update" is used to add entries. If such a transition does not exist, the Journal Log uses the first transition of the type "update." If the transition requires any input from users, such as required fields or notes, the Journal log is not available.

  By default, the first Journal field found is used in the log, but users can select other Journal fields from the drop-down list.



  Users cannot delete Journal Log entries for Journal fields set as "append only."

  Note: If there are no Journal fields in your application, the Journal Log contains only the note, file, image, and link options.

Enabling the Experts Feature

The Experts feature enables users to see a list of experts based on the number and kind of similar items they worked on.

The experts are found and ranked based on the following criteria:

- The title words in the item are used to search for similar items within the same project and subprojects. Similar items are found and ranked based on a weighted keyword search of the title and description within the items.
- Only items that have been in the same state in the past six months are evaluated.
- Deleted users are not included in the suggested expert list.
- The current user is not included in the suggested expert list.

To enable the Experts feature, you must first:

1. Configure your database management system for full-text indexes, using the information in S138517 in the Knowledgebase at serena.com.

2. In SBM Composer, select the **Enable Searching for Social Widget** check box on the **Options** tab of the Table Property Editor for the application primary table, and then deploy your changes. This step must be completed for each application that will use the Experts feature.

Enabling the "Follow" Feature

Users who choose to follow an item are sent e-mail notifications based on changes to the item. You can define what it means to follow an item by creating notifications for each workflow in the system.

For example, you may want to send users an e-mail when any changes are made to an item they are following. In this case, you can create a notification with a rule like this:

"Any Item Changes"

Assign the rule to a notification so that e-mails are generated when any item changes. Once you select this notification for a workflow's **Social** view, users will receive an e-mail any time a change is made to the item they are following.

To enable the "follow" feature:

Note: Users are not able to follow items in a project until you have followed these steps for the workflow assigned to the project.

1. Create notifications related to features on the **Social** view.
2. Edit a workflow used for the notifications you created.
3. Select the **Social View** tab.
4. From the list, select the notifications that will be sent to followers of an item once the notification rule becomes true.
5. Save your changes.

Disabling the Social View

By default, the **Social** view is enabled for all primary items in all projects.

To disable the Social view:

1. From the **Administrator Portal**, select the **Projects** icon.
2. Select **All Projects** in the **Process Apps/Applications** pane.
3. In the content pane, select Base Project, and then click **Details**.
4. In the Social View section, clear the **Use Social View** check box.
5. Save your changes.

Time Capture

Overview

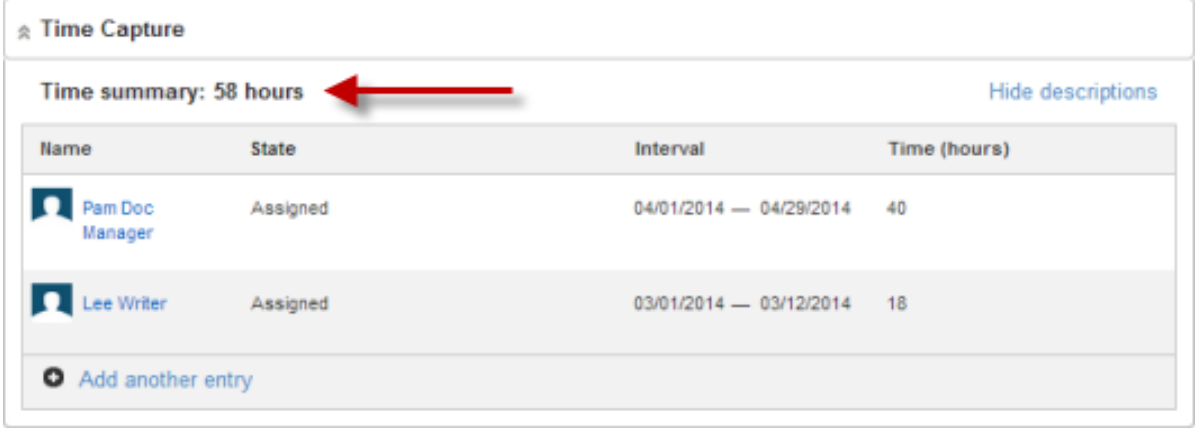
The Time Capture feature enables users to record the amount of time they spend working on primary items. Time can be captured on state and transition forms. The Time Capture feature can be enabled or disabled at various levels (system, workflow, project, or for specific states and transitions).

For transition forms, time entries always apply to the current state of an item. For example, if an item is in an "Assigned" state, all time entries applied during a transition out of the state or during an update are attributed to the "Assigned" state. In other words, work is considered to have occurred while the item was assigned. You can also require users to record time spent for all transitions or for specific transitions.

For state forms, all states an item has resided in are available for users to capture time. This is so users can capture time for work they completed while the item resided in a particular state.

Entries can be in quarter-hour increments in digit format (4.25 or 4,25, for example, to represent 4 hours and 15 minutes), cannot exceed 30 days, and cannot be in the future. Dates are shown in the date/time format selected in each user's profile.

When users are viewing a state form, a time summary shows the total time captured for a particular item for all users. When users are working with a transition form, the summary shows entries for the item's current state.



Summary reports can be used to sum time capture entries for particular projects based on specific report criteria.

Time Capture changes are noted in the Change History section.

Changed Value	Prior Value	New Value
Entry State		Assigned
User		Pam Doc Manager
Time Spent		40
Interval Start		04/01/2014
Interval End		04/29/2014

Enabling Time Capture Options

By default, Time Capture options are disabled, but they can be enabled for your entire system or at various levels. You can override the settings at each of these levels. This allows users to record time spent on items only when the information is required or is meaningful for your process.

Time Capture options can be enabled or disabled at these levels:

- **System**

  In SBM Application Administrator, use Time Capture options in the Base Workflow to enable or disable this feature for transitions and states in all workflows and projects.

- **Application Workflows**

  In SBM Composer, enable or disable Time Capture options for all states and transitions in specific workflows.

- **Projects**

  In SBM Application Administrator, set or override Time Caption options for all states and transitions in some projects assigned to a workflow, but not others.

- **States and Transitions**

  Explicitly show or hide Time Capture options for individual states and transitions in workflows (SBM Composer) or projects (SBM Application Administrator).

You can also require users to enter the amount of time spent on an item for all transitions in your system, in specific application workflows, for all transitions in a project, or for individual transitions.

Time Capture Form Placement

If enabled for a workflow or project, Time Capture options are available on forms as follows:

- **Quick Forms**
  - For states, options appear after the Change History section.
  - For transitions, options appear at the top of the form.
- **Custom Forms Without the Time Capture Widget**

  If you do not place the Time Capture widget on custom forms in SBM Composer, Time Capture options are placed in the same locations as they are placed for quick forms.

- **Custom Forms With the Time Capture Widget**

  Use the Time Capture widget in SBM Composer to determine placement of Time Capture options on state and transition forms.

Privileges and Time Capture

In general, Item privileges control users' ability to use the Time Capture options.

For example, users who can only view items can see entries, but not add, edit, or delete them.

Users who can update or transition items can add, edit, and delete their own entries, but cannot do so on behalf of other users. These users can also view entries made by other users.

The "View Change History" privilege is also required for users to view, edit, and delete Time Capture entries on state forms.

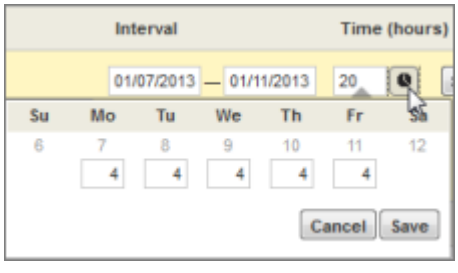
Managed administrators who have privileges to edit a project can edit and delete time capture entries on behalf of other users.

"Super" administrators can edit and delete time capture entries on behalf of other users.

For details on user privileges, refer to About Privileges [page 180]. For details on administrative privileges, refer to Administrative Privileges [page 259].

Calendars and Time Capture

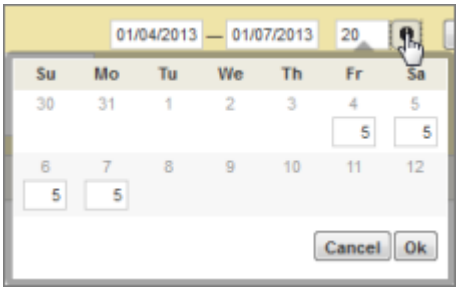
The system will automatically distribute time entries over several days. For example, if a user enters 20 hours for an item for a five-day duration, the system automatically distributes four hours to each day.



Users can change the distribution of hours as needed.

SBM calendar assignments are used to calculate this distribution. The first calendar meeting one of the following criteria is used for this distribution:

1. Calendars assigned to a user's resource record. For details, refer to About Resources [page 407].
2. Calendars assigned to a user's profile. For details, refer to Date/Time and Locale Preferences [page 248].
3. If no calendar is assigned to a user or that user's resource record, time is distributed evenly over the selected days, including weekends.



Working with Contacts (On-Demand)

The on-demand Global Process App contains the *Contacts* system auxiliary table, which stores contact records for users. A contact record enables you to define custom user attributes in addition to what is available on the user or resource record. A single contact record is associated with a single user record in the system.

Common use cases involving *Contacts* include:

- Defining contact attributes and displaying them on the **User Profile Card**. For example, you can add a fixed-length text field to store the address for a contact, and then display that address in the **Contact** section in the **User Profile Card**. For details, refer to Adding Contact Attributes to the User Profile Card [page 347].
- Adding the system *Contacts* field to primary tables, which enables users to associate a *Contact* with a primary item. The *Contacts* field is a system field, which means you can use the View if Contact privilege to limit who can view a particular item. For details, refer to Associating Contacts with Primary Items [page 347].

You can add additional fields to the *Contacts* table and add custom auxiliary tables to the Global Process App using SBM Composer after you "Get" the process app in SBM Application Repository.

Tip: To populate *User* and *Multi-User* fields that you add to auxiliary tables in the Global Process App, edit the user field in SBM Composer, associate one or more roles, deploy the process app, and then assign users and groups to those roles in Application Administrator using the following steps:

1. In Application Administrator, select **Projects**.
2. In the **Projects** tree, select **All Projects**.
3. Select the base project, and then click **Details**.
4. Open the **Roles** view, select a role, and then click **User Assignment** or **Group Assignment** to assign users.

The assigned users will now appear as selections in the user fields that you added to the auxiliary table.

Getting Started with Contacts

Before you begin working with contacts, ensure that you have granted the proper privileges:

- Grant Administration privilege to the *Contacts* table if it is not granted already. (Users in the Administrators group should have Admin privilege to the *Contacts* table automatically.) For details, refer to Table Administration Privileges [page 265].
- Grant users Table privileges to work with the *Contacts* table. For details, refer to Table Privileges [page 224].
- Grant View Your Contact Information and Edit Your Contact Information system privileges to users as appropriate. For details, refer to System Privileges [page 181].

You can create contact records for yourself and your users using either of the following options:

- Use the **Import users from spreadsheet** option in Application Administrator and select the **Create Associated Contacts** option. This creates a contact record for each user in the spreadsheet, and populates mapped contact attributes as well. For details, refer to Importing Users From a Spreadsheet [page 351].
- Use the **Import users from LDAP** option in Application Administrator and select the **Create Associated Contacts** option. This creates a contact record for each imported user, and populates mapped contact attributes as well. For details, refer to Importing Users and Contacts From LDAP [page 359].
- Edit individual users in Application Administrator, select the **Create/Update Record from User** option, and then click **Save**. For details, refer to General User Settings [page 158].

Adding Contact Attributes to the User Profile Card

You can add customized contact record attributes to the **User Profile Card** that is displayed in the end user interfaces. To add new contact record attributes to the **User Profile Card**:

1. Log in to Application Repository and "Get" the Global Process App from the repository.
2. Open the Global Process App in SBM Composer and add new fields (attributes) as desired.

   Tip: When you add field to the Contacts table, note that View privileges apply to the privilege section that you specify on the field. For example, if you add a field and specify the Manager privilege section, only users who can view fields in the Manager section will be able to see the field on the User Profile Card.
3. Deploy the Global Process App.
4. Update contact records individually using the **Auxiliary Data** page in Application Administrator or use the **Import users from spreadsheet** option to update the new attributes for your contact records.
5. Edit the **User Profile Card** page in Application Administrator and select which new contact attributes should appear in each section of the card.

Associating Contacts with Primary Items

To allow users to associate contacts with primary items:

1. Open a process app in SBM Composer, and add the *Contact* system field to the primary table.
2. Deploy the process app.
3. Open the Global Process App in SBM Composer, and then select the View if Contact Item privilege on applicable roles (for any roles that do not have View All Items selected already) in the Global Process App. This enables users to view items for which they are the contact.

For example, if you want to limit what Occasional Users can view, remove all View privileges except for View if Contact. This ensures that Occasional Users can only view items for which they are the contact.

4. Deploy the Global Process App.

Users should now be able to update or transition an item and select an associated contact, and the contact should be able to view the item.

Chapter 10: Administrative Utilities

The following topics describe how to use administrative utilities.

About Record Locks

A record is locked when a user opens an item for updating or transitioning or begins editing a row in the Rich Editable Grid. Other users who attempt to access a locked record receive a message that the record is currently locked. A user who attempts to open a single item in multiple browser windows also receives a record-lock message. In this case, users can break their own locks, but they cannot break the locks of other users.

Record locking with a 30-minute time-out setting is enabled by default for all primary and auxiliary tables. You can modify these default settings on the **Advanced** tab when you edit a primary or auxiliary table in SBM System Administrator.

The following information applies to record locks:

- Users can view locked items and add notes and attachments to them, but they cannot edit items that are locked by another user.
- When record locks are broken, users receive an error message stating that the lock on the item was broken by either a time out or a process with a higher priority.
- Record locks are automatically released when an update or transition is completed, when the user cancels the transition or update, or when the specified time-out period expires. Locks are also released when users save or discard modified rows in the Rich Editable Grid.

  Note: If users modify items in the Editable Grid and then navigate away from it without saving or discarding their changes, the modified items remain locked until the time-out period expires or the locks are manually removed.
- The following processes have priority over record locks and will break them: database imports; and transition actions such as triggers, sub-tasks, and scripts.

Orchestrations, SBM Web Services API (if breakLock is `true` in the TransitionItems call), and SBM API functions will also break record locks, except for the TSPrimaryItem::StartTransition and TSAuxiliaryItem::StartUpdate API methods.

- You can manually remove record locks on individual items from SBM Application Administrator. To prevent data loss, do this only when users cannot access items in the table for unexpected reasons, such as one user leaving a form open for an extended period. For details, refer to Removing Record Locks [page 350].
- Users who have privileges to view System reports can run the **Item Lock** report, which provides a list of items that are locked by users for tables selected when running the report. The report displays the title of the locked item, the user holding the lock, and the amount of time remaining on the lock.

Removing Record Locks

Record locks prevent multiple users from updating a primary or auxiliary item at the same time. You can remove record locks on individual items as needed. Typically, record locks only need to be removed when a user does not exit the form properly. For details on record locks, refer to About Record Locks [page 349].

Select the **Display locking user name to requesting user** check box to display the user name of the user who established the record lock to users who attempt to update or transition the locked item.

Managed administrators can remove record locks for items in tables they can administer if locks were established by users the administrator has privileges to manage.

To remove record locks:

1. From the **Administrator Portal**, click the **Record Locks** icon. Established record locks are listed, including the login ID and user name of the user who established the lock and the type of item that is locked. Use the **Items Per Page** setting to control the number of items that appear per page.
2. Select an established lock in the list.
3. Click **Delete**.

About User Import

SBM Application Administrator offers several mechanisms for importing users into your system. Each of these options is available on the **Import Users** page, which you can open by clicking the **Import Users** icon on the **Administrator Portal**.

The following options are available:

- **Import users from spreadsheet**

  Provides a quick way for administrators how may not have access to your LDAP store to add users to your system. For details, refer to Importing Users From a Spreadsheet [page 351].

- **Import and update users and contacts from LDAP**

Enables global administrators a way to import and update users and contacts directly from LDAP. For details, refer to Importing Users and Contacts From LDAP [page 359].

Importing Users From a Spreadsheet

Use the Import Users feature to import new users and update existing user accounts from a spreadsheet. Spreadsheets should contain basic information for each user, such as login ID, name, and e-mail address. You then specify a template user that provides role assignments, group membership, privileges, preferences, and more for imported users.

Spreadsheets can come from external tools, such as an Active Directory store or other Lightweight Directory Access Protocol (LDAP) providers, or you can manually create a spreadsheet. For details, refer to Preparing a Spreadsheet for Importing Users [page 352].

Key Benefits

- Quickly add new users to your system.
- Update basic information for existing users. For example, you can quickly update new phone numbers or e-mail addresses for a large set of users.
- Change the privilege sets, role assignments, user preferences, and more for a set of users, based on a template user.
- Change the product-access level for a set of users (based on license availability).
- Add or update resource records for a set of users.
- Add or update *Contacts* table records for a set of users.

User Import Considerations

Consider the following before you import users:

- When you specify a template user, consider using an account that derives privileges from a group or role (as opposed to an account for which privileges are granted directly to the individual user). Using a template account that inherits privileges from groups or roles improves the performance of the import operation.
- Login IDs are used to verify uniqueness of imported users. Take care to ensure login IDs are unique in your spreadsheet and in SBM.
- The Import Wizard stops if the spreadsheet contains more users than the number of allowed licenses.
- You can only import one spreadsheet at a time.
- You can choose to send newly imported users an e-mail message that contains their login information, including an initial password. If you choose not to send this e-mail message, you must manually change passwords and provide them to users before they can log in.
- If you have access to your organization's LDAP system, consider importing and updating users from the LDAP store. This feature is available in SBM Application Administrator and SBM System Administrator.

Import Privileges

Managed administrators must be granted the privileges in the following table before they can import or update user accounts. In addition, administrators can never update their own user records through the import process.

Privilege	Location	Description
Add Users	Administration - System page	Grant to enable the Import Users feature.
Edit Users	Administration - System page	Grant to enable administrators to update user accounts. These users must be members of groups that the administrator has privileges to manage. In addition, template users must be members of a group a managed administrator can manage.
Submit	Users - Table page	Grant this privilege for the *Contacts* table to enable administrators to add new *Contacts* records when they import user records.
Update	Users - Table page	Grant this privilege for the *Contacts* table to enable administrators to add new *Contacts* records when they import user records.

Preparing a Spreadsheet for Importing Users

Spreadsheets used to import users must adhere to the following requirements:

- Only files of type .xls can be imported. If you have an .xlsx file or any other type of spreadsheet file, you must convert it to .xls.
- Only data from the first worksheet in a file is imported.
- Columns represent user, resource, and *Contacts* record attributes, such as login ID or e-mail address. There is no limit to the number of columns you can have in the spreadsheet, but only certain SBM user, resource, or *Contacts* data can be mapped to these columns. For details, refer to the following section.
- The spreadsheet must contain columns with Login ID and e-mail address information. These columns must be mapped before you can import the spreadsheet. Rows that do not contain data for these attributes are skipped. In addition, only one e-mail address is allowed for each row.
- Each row represents a single user, except the first row, which is used to define columns available for mapping. Data from this row is not imported as a user or *Contacts* record.
- Each spreadsheet is limited to 10,000 rows. To import more than 10,000 users, create multiple spreadsheets and import them separately.

Here is an example of a simple spreadsheet used to import users:

	A	B	C	D
1	LOGIN	NAME	EMAIL	ADDRESS
2	jjones	Jenny Jones	jjones@mycompany.com	1235 Happy Lane
3	bknight	Bobby Knight	bknight@mycompany.com	567 Basketball Dr.

In this example, row 1 defines the columns to be mapped. This information is not imported. Row 2 is used as sample data, but the user is imported.

Mapping Attributes to SBM Fields

The following table explains how data in the User Attributes columns is mapped to SBM user, resource, and *Contacts* records.

Note: The *Contacts* table contains the following required system fields: *First Name*, *Middle Name*, *User Name*, *E-mail*, and *Company* (on-premise only, based on the system *Companies* table). Other fields, such as *Phone Number*, are optional and may not be available in the *Contacts* table. You can add these as needed in SBM Composer.

User Attribute	User Mapping	Contact Mapping
Login ID	Required. For on-demand customers, the login ID must be an e-mail address.	N/A
Name	Added to the Name field for the user record.	Added to the *User Name* field. Also parsed to *First Name*, *Middle Name*, and *Last Name* fields. For example, if the Name row in the spreadsheet is John Q. Smith, the name is parsed across the three fields in the *Contacts* record.
E-mail	Required. Added to the E-mail field.	Added to the *E-mail Address* field, if available.
Telephone	Added to the Telephone field.	Added to the *Phone Number* field, if available.
Mobile Number	Added to the Mobile Phone field.	Added to the *Mobile Number* field, if available.
Title	Added to the Title field.	N/A

Resource Attribute	User Mapping	Resource Mapping
Business Unit	N/A	Added to the *Business Unit* field.
Department	N/A	Added to the *Department* field.
Description	N/A	Added to the *Description* field.
Employee ID	N/A	Added to the *Employee ID* field.
End Date	N/A	Added to the *End Date* field.
Job Function	N/A	Added to the *Job Function* field.
Location	N/A	Added to the *Location* field.
Manager	N/A	Added to the *Manager* field.
Skills	N/A	Multiple columns with the same name can be mapped to the **Resource: Skills** attribute.
Start Date	N/A	Added to the *Start Date* field.
Teams	N/A	Multiple columns with the same name can be mapped to the **Resource: Teams** attribute.
Title Group	N/A	Added to the *Title Group* field.
Type	N/A	Added to the *Type* field.

Contact Attribute	User Mapping	Contact Mapping
Company	N/A	Added to the *Company* if the value in the spreadsheet is an active value in the *Companies* table (on-premise only).
Address 1	N/A	Added to the *Address 1* field, if available.
Address 2	N/A	Added to the *Address 2* field, if available.
City	N/A	Added to the *City* field, if available.
State	N/A	Added to the *State* field, if available.
Country	N/A	Added to the *Country* field, if available.

Contact Attribute	User Mapping	Contact Mapping
Zip Code	N/A	Added to the *Zip Code* field, if available.
Fax Number	N/A	Added to the *Fax Number* field, if available.

Note: These contact attributes do not exist by default on the *Contacts* table for on-demand customers; however, you can add these fields to the on-demand *Contacts* table using SBM Composer.

Importing New Users from a Spreadsheet

Use the following steps to add new user accounts without updating existing user accounts.

To import new user accounts and *Contacts* records:

1. Prepare a spreadsheet by exporting it from an external user store or creating it manually. For guidelines, refer to Preparing a Spreadsheet for Importing Users [page 352].
2. From the **Administrator Portal**, click **Import Users**.
3. Verify that the **Do Not Modify** option is selected. This prevents existing user accounts from being updated if they exist in the spreadsheet.
4. In the **Import user spreadsheet** area, click **Browse** and navigate to the spreadsheet that contains users you want to import.
5. Click **Find** to search for a user that will serve as a template for the imported users. Imported accounts receive the template user's product-access type, role assignments, group membership, privileges, preferences, notification subscriptions, and password settings.
6. To create *Contacts* records for the imported users, select the **Create Associated Contacts** check box.
7. Map spreadsheet data to SBM user and *Contacts* record fields. For guidance, refer to Mapping Attributes to SBM Fields [page 353].
8. Click **Import**.
9. Select the **Import Log** tag to monitor the progress of your import.

Updating Users From a Spreadsheet

Use the following steps to update existing user accounts, resources, and *Contacts* records.

Note: Users included in your spreadsheet but who do not already exist in SBM are added when you follow the steps below. To update existing accounts only, remove new users from the spreadsheet.

To update existing user accounts, resource, and *Contacts* records:

1. Prepare a spreadsheet by exporting it from an external user store or creating it manually. For guidelines, refer to Preparing a Spreadsheet for Importing Users [page 352].
2. From the **Administrator Portal**, click **Import Users**.
3. Select one of the following options:
   - **Replace mapped attributes**

     Replaces mapped attributes with data in the spreadsheet. For example, you can update phone numbers for users quickly with this option.
   - **Replace user**
     Replaces mapped attributes and all user properties, except the user's unique database ID, for existing users. All account attributes, such as product-access type, privileges, and preferences, are replaced.

     CAUTION:

     The **Replace user** option completely overwrites existing user accounts. Use this feature cautiously.
4. In the **Import user spreadsheet** area, click **Browse** and navigate to the spreadsheet that contains users you want to import.
5. Click **Find** to search for a user that will serve as a template for the imported users. If you selected the **Replace User** option, imported accounts receive the template user's product-access type, role assignments, group membership, privileges, preferences, notification subscriptions, and password settings.
6. To update *Contacts* records for the imported users, select the **Create Associated Contacts** check box.
7. Map spreadsheet data to SBM user and *Contacts* record fields. For guidance, refer to Mapping Attributes to SBM Fields [page 353].
8. Click **Import**.
9. Select the **Import Log** tag to monitor the progress of your import.

Spreadsheet Import Options

Use the **Import Options** page to set options for handling existing users, sending e-mails about the import, and importing a spreadsheet.

The options described in this section are available when the **Import users from spreadsheet** option is selected in the **What do you want to do?** section.

Refer to the following sections for details about importing users from a spreadsheet:

- Importing New Users from a Spreadsheet [page 355]
- Updating Users From a Spreadsheet [page 356]
- Import Log [page 377]

Logging And E-mail Options

Use these options to send a copy of the import log file by e-mail when the import process completes and to send e-mail messages to newly imported users.

The Notification Server must be configured and running to send import logs and new user confirmations. On-premise customers use SBM Configurator to manage the Notification Server. The Notification Server is enabled in on-demand systems.

Change these options as needed:

- **Send the log by e-mail when import completes**

  This check box is selected by default. Clear it to stop the import log from being sent by e-mail.

- **E-mail**

  By default, the user logged into SBM Application Administrator when the import process is started is sent the log message. Change the e-mail address as needed. To send the log to multiple addresses, separate each address with a comma.

- **Send notification e-mails to created users**
  Select this check box to send e-mail messages to newly imported users. The message is sent to the address that is added during the import process and includes login information. Users must change their password on their first login attempt.

  Note: On-premise customers can use SBM System Administrator to modify the template for e-mails sent to newly imported users. This template is located on the **External Users** tab of the **Settings** dialog box.

Existing User Options

When you import users, login IDs are used to guarantee uniqueness. Use the following options to determine how the import process handles login IDs that match in the spreadsheet and in SBM.

- **Do not modify**

  Select to ignore spreadsheet rows where the login ID matches that of an existing SBM user.

  Tip: If the user already exists, but does not have an associated resource record, a new resource record is created for that user if you map any resource attributes.

- **Replace mapped attributes**

Select to replace mapped attributes with data in the spreadsheet. This is useful for updating information, such as e-mail address and phone number, in existing SBM user accounts.

- **Replace user**

  Select to replace mapped attributes and template attributes for existing users. This enables you to quickly change all user properties for existing users. For example, if a set of users is moved to a new department and needs a different privilege set, you can import those users based on a template of a user with the new privilege set. The unique database ID for the replaced users is not changed so that ownership and other historical information is not affected; however, all account attributes, such as product-access type, privileges, and preferences, are replaced.

  CAUTION:

  The **Replace user** option completely overwrites existing user accounts. Use this feature cautiously.

Import Spreadsheet Options

Use the following options to import and map data in a spreadsheet to user, resource, and *Contacts* records attributes.

- **Spreadsheet File**

  Browse to a spreadsheet that is formatted based on the specifications in Preparing a Spreadsheet for Importing Users [page 352].

- **Import users as a copy of**
  Click **Find** to search for a user who should serve as a template account for imported users. Imported accounts contain mapped attributes from the spreadsheet, along with the template user's product-access type, role assignments, group membership, privileges, preferences, notification subscriptions, and password settings.

  Note: If the template user has a private report specified as a Home Page report, the "All Active Items I Own" built-in report for the preferred application is set as the Home Page report for imported users.

- **Create Associated Contacts**

  Select this check box to automatically create *Contacts* table records for imported users.

- **User Attribute Map**

  The User Attribute Map section contains information from the selected spreadsheet. Use this information to correctly map data in the spreadsheet to SBM user accounts, resource, and *Contact* records. For guidance, refer to Mapping Attributes to SBM Fields [page 353].

  - **Spreadsheet Column Titles**

    Lists the information in the first row of the spreadsheet. This is considered a header row used for mapping and data in this row is never imported as a user record.

  - **Spreadsheet Sample Data**

Lists information from the second row of the spreadsheet. Data in this row is provided to assist you with mapping and is also imported with a user account.

- **User Attributes**

  Select the applicable user attribute from the list for each column title. At a minimum, you must map the Login ID and E-mail attributes.

Importing Users and Contacts From LDAP

SBM enables you to import and update user accounts, resources, and *Contacts* record information from a directory using LDAP.

LDAP requires external setup, which varies based on the LDAP provider you are using. In general, these instructions assume that your LDAP system is configured and that you have access to it and understand basic LDAP concepts. If you will use a secure connection to LDAP, refer to Preparing LDAP for SBM [page 360] ror information about preparing CA certificates for use with SBM.

Note: *On-premise only* – For information about using LDAP to authenticate users and the LDAP "auto add" feature, refer to the *SBM System Administrator Guide*.

- **LDAP User Import**

  Use search filters to specify the users you want to import, and then import those users as "copies" of an existing SBM user. You can choose to create *Contact* records for imported users as well. For details, refer to Importing LDAP Users [page 360].

- **Import LDAP Users as SBM Contacts** – You can import LDAP users as contacts by mapping LDAP user attributes to *Contacts* table fields, and then importing selected LDAP users. For details, refer to Importing Contacts From LDAP [page 361].

- **Update SBM User Account Information** – You can update mapped LDAP attributes for all SBM users and contacts at once. You can limit the number of users you update by product-access type, account status, or by using a search filter to select a set of users and/or contacts to update. For details, refer to Updating Users and Contacts from LDAP [page 362].

LDAP Import Considerations

Consider the following information before you import or update user accounts and contact information from LDAP:

- You can use the SBM Application Administrator to import users and contacts from LDAP. You can also update resource attributes by mapping data from LDAP.
- Managed administrators must be granted the **Global Administration** privilege to use this feature in SBM Application Administrator.
- If LDAP fields contain sensitive data that administrators should not see, privileges can be specified in the LDAP tool to limit administrators' access to these fields.
- Care must be taken when you modify and delete mapped fields in LDAP and SBM. For example, if the name of an attribute is changed in LDAP, it is no longer mapped to the SBM field. Also, fields that are deleted in either tool are no longer mapped.

- Contact imports only apply to the SBM system *Contacts* table. You cannot import from LDAP into custom auxiliary tables that store contact data.
- When you update User and *Contact* records, SBM fields that contain data are not modified if the mapped field in LDAP is empty. For example, if a *Contact* record contains a phone number and the LDAP record does not, the phone number for the *Contact* record is retained after updating. To update SBM with an LDAP attribute that has no active replacement, you must set the LDAP attribute to some non-empty value such as "none."

Preparing LDAP for SBM

On-premise only.

If you will connect to LDAP using a secure connection, you must prepare your system according to the information below.

The CA Certification file is generated differently for each directory service. To determine how your CA Certification file is generated, consult your directory's documentation on how to set up a certificate authority and generate a DER-encoded root certificate or a PEM-encoded multi-certificate chain of trust.

Once you've created the root certificate, perform the following steps:

1. Using the newly generated root certificate, sign a server certificate for the LDAP server.
2. Place the root certificate on the server that hosts SBM Application Engine and enter the full path to that root certificate in the **Certificate location** field.
3. Grant the Internet Guest Account (IUSR_machinename) permissions to this directory. This is required to ensure that authentication succeeds when you deploy process apps from SBM Composer or SBM Application Repository.
4. Clear the **Secure connection** check box to successfully connect to the LDAP server *without* using the key file to make sure that you have it configured properly.
5. Select the **Secure connection** check box and verify the full path in the **Certificate location** field.
6. Test again and it should connect successfully.

Note: If you are using multiple Web servers, the key file must either reside in a fully qualified network path accessible by all servers or a copy of the key file must reside in identically named paths on each server. For performance considerations, copy the key file in identically named paths on each server.

Importing LDAP Users

You can import user accounts from LDAP into SBM. Use search filters to specify the users you want to import, and then import those users as "copies" of an existing SBM user. Optionally, you can choose to create Contact records for imported users as well.

Tip: If you want contact records to be associated with SBM user accounts, import contact data at the same time you import user account data.

When you import user records, uniqueness is guaranteed by the login ID and the LDAP UID. A new user is not automatically added if a user already exists with the same login ID.

To import user accounts from LDAP:

1. From the **Administrator Portal**, click **Import Users**.
2. Select the **Import users from LDAP** option.
3. Specify LDAP search and server settings as described in LDAP Search Settings [page 364].
4. Click **Refresh** in the LDAP Sample Attributes Data section until you find an LDAP user with attributes that match the users you want to import into SBM.
5. Map SBM user attributes to LDAP attributes, following the steps in User Attributes Map [page 368].
6. Optionally, specify group attributes to create new SBM groups based on LDAP groups for imported users. Use the **Group Query Parameters** section to limit the groups that are created. For details, refer to User Attributes Map [page 368].
7. In the **User Import Options** section, click **Find** to select a template SBM user and replacement options as described in User Import Options [page 369].
8. Optionally, select the **Create Associated Contacts** check box to create SBM contact records for imported users. For details, refer to User Import Options [page 369].
9. Specify an additional filter, and then click the **Refresh** button in the **Find Candidates** section to return a list of potential LDAP users to import.

   Tip: If no results are returned with the specified filter, click **Refresh** in the **LDAP Attributes Sample Data** section, and then click **Refresh** again in the **Find Candidates** section.
10. Select the users you want to import.
11. Set logging parameters as described in LDAP Logging and E-mail Options [page 366].
12. Scroll up, and then click the Save icon next to **Import Option Set**. Save your settings so that they are available to you for future imports. For details, refer to Saving Import Options [page 378].
13. Click **Import**.
14. Select the **Import Log** tag to monitor the progress of your import.

Importing Contacts From LDAP

You can choose to import contact data only from LDAP into SBM.

Note: If you want to associate contact information with imported user accounts, follow the steps in Updating Users and Contacts from LDAP [page 362] and make sure to select the **Create associated contacts** check box.

When you import *Contact* records, uniqueness is determined by the specified equality key.

Also, if you have added the *Active/Inactive* optional system field to your *Contacts* table, be sure that its default value is set to **Active**. If not, *Contact* records imported from LDAP are not visible in SBM. Also, if your *Contacts* table contains required fields, set default values for these fields so that contacts imported from LDAP are guaranteed to have values.

To import contacts from LDAP:

1. From the **Administrator Portal**, click **Import Users**.
2. Select the **Import contacts from LDAP** option.
3. Specify LDAP search and server settings as described in LDAP Search Settings [page 364].
4. Click **Refresh** in the LDAP Sample Attributes Data section until you find an LDAP user with attributes that match the users you want to import into SBM.
5. Map SBM *Contacts* table field to LDAP attributes, as described in Contacts Attributes Map [page 372].
6. Select options for handling existing contact data as described in the information in Contact Import Options [page 373].
7. Specify an additional filter, and then click the **Refresh** button in the **Find Candidates** section to return a list of potential LDAP users to import as contacts.
8. Select the contacts you want to import.
9. Set logging parameters as described in LDAP Logging and E-mail Options [page 366].
10. Scroll up, and then click the Save icon next to **Import Option Set**. Save your settings so that they are available to you for future imports. For details, refer to Saving Import Options [page 378].
11. Click **Import**.
12. Select the **Import Log** tag to monitor the progress of your import.

Updating Users and Contacts from LDAP

You can update mapped LDAP attributes for all SBM users and contacts at once. You can also limit the number of users you update by product-access type, account status, or by using a search filter to select a set of users, a set of contacts, or a set of users and contacts to update. The update process only updates changed LDAP values in SBM user attribute, resource attribute, and system *Contacts* table fields.

When you update user records, uniqueness is guaranteed by the login ID and the LDAP UID. When you update *Contacts* records, uniqueness is determined by the specified equality key.

To update user and contact information from LDAP:

1. From the **Administrator Portal**, click **Import Users**.

2. Select the **Update from LDAP** option.
3. If you have an import option set containing user and contact import mappings, select it from the **LDAP Option Set** drop-down list. If you do not have an import option set available, create one using the guidance in LDAP Search Settings [page 364].
4. Click **Refresh** in the LDAP Sample Attributes Data section until you find an LDAP user with attributes that match the users you want to import into SBM.
5. Select **Update Users** to update mapped attributes for user accounts, and then select options to limit the updated user accounts based on information in User Update Options [page 375].
6. Select **Update Contacts** to update mapped attributes for contacts, and then specify a search filter to limit update contact records based on information in Contact Update Options [page 376].
7. Set logging parameters as described in LDAP Logging and E-mail Options [page 366].
8. Scroll up to the top of the page. In the **Scheduling** section, click **Add** to create a scheduled update, or click **Update Now** to begin an update immediately.
9. Select the **Import Log** tag to monitor the progress of your import.

LDAP Import Settings

Use the **Import Options** page to set LDAP search and server options and settings for each type of import.

For details, refer to:

- LDAP Import - Server Options [page 363]
- Options for Importing Users from LDAP [page 367]
- Options for Importing Contacts from LDAP [page 372]
- Options for Updating from LDAP [page 375]

LDAP Import - Server Options

Use the **Import Options** page to select the type of LDAP import you would like to perform, set up a schedule, enter LDAP search settings, and define logging.

Note: This section describes options applicable to all import types.

For information about options for specific import types, refer to:

- **Import users from LDAP** - Refer to Options for Importing Users from LDAP [page 367].
- **Import contacts from LDAP** - Refer to Options for Importing Contacts from LDAP [page 372].

- **Update from LDAP** - Refer to Options for Updating from LDAP [page 375].

LDAP Scheduling Options

This section enables you to schedule LDAP imports and updates. For example, if you want to ensure that SBM user data is synchronized with your LDAP user data, create a schedule that will automatically update your SBM users from LDAP on a recurring basis.

Tip: You must enter valid LDAP search settings before you can schedule an import or update task.

Status messages for scheduled imports and updates appear in the Notification Server log file (click **Open Log** in the **Notification Server** tab in SBM Configurator to view the messages).

After you have defined one or more LDAP option sets, click **Add (+)** to launch the scheduler. In the **LDAP Scheduling** dialog box, select an LDAP Option Set to schedule, enter the desired frequency that it should execute, and then click **OK**.

To delete an existing schedule, select the schedule, and then click **Details** or double-click. In the **LDAP Scheduling** dialog box, click **Remove schedule**, and then click **OK**. A summary of the scheduled import or update appears in the **Scheduling** section.

LDAP Search Settings

Save LDAP import option sets so that you can reuse them for scheduled imports and for updating user account and contact data. Server information, user and contact attribute mapping, and template user settings are saved with the import option set.

- **LDAP Option Set**
  Use the following options to manage and reuse LDAP search option sets. LDAP option sets marked with an asterisk indicate that they are currently used by a scheduled import or update.
  - **Add (+)**

    Select this icon to clear existing search settings and create a new LDAP search option set.

  - **Save (**  **)**

    Select this icon to save settings as an LDAP search option set.

  - **Delete (**  **)**

    Select this icon to delete an LDAP search option set.

- **Server**

  Specify the server name, IP address, or fully qualified domain name of the LDAP server. If your directory is replicated on more than one server, list each server's name separated by a space. If a replicated server uses a different port than is specified in the **Port** box on this dialog box, type *:portnumber* after the server name.

- **Port**

Specify the port number of the directory server. The default setting for LDAP using clear text is 389; the default LDAP port for Secure Sockets Layer (SSL) is 636. You can specify a different port if necessary for your installation.

- **Secure connection**
  Select this check box to connect to LDAP via Secure Sockets Layer (SSL). If this check box is selected, the **Port** setting automatically changes to 636, which is the default LDAP port for SSL. You can alter this value if necessary.

  Tip: SSL is less efficient than the clear text authentication method because response times may be slower. For best results, use the unencrypted bind whenever possible. If your SBM server and directory server are local to one another, it may be unnecessary to use SSL.

- **Certificate location**
  This field is enabled if the **Secure connection** check box is selected. Enter the full path to the certificate on the SBM Application Engine Web Server. This certificate is used by Application Engine for Web service authentication requests that do not have SSO security tokens. SBM accepts the following encoded certificates:

  - A DER-encoded root certificate for the issuer of the LDAP server certificate. If you choose to specify a DER-encoded certificate, it must be the root certificate authority (CA) certificate, and the LDAP server must be configured to transmit all other certificates in the chain of trust during the SSL handshake.

  - A PEM-encoded file that includes the root CA certificate and, optionally, any intermediate CA certificates in the chain of trust. If a multi-step SSL chain of trust must be honored by SBM to connect to LDAP, you can specify a single PEM file that contains the root CA certificate and any intermediate CA certificates. If there are intermediate CA certificates that are not included in this file, the LDAP server must be configured to transmit those certificates during the SSL handshake.

    Important: The LDAP server must *not* require client authentication, as SBM does not supply a client certificate.

- **Search Base**

  Type the Directory root at which searching for user information will begin. All nodes at and beneath the base are searched for records of users being authenticated. The search timeout period is 30 seconds.

- **Search Filter**
  Select one of the provided search filters or type your own search filter. The search filter is used to authenticate users and for mapping and updating user information. The search filter must contain one or more format specifiers ({0} for the first, {1} for the second—if needed), which are replaced by SBM at runtime with the SBM login ID of the user being authenticated. For example:

  ```
  (&(objectClass=user)(sAMAccountName={0}))
  ```

  In this case, when user "Joe Smith" attempts to log in, the {0} specifier is replaced by his SBM login ID `jsmith` and he is authenticated against LDAP. The authentication will succeed if the SBM login ID matches his LDAP `sAMAccountName` value and he provides the proper password.

- **Follow Referrals**

Select this checkbox to enable LDAP referrals. This feature can enable SBM to locate LDAP user objects on separate servers in the event that some users can not be found in the primary server's LDAP directory. If your LDAP directory entries are split across two or more LDAP servers, the primary LDAP server can be configured to respond to queries in multiple ways:

- If the primary server enables "chaining", it will automatically search any secondary servers and build a list of responses as though all the entries were on the primary server. In this scenario, SBM does not need to be configured to search other servers.
- If the primary server does not enable "chaining", it may return "referrals" for the secondary servers. In that case, SBM must either follow the referral by directing a new search request to the secondary server, otherwise SBM will not find any directory entries that are not on the primary server.

If all of the entries of interest to SBM are on the primary server or if the primary server enables chaining, then SBM does not need to follow referrals; if there are necessary entries on a secondary server and the primary server does not do chaining, then SBM should be configured to follow referrals.

Note: There are some limitations on how SBM will interact with secondary LDAP servers when following referrals. Because the Search DN and password may only be applicable to the primary server, queries to secondary servers will be performed anonymously. Consequently, the secondary LDAP servers must allow anonymous searching and authentication in order for SBM to follow referrals successfully.

- **Search DN**

  Type the distinguished name of an LDAP user account that has permission to search and read other user accounts that are to be authenticated in or imported into SBM. If your LDAP provider allows anonymous searches, this box can be empty. If a DN is provided, however, it must be an active and valid LDAP account located in the same root level directory specified in the Search Base and not in a subordinate container. The DN must be able to search all subordinate containers, so it must be placed in a root level directory that encapsulates the rest of the containers that hold your user accounts.

- **Password**

  In the **Password** box, type the password for the user account specified in the **Search DN** box. The password is encrypted before it is stored in the SBM database.

LDAP Attributes Sample Data

This section contains sample data to assist you in mapping LDAP attributes to SBM attributes. Initially, the section does not contain any information. Click **Refresh** to populate the section with LDAP attributes and sample data from a user in your LDAP store. Click **Refresh** to see sample data from other users in your LDAP directory.

User accounts are listed based on the order they are stored in the LDAP directory.

LDAP Logging and E-mail Options

Use these options to send a copy of the import log file by e-mail when the import process completes and to send e-mail messages to newly imported users.

The Notification Server must be configured and running to send import logs and new user confirmations. On-premise customers use SBM Configurator to manage the Notification Server. The Notification Server is enabled in on-demand systems.

Change these options as needed:

- **Send the log by e-mail when import completes**

  This check box is selected by default. Clear it to stop the import log from being sent by e-mail.

- **E-mail**

  By default, the user logged into SBM Application Administrator when the import process is started is sent the log message. Change the e-mail address as needed. To send the log to multiple addresses, separate each address with a comma.

- **Log Level**
  In the drop-down list, select one of the following options:

  - **None**

    Select to disable logging.

  - **Minimal**

    Select to log minimal information about LDAP imports and updates, such as the number of users imported and updated.

  - **Detailed**

    Select to log detailed information about LDAP imports and exports, including field mapping assignments.

  - **Verbose**

    Select to log detailed trace information about LDAP imports and exports, such as the login IDs of the accounts imported or updated. If you are experiencing trouble with this feature, set the logging to Verbose to assist you or Serena support staff in diagnosing problems.

- **Send notification e-mails to created users**
  Select this check box to send e-mail messages to newly imported users. The message is sent to the address that is added during the import process and includes login information. Users must change their password on their first login attempt.

  Note: On-premise customers can use SBM System Administrator to modify the template for e-mails sent to newly imported users. This template is located on the **External Users** tab of the **Settings** dialog box.

Options for Importing Users from LDAP

The following options are available when you select the **Import users from LDAP** option on the **Import Users** page. You must first apply LDAP server and search options before you can import users. For details, refer to LDAP Import - Server Options [page 363].

User Attributes Map

The **User Attributes Map** section enables you to map user account attributes defined in the LDAP schema to SBM user, resource, and contact attributes. The mapping assignments apply to importing and updating user records.

You must first provide LDAP server connection and search specification settings and successfully connect to the LDAP server before mapping user attributes.

- **SBM User Attributes**
  This column lists the following SBM user account attributes:
  - Four user account attributes (login ID, name, telephone, and e-mail)
  - All non-system, fixed-length *Text* fields in the *Contacts* table
  - The *Companies* system field from the *Contacts* table
  - Resource attributes, including Job Functions and Skills.

  Note: SBM user accounts must have a login ID and name. If an imported user account does not contain a name value, the LDAP login ID value is added as the user's name.

- **Mapped LDAP User Attributes**
  Select an LDAP attribute to map to the SBM user attribute.

  Tip: You can map attributes from multiple LDAP accounts, if necessary. To do this, map the attributes from the first LDAP account returned after you click **Refresh** in the **LDAP Attributes Sample Data** section. If this account does not contain all the attributes you need, click **Refresh** again to return another LDAP account. Map attributes as needed from this account, and continue to click **Refresh** until you have mapped all necessary attributes.

  Tip: If you have multiple LDAP attributes with the same name, and you map one of the attributes to either resource Teams or resource Skills, SBM uses the values from each attribute to create multiple teams and skills. For example, if you have three `objectClass` attributes in LDAP (each with different values) and you map `objectClass` to Skills, then three different skills are added to the associated resource record.

- **Group Attributes**

  Type one or more LDAP user attributes in a comma-separated list, similarly to the group query parameters, that should be examined by SBM to create new groups when users are imported.

  For example, if you select `memberOf` as the attribute, SBM will only use the containers in the `memberOf` LDAP attribute as possible groups for the new user. Each `memberOf` attribute on the user's LDAP account will be examined. You can select more than one attribute. Group Attributes must contain distinguished names, and the elements within those distinguished names are used as group names (subject to filtering by the Group Query Parameters, if any are specified).

  For example, if you want to create groups based off the parameters in both the `memberOf` and `productTeam` attributes, you would select:

```
memberOf
productTeam
```

In LDAP, user "Joe" might have the following values for these attributes:

```
memberOf: CN=Domain Admins,DN=Users,DC=Acme,DC=com
memberOf: CN=Managers,DN=Users,DC=Acme,DC=com
productTeam:  OU=DevTeam,DC=Acme,DC=com
```

SBM would then potentially be able to use any CN, DN, or OU parameter in any attribute to create corresponding groups. You can limit the groups that will be created by specifying specific parameters instead using **Group Query Parameters**.

Note: If the **Group Attribute** field is left empty, SBM considers the entire Full Directory Name (also known as `distinguishedName`) as the attribute to examine (for example, `CN=LDAPTest,OU=QAGroup,DC=acme,DC=com`). In this case, the first parameter is ignored by SBM to avoid creating a group call "LDAPTest", which is typically a user account and not a group. Whenever the `distinguishedName` attribute is specified, the first parameter will be ignored.

- **Group Query Parameters**

  Enter the particular parameters you want SBM to process when attempting to create new groups. In effect, this field acts as an additional filter on the **Group Attributes** you specify. For example, you might only want the CNs and OUs of each attribute examined. In that case, you would enter:

  ```
  CN,OU
  ```

  Using the example stated for group attributes, these parameters would only create new groups based off the CNs and OUs in each attribute, which would result in the creation of the following groups:

  ```
  Domain Admins
  Managers
  DevTeam
  ```

User Import Options

Use the following options to select a template user account, handle existing users, and, optionally, create associated contact records that are associated with the imported accounts.

- **Import Users as a copy of**

Click **Find** to search for or select an SBM user account that serves as a template account for imported users. Once selected, the name, login ID, and product-access type of the selected user template account is shown in the **Import Users as a copy of** box. Imported accounts contain the values of mapped attributes, along with the product-access type, role assignments, group membership, privileges, preferences, application settings, notifications subscriptions, and password settings of the template account. This process is similar to copying an SBM user account.

Note: If the template user has a private report specified as a **Home Page** report or a Quick Link, users whose accounts are imported will receive an error when they run that report. For best results, select a template user whose application settings specify built-in or non-private level reports.

- **Create Associated Contacts**
  Select to automatically create *Contact* records that are associated with imported users. Contact records imported with a user account contain values for the mapped *Contact* table fields and the values for *Contact* table fields that are not listed on the **User Map** tab (First Name, Middle Name, Last Name, E-mail, and Phone Number).

  CAUTION:

  If you import an LDAP user as a contact and later want to import that LDAP user as an SBM user, a duplicate *Contact* record is created if the **Create Associated Contacts** check box is selected. If you do not select the **Create Associated Contacts** check box when later re-importing the contact as an SBM user, that user account will not have a *Contact* record associated it, even though the original *Contact* record remains in the system. In other words, newly imported users are not automatically associated with existing *Contact* records. If you import users with the **Create Associated Contacts** check box selected, new *Contact* records associated with imported users are created. This applies to users that are automatically added to SBM as well. An alternative to importing contacts as users is to utilize the "Grant Login" feature in *Contacts* records.

- **If user already exists**
  Select one of the following options for handling LDAP user accounts that have the same login ID as SBM accounts. The comparison of login IDs between LDAP and SBM is not case-sensitive.

  - **Do not modify**

    Select this option to ignore LDAP user accounts that already exist in SBM.

    Tip: If the user already exists, but does not have an associated resource record, a new resource record is created for that user if you map any resource attributes.

  - **Replace mapped attributes**

    Select this option to update any mapped attributes that have changed in LDAP. This option is useful for updating information in existing SBM accounts while you import new accounts from LDAP.

  - **Replace user**

    Select this option to replace existing SBM user accounts with the mapped and template user attributes. This option is useful for quickly modifying multiple user

account attributes in SBM. For example, if a user is promoted to a managerial position, you can import that user based on a template from an existing manager's account. The unique database ID for the replaced user does not change so that ownership of primary items is not affected; however, all account attributes, such as product-access type, privileges, preferences, etc., are replaced. Because this option enables you to completely overwrite an existing user's account, use this feature cautiously.

- **Alias**

  On-demand only – Use the **Alias** field to enter an e-mail address domain that will be appended to the **Login ID** for imported users. For example, if you map Bill's **sAMAccountName** (`Bill`) to **Login ID** and enter `@acme.com` in the **Alias** field, Bill is imported with a **Login ID** like `bill@acme.com`.

Find Candidates Options

Use this section to query LDAP for a list of potential users or contacts who can be imported into SBM. You can then select candidates to import.

- **Refresh**

  Click to initiate the search for LDAP users matching the criteria specified in the search filter. When the search is complete, the LDAP users who match the search criteria are listed. You can sort the list by clicking on the column headings.

  Tip: If the desired user is not found, click **Refresh** in the **LDAP Attributes Sample Data** section, and then try again.

  Note: The amount of time needed for the search depends on the speed of the connection to the LDAP server and the number of users qualified by the search.

- **Select All**

  Click to select all candidates in the list.

- **Clear All**

  Click to clear your selections.

- **Filter**
  Select a search filter or type a new search filter. The search filter you provide depends on how user accounts are organized in LDAP and the type of user accounts you want to import. For example:

  - You may want to include *objectClass=SBMUser* (or a similar value, depending on your LDAP configuration) in your search filter to return all LDAP users classified as SBM users.
  - If groups exist in your LDAP system that are similar to groups in SBM, include the group name in your search filter criteria. Other attributes such as organizational unit, department, and title might also be useful.
  - Consider common traits of users as you construct search filters. For example, (telephoneNumber=555*) returns accounts in which users have phone numbers beginning with 555.

- **Import**

  Select candidates you want to import.

- **Exists in SBM**

  A disabled checkmark indicates that a user or contact matching the LDAP attributes already exists in SBM.

- **Login ID**

  Listed for user imports. Indicates the SBM login ID.

- **Name**

  Listed for user imports. Indicates the SBM user name.

- **First Name**

  Listed for contact imports.

- **Last Name**

  Listed for contact imports.

Options for Importing Contacts from LDAP

The following options are available when you select the **Import contacts from LDAP** option on the **Import Users** page. You must first apply LDAP server and search options before you can import contacts. For details, refer to LDAP Import - Server Options [page 363].

Contacts Attributes Map

The **Contact Attributes Map** enables you to map user account attributes defined in the LDAP schema to fields in the SBM *Contacts* table. The mapping assignments apply to importing and updating *Contact* records.

- **SBM Contact Attribute**
  This column lists the following *Contacts* table fields:
  - All non-system, fixed-length *Text* fields
  - The *Company* system field (used on-premise only)
- **Mapped LDAP Attribute**
  Type or select an LDAP attribute to map to the contact attribute. Use the attributes listed in the **LDAP Attributes Sample Data** section for guidance.

  Tip: You can map attributes from multiple LDAP accounts, if necessary. To do this, map the attributes from the first LDAP account returned after you click **Refresh** in the **LDAP Attributes Sample Data** section. If this account does not contain all the attributes you need, click **Refresh** again to return another LDAP account. Map attributes as needed from this account, and continue to click **Refresh** until you have mapped all necessary attributes.
- **Equality Key?**
  After LDAP attributes and *Contact* fields are mapped, select at least one field to use as an equality key. An equality key is required for importing *Contact* records and

helps ensure uniqueness. Consider the following information when you select an equality key:

- Equality key values must be identical in LDAP and SBM. The match is not case-sensitive, but space usage must be identical.
- Values in equality key fields are never updated when you use LDAP Import or Update features in SBM, so choose fields that have values that you expect to remain constant.
- *First Name* and *Last Name* fields might not be the best choices for equality keys due to possible duplicate values, name changes, misspellings, etc. An e-mail field might be a better choice.
- If your LDAP configuration contains an attribute such as a Customer Number, consider creating a similar field in the *Contacts* table and using these as equality keys. Remember when you create the field in SBM Composer that only fixed-length *Text* fields can be mapped to LDAP attributes.

Contact Import Options

Select one of the following options for handling LDAP user accounts that have the same equality key value as *Contact* records.

- **Do not modify**

  Select this option to ignore LDAP user accounts that already exist in SBM as *Contact* records.

- **Replace mapped attributes**
  Select this option to replaced mapped attributes that have changed in LDAP. This option is useful for updating information in existing *Contact* records when you import new records from LDAP.

  Tip: You can use the **Replace Mapped Attributes** option to selectively update *Contact* records with information from LDAP. To update all *Contact* records in the SBM database based on a search filter and specified equality keys, use the **Update from LDAP** feature.

- **Create duplicate**

  Select this option to ignore specified equality keys and create duplicate *Contact* records containing mapped attribute values. Use this option cautiously, however, because when you later update *Contact* records, either or both *Contact* records can be updated with identical values, depending on the equality keys in effect at the time of the update.

Find Candidates Options

Use this section to query LDAP for a list of potential users or contacts who can be imported into SBM. You can then select candidates to import.

- **Refresh**

Click to initiate the search for LDAP users matching the criteria specified in the search filter. When the search is complete, the LDAP users who match the search criteria are listed. You can sort the list by clicking on the column headings.

Tip: If the desired user is not found, click **Refresh** in the **LDAP Attributes Sample Data** section, and then try again.

Note: The amount of time needed for the search depends on the speed of the connection to the LDAP server and the number of users qualified by the search.

- **Select All**

  Click to select all candidates in the list.

- **Clear All**

  Click to clear your selections.

- **Filter**
  Select a search filter or type a new search filter. The search filter you provide depends on how user accounts are organized in LDAP and the type of user accounts you want to import. For example:

  - You may want to include *objectClass=SBMUser* (or a similar value, depending on your LDAP configuration) in your search filter to return all LDAP users classified as SBM users.
  - If groups exist in your LDAP system that are similar to groups in SBM, include the group name in your search filter criteria. Other attributes such as organizational unit, department, and title might also be useful.
  - Consider common traits of users as you construct search filters. For example, (telephoneNumber=555*) returns accounts in which users have phone numbers beginning with 555.

- **Import**

  Select candidates you want to import.

- **Exists in SBM**

  A disabled checkmark indicates that a user or contact matching the LDAP attributes already exists in SBM.

- **Login ID**

  Listed for user imports. Indicates the SBM login ID.

- **Name**

  Listed for user imports. Indicates the SBM user name.

- **First Name**

  Listed for contact imports.

- **Last Name**

  Listed for contact imports.

Options for Updating from LDAP

Use the **Update from LDAP** option to update mapped LDAP attributes for all SBM users and contacts at once. You can also limit the number of users you update by product-access type, account status, or by using a search filter to select a set of users, a set of contacts, or a set of users and contacts to update.

The update process only updates changed LDAP values in SBM user attribute and *Contact* table fields.

You must first apply LDAP server and search options. This means if you performed an initial user import and you want to map new attributes, you must map those attributes on the **Import Users from LDAP** page, save the **LDAP Option Set**, and then perform or schedule a new update operation. For details, refer to LDAP Import - Server Options [page 363].

User Update Options

The following options are enabled when you select the **Update Users** check box:

- **Update existing SBM users whose access level is:**

  Select product-access levels applicable to the user accounts you want to update.

- **And whose status is**

  Select active users, deleted users, or both.

- **Search Filter**

  By default, the search filter specified in the **LDAP Search Settings** section is used.

- **Override search filter for user update**

  Click to modify the specified search filter or provide a different filter for the update.

- **Remove users if no matching LDAP entry is found**

  Select to remove users from SBM who cannot be found in your LDAP store. These users will be marked as deleted upon the next update.

  This setting affects even those users who were not automatically added from LDAP. Any user who cannot be found in LDAP will be marked as deleted. If you do not want to impact these users, you can try to limit who is deleted by selecting only users with a certain product access or status in the check boxes above.

- **Remove users matching this LDAP filter**

  Select to identify LDAP users that should be marked as deleted in SBM. For example, the following filter removes any user that has the LDAP attribute "deleted" set to "true."

```
(&(&(objectClass=user)(sAMAccountName={0}))(deleted=true))
```

Any attribute can be used to flag users that should be deleted. In this example, if Joe is selected for update and has a "deleted" attribute value of "true" in LDAP, then on the next update Joe will be marked as deleted in SBM. However, he will not be removed from any of the groups to which he currently belongs.

Note: The various product-access levels and the active or deleted status check boxes can be used to further filter users that should be removed. The filter you provide in the **Remove users matching LDAP filter** field acts an additional filter beyond the main search filter.

- **Alias**

  On-demand only – Use the **Alias** field to enter an e-mail address domain that will be appended to the **Login ID** for updated users. For example, if you enter `@acme.com` in the **Alias** field, Bill's **Login ID** is updated to: `bill@acme.com`. Note that if you have already appended an alias when you imported users, any value that you enter here is appended to the end of the current **Login ID**; therefore, ensure that you want to append another alias before entering a value here.

Contact Update Options

Use the following options to limit the contact records to update.

The following considerations apply to Search Filters for updating *Contact* records:

- The search filter must contain the same number of *{0}* format specifiers as Equality Keys.
- The *{0}* format specifiers must also be in a specific order. If you edit the search filter, do no change the order of filter components.
- If an Equality Key field does not have a value in SBM, the search filter is modified to contain an absence filter component before the search begins. For example, if you have selected first name, middle name, and last name fields as Equality Keys, and the contact you are updating does not have a value in the middle name field (Sally Smith, for example), the final search filter is formatted as: *(&(objectClass=inetOrgPerson)(givenName=Sally)(!(initials=*))(sn=Smith))*

Select the **Update Contacts** check box to enable the settings.

Note: To update *Contact* records associated with a user account, you must update the user record. For details, refer to Options for Importing Users from LDAP [page 367].

- **Search Filter**

  By default, the search filter specified in the **LDAP Search Settings** section is used.

- **Override search filter for user update**

  Click to modify the specified search filter or provide a different filter for the update.

Import Log

Use the **Import Log** page to view the progress of an import and view the log for that import.

Note: By default, the log information is sent by e-mail to the user performing the import process. You can modify the e-mail settings on the **Import Options** page.

The following log options are available:

- **Clear Log**

  Click to remove an existing import log.

- **Refresh**

  Click to refresh the current log.

- **Auto Refresh**

  Click to automatically refresh the current log every 10 seconds.

- **Import Progress**

  Shows the progress of the import currently in progress.

- **Import Log**

  Shows the log for the current or last import. Select **All** to show the full log; select **Errors** to show only errors that occur during the import process.

- **Copy Log to Clipboard**

  The log is overwritten after each replacement. To save log information, click the **Copy Log to Clipboard** button, and then paste the log information into a separate document.

Refer to the following sections for details about importing users from a spreadsheet:

- Importing New Users from a Spreadsheet [page 355]
- Updating Users From a Spreadsheet [page 356]
- Importing Users From a Spreadsheet [page 351]

Refer to the following sections for details about importing users from LDAP:

- Importing LDAP Users [page 360]
- Importing Contacts From LDAP [page 361]
- Updating Users and Contacts from LDAP [page 362]

Refer to the following sections for details about importing data:

- About Data Import [page 378]
- Steps for Importing Data [page 382]
- Data Import Settings [page 383]

Saving Import Options

Use the **Import Option Sets** options to save mappings for future use. You can save settings for:

- **Data imports from spreadsheets**

  You can store field mappings for selected import tables. Saved field mappings can be used by any administrator who has privileges to submit and update items into the table selected for the field map.

- **LDAP user and contact imports**

  You can store LDAP server and search settings, attribute mappings, user import options and import selection lists. Saved option sets can be used by any administrator who has privileges to import from LDAP.

Be sure to save any changes made to import option sets so that they are available for future updates and for other users.

For details about data imports, refer to About Data Import [page 378].

For details about importing from LDAP, refer to Importing Users and Contacts From LDAP [page 359].

About Data Import

Use the Import Data feature to add new items or update existing items from a spreadsheet. You can import items into an auxiliary table or a specific project in a primary table (application table).

For details, refer to:

- Steps for Importing Data [page 382]
- Data Import Settings [page 383]
- Best Practices for Importing Data [page 386]
- Other Options for Importing Data [page 388]

Note: SBM provides several mechanisms for importing data. For details on which import feature best meets your needs, refer to Other Options for Importing Data [page 388].

Preparing a Spreadsheet for Importing Data

The key to achieving a successful import lies in taking the time to prepare source data for importing. This requires an intimate knowledge of the field types and existing data in your system, and of the data you are importing.

Spreadsheets used to import data must adhere to the following requirements:

- Only files of type .xls can be imported. If you have an .xlsx file or any other type of spreadsheet file, you must convert it to .xls.
- Only data from the first worksheet in a file is imported.
- You can only import one spreadsheet at a time.

- You can only import into a single project or auxiliary table at a time.
- Spreadsheet columns represent SBM fields and all spreadsheet data is treated as text. Spreadsheet columns must be formatted as Text types.
- Each row represents an item that will be imported, except for the first row, which is used to define columns available for mapping. Data from this row is never imported.
- To import primary items, the spreadsheet must include columns for the system *State* and *Title* fields.
- To import auxiliary items, the spreadsheet must include a column for the system *Title* field.
- If you are using the import to update items, include a column that can be used to determine uniqueness. For details, refer to Record Matching [page 380].
- For best results, limit the number of rows to 10,000. To import more than 10,000 items, create multiple spreadsheets and import them separately.
- To ease data mapping, label spreadsheet columns with the same name as your SBM fields. This enables you to use auto mapping.

Here is an example of a simple spreadsheet used to import users:

	A	B	C
1	**TITLE**	**TECHNICIAN**	**State**
2	Upgrade from 4.0 does no	Newton Technician	Assigned
3	Change icons to more mo	Newton Technician	Assigned
4	404 page not found error	Laura Technician	Assigned
5	502 Error	Laura Technician	Assigned
6	New color scheme	Laura Technician	Assigned
7	Please update the UI with	(None)	Resolved
8	404 page not found error	(None)	Resolved
9			

In this example, row 1 defines the columns to be mapped. This information is not imported. Row 2 is used as sample data, but data is imported.

Import Privileges

The following privileges are required before administrators can import new items or update existing items.

Privilege	Privilege Location	Notes
Remote Administration	User - System page	Grant to enable administrators to log into SBM Application Administrator.

Privilege	Privilege Location	Notes
Submit New Items	User - Item page (primary items) User - Table page (auxiliary items)	Grant to enable administrators to import new items to a specific project or auxiliary table.
Update All Items	User - Item page (primary items) User - Table page (auxiliary items)	Grant to enable administrators to use the Data Import feature to update existing items.

Record Matching

To use the Import Data feature to update existing primary and auxiliary items in your system, you need a field in your application that contains a unique value for each primary and auxiliary item and a column in the spreadsheet that contains unique values for each row. You must then map the unique SBM field to the spreadsheet column that contains unique values.

During the import process, the value of each row is matched against existing values in the system. Matching is case insensitive.

If a match is found, the existing item is updated with data from the spreadsheet if the **Replace mapped attribute** option is selected. If no match is found, a new item is created.

CAUTION:

If the values in either SBM or the spreadsheet are not unique, you may have unexpected results. For example, you may update an existing primary or auxiliary item from multiple rows or data may be updated in the wrong SBM item.

Field Mapping Considerations

You can map to most SBM fields; exceptions are the *Project* field, primary *Multi-Relational* and primary *Single Relational* fields, *Multi-User* fields, *Folder* fields, *Sub-Relational* fields, the system-provided *Last Incident* field, and deleted fields.

Note: The import process ignores the read-only setting for fields. If you map to a read-only field, data in the spreadsheet is added or updated, based on import settings.

The following information provides guidance on mapping to specific fields or field types.

Item IDs

- To automatically generate Item IDs for newly imported items, do not map a spreadsheet column to the Item ID field. When IDs are generated, numbering properties specified for the project apply to the imported items.

- To retain Item IDs from data in the spreadsheet, map the ID column to the Item ID field, but be aware that doing so overrides the system's automatic ID generation and may result in duplicate Item IDs.
- To retain historical data while automatically generating Item IDs, consider creating a custom field to store imported IDs and mapping to this field when you import data. For example, in SBM Composer, create a *Text* field named *Old ID Numbers*. After deployment, you can map the ID column in the spreadsheet to the *Old ID Numbers* field. This enables users to search for the old ID numbers, but ensures unique, system-generated IDs in imported items.
- If you use *Item Type* prefixes, such as ENH for enhancements, include a column in the spreadsheet for item types (Requests, for example) and map this column to the system *Item Type* field. Each spreadsheet row can contain either the *Item Type* value, such as Request, or a prefix, such as REQ. SBM will match spreadsheet values to *Item Type* prefixes and values specified in SBM Composer.

States and Ownership

- When you import primary items, you must map a spreadsheet column to the *State* field.
- Each row in a column mapped to the *State* field must have valid data. Rows that do not have a *State* field value are skipped. If a row contains a value that does not match an existing state, the row is skipped.
- SBM states use the *Active/Inactive* field to automatically determine the status of items in each state. You can map to the *Active/Inactive* field, but it is more beneficial to use the automatic setting of the *Active/Inactive* field.
- After importing data, review imported items to ensure they are owned by the correct users.

Selection Values

Selection values are unique to each of these field types:

- *Single Selection*
- *Multi-Selection*
- *User*
- *Single Relational (referencing auxiliary tables)*
- *Multi-Relational (referencing auxiliary tables)*
- *Multi-Group*

Data in spreadsheet rows for columns mapped to selection fields must match existing data in the system. If not, the row is skipped. Matching is based on case-insensitive searches of the selections available for a field. For *User* fields, matching is based on the login ID or name of users in the system.

Tip: Check for spelling consistency in field selections before importing data. For example, "Not Applicable" and "NotApplicable" are treated as separate selections.

Empty rows are imported as "none" values unless you select the **Set default values for empty cells** check box and the mapped field has a default value.

For guidance on importing multiple values to *Multi-Selection*, *Multi-Group*, and *Multi-User* fields, refer to Handling Multiple Selection Values [page 387].

Date/Time Values

- Spreadsheet columns must be formatted as Text types, including those for *Date/Time* fields. For best results, row data for *Date/Time* fields should follow these guidelines:
  - For SBM fields that are set as Date Only or Date and Time, spreadsheet data should match the display format, such as mm/dd/yyyy or mm/dd/yyyy hh:mm:ss. After the import process, values will appear to users in the format specified in their user profile.
  - Date/Time keywords, such as startof_lastweek or endof_thisyear, can be used with *Date/Time* fields set as Date Only or Date and Time.
  - For Time Only or Elapsed Time fields, specify spreadsheet values in this format: hh:mm, hh:mm:ss, or d hh:mm:ss (Elapsed Time fields only).
- If you do not map to system *Date/Time* fields, such as *Submit Date* and *Close Date*, values may be established as the date items were imported.

Text Field Values

Spreadsheet data should comply with *Text* field settings. For example, if you map to a *Text* field set to have a fixed length of 80 characters and a spreadsheet row has 100 characters, the last 20 characters are truncated in the imported item.

Steps for Importing Data

For guidance on the settings on the **Import Options** page, refer to Data Import Settings [page 383].

To import data from a spreadsheet:

1. Prepare a spreadsheet using the guidance in Preparing a Spreadsheet for Importing Data [page 378].
2. From the **Administrator Portal**, click **Import Data**.
3. In the **Data Source and Destination** area, browse to the spreadsheet that contains the data you want to import.
4. From the **Import into table** list, select the primary or auxiliary table to which data will be imported.
5. If you select a primary table, select the project to which data will be imported. Only projects you have privileges to submit items into are available.
6. To avoid duplicate items in your system, select the following options as they apply:
   - To import all rows in the spreadsheet as new items, do not select a spreadsheet column for duplicate detection.

- To modify existing SBM items while importing new items in the spreadsheet, select a column for duplicate detection, and then select the **Replace mapped attributes** option.
- To keep existing SBM items intact while importing new items in the spreadsheet, select a column for duplicate detection, and then select the **Do not modify** option.

7. In the **Field Mapping** area, map spreadsheet columns to SBM fields, using the information in Field Mapping Considerations [page 380] for guidance.
8. Click **Import**.
9. When the import process is complete, run a report to review imported items to verify they imported as expected. If not, modify your spreadsheet and repeat the import process.

Note: The user performing the import and the time of the import are reflected in the Change History.

Data Import Settings

Use the **Import Options** page to set options for importing spreadsheets, including data mapping and duplicate record handling.

Data Source and Destination

Use these options to select a spreadsheet that contains records to be imported and the destination for these items in SBM.

Note: The administrator performing the import operation must have privileges to submit items into the selected table or project (for primary items).

- **Spreadsheet**

  Browse to a spreadsheet that is formatted based on the specifications in Preparing a Spreadsheet for Importing Data [page 378].

- **Import into table**

  The list contains tables that the importing user has privileges to submit items into and that is configured to allow imports. For on-premise systems, this setting can be found on the **Advanced** tab of the **Edit Table** dialog box in SBM System Administrator.

  Select the primary or auxiliary table into which data will be imported.

- **Project**
  If you select a primary table, you must also select a project into which items will be imported.

Note: The **Allow new items to be submitted** option must be selected on the **General** page for the project you select. In addition, you must have privileges to submit items into the selected project.

Duplicates

Optionally, select a spreadsheet column to detect and handle duplicate records in the spreadsheet and the selected project or auxiliary table. If you do not specify a column for duplicate detection, new records are added for every row in the spreadsheet.

Detection is based on identical values in the spreadsheet row and the SBM field. For guidance, refer to Record Matching [page 380].

The following duplication detection options are available:

- **Spreadsheet column for duplicate detection**

  Select the spreadsheet column that should be used for duplicate detection. Values in the column's row are matched with values in SBM fields.

- **If matching record exists in SBM database**:
  - **Do Not Modify**

    Select this option to ignore duplicate items in the spreadsheet and leave existing SBM items intact.

  - **Replace Mapped Attributes**

    Update mapped fields in existing SBM items based on data in the spreadsheet.

Notification E-mail Options

Use these options to send a copy of the import log file by e-mail when the import process completes and to send e-mail messages to newly imported users.

The Notification Server must be configured and running to send import logs and new user confirmations. On-premise customers use SBM Configurator to manage the Notification Server. The Notification Server is enabled in on-demand systems.

Change these options as needed:

- **Send notification e-mail when import completes**

  This check box is selected by default. Clear it to stop the import log from being sent by e-mail.

- **E-mail**

  By default, the user logged into SBM Application Administrator when the import process is started is sent the log message. Change the e-mail address as needed. To send the log to multiple addresses, separate each address with a comma.

Field Mapping

Use the **Field Mapping** section to map spreadsheet columns to SBM fields. You can save field mappings for specific tables and reuse them for additional imports and updates. For guidelines, refer to Field Mapping Considerations [page 380].

- **Field Mapping**

  This drop-down list stores field mappings saved for the selected import table. This enables you to quickly perform additional imports or update existing data. Saved field mappings can be used by any administrator who has privileges to submit and update items into the table selected for the field map.

Use the options to manage field mappings:

- **Set default values for empty cells**

  Select this check box to use default values for cells that do not contain data. If a default value is not set for the mapped field, the field value is empty after the import is complete.

- **Save ()**

  Select this icon to save field mappings.

- **Clear**

  Select to clear existing mappings and create new field mappings.

- **Delete ()**

  Select this icon to delete a field mapping.

- **Spreadsheet Columns**
  - **Column**

    Lists the information from the first row of the spreadsheet. This is considered a header row used for mapping and data in this row is never imported as a data record.

  - **Sample Data**

    Lists information from the second row of the spreadsheet. Data in this row is provided to assist you with mapping and is also imported as a primary or auxiliary item.

  - **SBM Field**

    As you map fields, this column shows the SBM field mapped to the spreadsheet column.

- **Mapping Options**
  - **Auto Map**

    Click this button to automatically map similar columns in the spreadsheet to SBM fields. Matching is based on a case-insensitive comparison of the spreadsheet column header and the field name.

  - **Map**

    To map fields individually, select a spreadsheet column and an SBM field, and then click **Map**.

  - **Unmap**

    To individually unmap fields, select a spreadsheet column and an SBM field, and then click **Unmap**.

  - **Unmap All**

    Click this button to remove all field mappings.

- **SBM Fields**
  - **Search**

    Search for fields by display name. Searches are case-insensitive.
  - **Field Name**

    Indicates the display name for the SBM.
  - **Type**

    Indicates the type of SBM field.

Best Practices for Importing Data

Resolving Import Problems

Inspect imported data after each process finishes. If data was not imported as you expected, modify your spreadsheet and import data again. Be sure to:

1. Review mapping guidelines specified in Field Mapping Considerations [page 380].
2. Modify spreadsheet columns and rows based on these guidelines.
3. Include a column that can be used to detect duplicate items in your system.
4. Select the **Replace mapped attributes** option on the **Import Options** page.
5. Map fields as needed.
6. Perform the import.
7. Inspect imported data.

Note: On-premise customers should consider backing up the SBM Application Engine database before beginning a data import.

Generating Item IDs

If you are importing new issues into a project, take advantage of SBM's automatic Item ID assignment. If you do not map to the SBM Item ID field, the system will generate Item IDs based on numbering properties for the project you are importing into.

For best results, include a column in the spreadsheet for item types (Requests, for example) and map this column to the system *Item Type* field. Each spreadsheet row can contain either the *Item Type* value, such as Request, or a prefix, such as REQ. SBM will match spreadsheet values to *Item Type* prefixes and values specified in SBM Composer.

Mapping Users to Imported Data

If your spreadsheet contains columns that will be mapped to *User* fields, verify that imported data corresponds to existing login IDs or user names. If data in a row is not matched to user accounts, the row is skipped.

If accounts do not exist for imported items, use the Import Users feature to import users before you import associated data. This enables you to import users as a copy of an existing user, which saves manual configuration later.

Handling Selection Field Values

Values for selection fields, such as *Single Selection* and *User* fields, must exist in your system before you can import items that include these values. Spreadsheet rows that contain invalid values for these field types are skipped.

To prevent errors on import, review the guidelines in Field Mapping Considerations [page 380] and verify that existing values are available before you import data.

Handling Multiple Selection Values

If you are mapping to *Multi-Selection*, *Multi-Group*, or *Multi-User* fields and you want to add multiple selection values to one of these fields, follow these steps:

1. In your spreadsheet, create one row for each selection you want to add to a field that allows multiple selection values. For example, if you want to add two values to a *Product Version* field, create two rows.
2. Make sure each column for these rows has identical data, except for the *Product Version* field. For example, the *Title* and *State* columns should have identical data, but the *Product Version* column should include a single value for each row, such as Version 1 and Version 2.
3. On the **Import Options** page, select a field in the **Spreadsheet column for duplicate detection** list, and then select the **Replace mapped attributes** option.
4. Import the spreadsheet.

One item should be imported, but the "multi" field will have two values.

Handling Required Fields

You do not need to provide data for required fields in order to import them, but users will need to provide valid values for required fields before they can work with imported items.

If you choose not to import values for required fields during the import process, verify that required fields are visible to users who might update or transition imported items, and that they have permissions to modify required fields.

Setting (None) Values

You can set *Multi-Group*, auxiliary *Multi-Relational*, *Multi-Selection*, auxiliary *Single Relational*, *Single Selection*, and *User* fields to have "None" values after import. This can be useful if you are re-importing data and want to clear previously imported values for fields.

To do so, clear data from spreadsheet rows mapped to applicable fields before the import and be sure to clear the **Set default values for empty cells** check box in the **Field Mapping** area.

Importing Contacts

For best results, use the Import User feature to establish items in the system *Contacts* table. This ensures that spreadsheet data is correctly mapped to *Contacts* fields. For details, refer to Spreadsheet Import Options [page 356] and Mapping Attributes to SBM Fields [page 353].

After you establish *Contacts* records through the Import User feature, you can use the Import Data feature to update additional data for *Contacts* records as needed.

Other Options for Importing Data

SBM offers several options for importing data into the system. The option you choose to use depends on:

- The type of data you want to import.
- The source of the data to import.
- Your access to administrative capabilities, such as the SBM database and the SBM System Administrator (on-premise customers only)

Data import options are:

Data Type	Source	SBM Feature	Use When...
Primary and auxiliary items	Spreadsheet	Import Data feature in Application Administrator	• You are able to export data from another tool into a spreadsheet or you are able to easily create a spreadsheet for adding or updating items. • You do not need to import values for selection-type fields. • You do not have ODBC access to the SBM database or SBM System Administrator.
Values for *Single Selection* and *Multi-Selection* fields	Comma-separated values, spreadsheet	Selection import/ export feature in SBM Composer	• You need to quickly add or modify values for these field types. • You only want to import selections, and not primary and auxiliary items.

Data Type	Source	SBM Feature	Use When...
Primary and auxiliary items; values for selection fields, such as *Single Selection* and *User* fields	ODBC Data Source	Import Data feature in SBM System Administrator (on-premise customers only)	• You have ODBC access to the source database and to SBM System Administrator. • You have a good understanding of the data in both the source and destination databases. • You have a large amount of data to import. • • You are importing from another SBM database and want to import change history records and attachments. • You want to import mapped selection values along with imported primary and auxiliary items. If you dot this, you are also able to perform a "get process app" in Application Repository after importing data that adds values to *Single Selection* and *Multi-Selection* fields. You must then open the process app from the repository in SBM System Administrator before you deploy the process app again. If you do not perform these steps, the imported selections are deleted the next time you deploy the process app.

About Auxiliary Data

Use the Auxiliary Data feature to add and edit items in auxiliary tables.

The Auxiliary Data feature is useful for quickly adding or updating a few auxiliary items at one time. To add or update a large number of auxiliary items, consider using the Data Import feature. You must have administrative privileges to import auxiliary items, however. For details, refer to About Data Import [page 378].

The Search Page

Use the **Search** page to select an auxiliary table and provide search criteria for specific fields. The fields available for searching are those for which the **Appears on Lookup Form** check box is selected in SBM Composer.

Tables for which you have "view" privileges are available in the **Table** list.

After you provide search criteria, click **Search** to return a list of results in the **Search Results** pane.

Click the column headers to sort the results lists. The first column may contain multiple fields specified by your administrator. You can sort this column by the values in this field.

For example, if the column contains a *Title* and *First Name* field in that order, results may appear as:

Manager, Adam

Manager, Bruce

Manager, Carol

Based on your privileges, you can edit items in the list or add new items to the table.

Tip:

Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Adding New Auxiliary Items

Click the **New** button to open the **Submit** form for the selected auxiliary table. Provide data for the item as needed, and then click **OK**.

To add auxiliary items, you must have privileges to submit items in the selected table.

Editing Auxiliary Items

Select an item in the results list, and then click **Details** to open the item in a "view" form. Depending on your privileges, you can update or delete the item. You can also send e-mail messages, add attachments, and other actions, depending on your privileges.

Tip: If the results list contained multiple items, use the navigation arrows at the bottom of the page to move through the list. Use the breadcrumbs at the top of the page to return to the **Search** page.

About Calendars

By default, SBM calculates time using a 24-hour/seven-day-week calendar. You can create custom calendars to establish hours of operation, however, and assign them to the following features:

- **Duration Reports**

  You can specify a calendar for Duration reports, such as Time in State and Average Time to State reports. This enables you to calculate the amount of time items remain in a particular state or how long it takes items to reach a state based on your organization's hours of operations. For details on using calendars with Duration reports, refer to the *SBM User's Guide*.

- **Notification Escalations**
  You can assign a calendar to notification escalations to ensure that they are generated only during your organization's hours of operation rather than 24 hours a day, seven days a week. This prevents escalations from generating repeatedly over weekends and during holiday breaks, for example. You can assign a custom calendar to each notification escalation, or you can assign custom calendars to user accounts, and then select one of the following options for each notification escalation:

  - **User Owner**

Performs time calculations based on the calendar set for the current owner of the item being assessed for escalation.

- **User Submitter**

  Performs time calculations based on the calendar set for the submitter of the item being assessed for escalation.

For details on using calendars with escalations, refer to About Escalations [page 271].

- **Resources**

  You can create separate calendars and assign them to resources to determine a resource's weekly working hours. This is then used to calculate capacity in Serena Demand Center and to calculate time distributions for the Time Capture feature. Ideally, you should create and use unique calendars for resources to prevent any conflict with other features that may rely on calendars. For details, refer to About Working Hours, Capacity, and Scheduling [page 408].

Elapsed time for these features is calculated based on each calendar's defined operating hours. For example, the time to escalate may be set to 8 hours, and a calendar's hours of operation is set at Monday through Friday from 8 a.m. to 5 p.m. If an event that triggers an escalation to fire begins at 3 p.m. on Friday and the event is not resolved, an escalation is sent at 2 p.m. on the following Monday.

Note: Calculations are not combined for multiple calendars, and you can only apply one calendar to each notification escalation or report.

Using Calendars Across Multiple Time Zones

A time zone is set for each calendar, and this time zone is used for all calculations based on the calendar. Time zones applied in each user's preferences do not automatically apply to hours of operation calculations.

To apply hours of operation across multiple time zones:

- Create calendars for specific time zones, and then apply them to individual notification escalations and reports.
- Create calendars for specific time zones, and then assign them to users in those time zones.
- For notification escalations, select the User Owner or User Submitter calendars to apply them to the time zones set for the calendar assigned to the user who owns or submits an item when it is evaluated for escalation.

  Note: Notification escalations that use the User Owner or User Submitter calendars are calculated against an item's current owner or submitter. This user may change during the time-to-escalate period. For example, if a user with a US/Eastern time zone owns an item for two hours, and then assigns the item to a user with a US/Pacific time zone, the escalation is fired based on the user with the US/Pacific time zone.

Calculating Elapsed Time for State Changes

By default, elapsed time for state changes is recorded based on a 24-hour day, seven-day week. A record is added to the database every time a primary item moves from one state to another. These records are used for calculating elapsed time for the Average Time to State duration reports.

Note: If you upgraded your system from Serena TeamTrack and you want to report on elapsed time for state changes on primary items in the database before the upgrade, you should run the `PostUpgradeUtil.exe` AFTER you upgrade but BEFORE you use the new report types. For details, refer to *Moving to Serena® Business Manager*.

You can also create custom calendars to use for duration reports. This allows users to run reports that show elapsed time for state changes based on the hours of operation defined in the calendar. To record elapsed time for state changes based on a calendar, select the **Save Elapsed Time for Calculating State Changes in Duration Reports** check box located on the calendar's **General** page.

The following information applies to elapsed time calculations for state changes:

- Recording of elapsed time for state changes used by duration reports begins when the **Save Elapsed Time...** check box is selected for a particular calendar and ends if this check box is cleared. Reports that use calendars with this check box selected only return data for the period when elapsed time for state changes was collected.
- Elapsed time for state changes made to primary items outside of a calendar definition are recorded as zero. For example, if a calendar defines hours of operation from 9 a.m. to 5 p.m., and an item changes state at 7 p.m., the elapsed time for that state change is recorded as zero.
- Creating a large number of calendars that record elapsed time for state changes could impact your system's performance.
- Elapsed time records for state changes cannot be deleted or archived.
- If a calendar that is used by existing reports is deleted, users who execute the reports are notified that the report will no longer reflect time-in-state data.

Calendar Settings

Use calendar settings to create calendars, define a standard week for each calendar, and set overrides, or exceptions, to the standard week. For details about calendars, refer to About Calendars [page 390].

Calendars View

The **Calendars** view lists custom calendars created for your system.

The following options are available on the **Calendars** view:

- **Add**

  Click to add a new calendar.

- **Details**

  Select a calendar, and then click to modify it.

- **Delete**

  Select a calendar, and then click **Delete**. If you delete a calendar that is assigned to a notification escalation, user account, or report, the default 24-Hour Calendar is applied. If you delete a calendar that is used by existing reports, users who execute the reports are notified that the report will no longer reflect time-in-state data.

- **Copy**

  Select a calendar, and then click to copy it. You must provide a unique name for the copied calendar.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

For details about calendars, refer to About Calendars [page 390].

General Calendar Options

Use the following options to set a time zone and standard work week for the calendar. For details using about calendars, refer to About Calendars [page 390].

- **Name**

  Provide a name of no more than 64 characters (bytes).

- **Time Zone**

  Select a time zone used for all calculations for the features to which the calendar is assigned. By default, Greenwich Mean Time (GMT) is selected. For details, refer to Using Calendars Across Multiple Time Zones [page 391].

- **Hours in a Standard Day**

  Specify the number of hours in a typical day for your organization. For notification escalations that use days as the time interval to send an escalation, the number of days specified is converted to the number of hours you indicate in this setting. For Time in State Trend reports, the number of hours you specify is used to calculate the number of days specified as time groups. For Average Time to State Trend reports, the number is used to calculate duration based on the time interval that is chosen to total report results.

- **Hours in a Standard Week**

  Indicates the total number of hours specified in the standard week section.

- **Save Elapsed Time for Calculating State Changes in Duration Reports**

Select to record the amount of time primary items spend in each state based on this calendar. For details, refer to Calculating Elapsed Time for State Changes [page 392].

Applying Hours for a Standard Week

Use this section to set a standard week for your calendar. For example, you can specify standard working times for each day of the week and each day can have its own standard times. You can specify a single time frame, such as 8 a.m. to 5 p.m. or break each day into multiple segments, such as 8 a.m. to 12 p.m. and 1 p.m. to 5 p.m.

By default, the standard week is set from Monday to Friday, 9 a.m. to 5 p.m.

To change the default standard week, select the **Calendar** icon for the day you want to modify, and then set new start and end times, OR:

1. From the list, select the day you want to modify or add to the calendar.
2. Click **Add** to add a new start and end time, or select a time frame and click **Delete** to remove it for the selected day.
3. Repeat these steps above for each workday as needed.
4. To create exceptions, such as holidays, to the standard week select the **Overrides** tab. For details, refer to Calendar Overrides [page 395].

Calendar Overrides List

The **Overrides** page lists overrides for the selected calendar. Overrides enable you to create exceptions, such as holidays, to the standard week. For details using about calendars, refer to About Calendars [page 390].

The following information is included for each override:

- **Override Date**

  Indicates the exact date for the override.

- **Yearly**

  If selected, the override occurs on an annual basis.

- **Note**

  Indicates the title or description provided for the override.

The following options are available on the **Overrides** page:

- **Add**

  Click to add a new override.

- **Details**

  Select an override, and then click to modify it.

- **Delete**

  Select an override, and then click to remove it.

- **Copy**

Select an override, and then click to copy it.

Calendar Overrides

Overrides enable you to create exceptions, such as holidays, to the standard week. Overrides apply only to the selected calendar. For details using about calendars, refer to About Calendars [page 390].

Provide the following information for each override:

- **Note**

  Provide a short title or description for the override.

- **Apply these working hours on a yearly recurring basis**

  Select this check box to set the specified day as an override every year.

- **Calendar**

  Use the calendar to select the day that should be set as an exception to the standard week.

- **Add**

  With a date selected, click **Add** to set a specific time frame for the override. For example, you may set limited hours for the day before a major holiday.

- **Delete**

  To remove an override time frame, select it, and then click **Delete**.

About Channels

Notification Channels enable you to send SBM notifications to your users through different messaging mediums in addition to standard e-mail. This means you can notify users not only through e-mail, but also through other mediums such as instant message (IM), social networks, and short message service (SMS).

(On-premise only) – You must register one or more plugins in SBM Configurator before you can create new channels. For details registering notification server plugins, see the *SBM Installation and Configuration Guide*.

There are two types of channels you can create:

- **Broadcast Channel** – Broadcast channels send messages to a target that is not an SBM user. For example, if you register the Twitter plugin in SBM Configurator, you can create one or more broadcast channels to post notification messages to Twitter walls that users can view.

  Note: You can create multiple broadcast channels for the same plugin. For example, you can create three separate channels using the Twitter plugin to post messages to three different Twitter walls.

- **Non-Broadcast Channel (User Channel)** – Channels that are not broadcast are considered user channels. These types of channels send messages to specific SBM users. For example, if you register the Google Talk plugin in SBM Configurator, you can create a user channel to send notifications to subscribed users via IM.

After you successfully create a channel, you can select the channel when you add or edit a notification. For details on using channels with notifications, refer to General Notification Settings [page 288].

Key Benefits

- Notify users using one or more messaging services.
- Broadcast important information to all users.
- Broadcast important information to a subset of users.
- Increase user interaction with your system.

Channel Settings

Use channel settings to create new channels and define specific channel parameters. For details about channels, refer to About Channels [page 395].

- Channels View [page 396]
- General Channel Options [page 396]

Channels View

The **Channels** view lists custom channels created for your system.

The following options are available on the **Channels** view:

- **Add**

  Click to add a new channel.

- **Details**

  Select an existing channel, and then click **Details** to modify it.

- **Delete**

  Select a channel, and then click **Delete**.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

For details about channels, refer to About Channels [page 395].

General Channel Options

Use the following options to create a new channel and enter its parameters. For details using about channels, refer to About Channels [page 395].

- **Name**

  Enter a name for the channel that will help you identify it in notifications.

- **Description**

  Enter a description of the channel.

- **Plugin**

  Select the channel's associated plugin from the drop-down list. (On-premise only) – You must register the plugin in SBM Configurator before you can associate it to a channel.

  Note: The default plugins for on-demand customers are RSS and XMPP.

  Tip: Click the edit icon to change the display name of the plugin. This enables you to change the plugin name to a more user-friendly version for users that will enter their own recipient IDs in their user profiles.

Setting Channel Parameters

Use this section to set the channel's parameters.

- **Broadcast Type** – Select this check box to create a broadcast channel. Broadcast channels send messages to a target that is not an SBM user. For example, if you want notification messages to be posted to a generic Twitter wall, select this option.

  Otherwise, clear the check box to create a non-broadcast, "user" channel. Use this option to have notifications for this channel sent to specific users that are subscribed to the notification or escalation. For example, you can create a non-broadcast user channel that uses the XMPP plugin to sends messages to select users via instant message (IM).

  User channels require specific recipient IDs. Users can manage their own recipient IDs in their user profiles, or you can manage recipient IDs for each user in the Channels tab. For details, see User Channel Settings [page 162].

  Note: This option is read-only for certain plugins. For example, Twitter-based channels are broadcast-only, so the check box is selected by default and set to read-only. XMPP-based channels send messages to specific users, so the check box is cleared and read-only.

- Certain plugins require parameters to receive messages from SBM. For example, if you configure a plugin for a social network like Twitter or Facebook, you must create a new social network account and an associated developer application in order to retrieve OAuth credentials that the channel will use to post updates to the account's Twitter or FaceBook wall. For more information about creating and registering plugins, visit http://www.serena.com/support and search for solution S139424.

About Localization

Use the Localization feature to translate or modify text for end-user interfaces, including Work Center, User Workspace, and Serena Request Center (version 5.0 and later). Default strings are provided for the English (United States), or en-US, locale.

Restriction: Users must have the Remote Administration privilege to modify or translate strings.

Use the Localization page to:

- Translate strings for design objects that are created in SBM Composer into another language. For details, refer to Design Object Strings [page 398].

- Translate strings for global design objects into another language. For details, refer to Global Design Object Strings [page 400].
- Override the default labels, messages, and strings for scheduled report e-mails that are sent by the Notification Server. For details, Notification Server Strings [page 400].
- Override the default labels, messages, and strings for interfaces such as Serena Request Center and Serena Request Center. For details, refer to Work Center and Request Center Strings [page 400].

The following string types cannot be translated or modified using the Localization feature:

- User data, such as report titles, feed names, and primary or auxiliary item data.
- Display names for system views (My Dashboard, for example).
- Project names displayed in Work Center and User Workspace.
- Certain data generated by the Application Engine, such as text on report pages in Work Center.

On-premise customers can use the *Languages*, *Strings*, and *String IDs* system auxiliary tables to customize or translate strings generated by the Application Engine. For details, refer to the "Customizing and Translating SBM User Workspace Strings" section of the *SBM System Administrator Guide*.

String Localization Categories

The following topics describe the types of strings that you can translate.

- Design Object Strings [page 398]
- Global Design Object Strings [page 400]
- Notification Server Strings [page 400]
- Work Center and Request Center Strings [page 400]

Design Object Strings

You can use the Localization feature to translate strings for design objects that are created in SBM Composer into another language. Design object strings in a process app are available for translation in Application Administrator after you deploy the process app.

Each primary and auxiliary table in the process app appears as a category on the Localization page. Design object strings are organized by section within each category.

Design object strings that you can translate include:

- Name and Help Text for workflows, states, transitions, fields.
- Field selections
- Form strings (displayed on custom forms)
- Labels associated with tables (displayed on quick forms)

- Name, description, and tab name for applications
- Name, description, and singular name for tables
- Workflow annotation and swimlanes in the workflow diagram

Important: Translated strings appear in the diagram only if you have enabled HTML5 features. For details, refer to HTML Support Options (Base Project Only) [page 43].

You can select one or more language locales in Application Administrator using the **Predefined Locales** page, deploy a process app, and then translate the process app's design object strings into each defined locale. When translation is complete, users who select the locale for the translated version will see the translated strings. For details, refer to Predefined Locales [page 406].

Translated design object strings appear throughout the end user interfaces, including the following areas:

- **Items**

  When viewing items, translated strings appear for all form types (state, transition, printable) in the following:

  - Field names and help text
  - Change history and state change history
  - *Single Selection*, *Multi-Selection*, and *State* field values
  - Transition buttons
  - Custom form strings
  - Form labels

- **Workflow help**

  Translated strings appear in the workflow diagram that users can view from an item.

  Important: Translated strings appear in the diagram only if you have enabled HTML5 features. For details, refer to HTML Support Options (Base Project Only) [page 43].

- **Reports**

  In report results, translated field names appear in column headers and in results that include selection values. During report creation, translated field names appear for columns to display, filtering, and sorting. Sorting in report results does not use translated string names.

- **Notifications**

  Translated strings appear in notifications when design object strings (such as *Single Selection*, *Multi-Selection*, and *State* field names and selections) are included in the e-mail template.

Global Design Object Strings

You can use the Localization feature to override global design object strings. This enables you to translate the names of states and transitions that are included in every process app.

Customizable string elements for global design objects include:

- System transition names and help text
- System state names and help text

Tip: You must use the **Add** button to add locales and translations for strings in the **Global Design Object Strings** category. Predefined locales are not added for global design objects automatically.

Notification Server Strings

You can use the Localization feature to override the default labels, messages, and strings for scheduled report e-mails that are sent by the Notification Server.

Customizable string elements include:

- Labels and various elements in the e-mail message.
- Warning messages.

Work Center and Request Center Strings

You can use the Localization feature to override the default labels, messages, and strings for Work Center and Request Center.

Customizable string elements for these interfaces include:

- Static page headers, such as **My Applications** heading in Work Center.
- Static toolbar, button, and control labels, such as the **+New** button in Work Center or the **Approvals** tab in Request Center.
- Static view labels, such as the **My activity** label in Work Center.
- Hover text for static elements.
- Error and warning messages.

Translating Strings

Use one of these methods for translating the default English (United States) strings into another language:

- **Importing a Translated XML File**

  Ideal for sending strings to a translation vendor or for translating all default strings at one time. For details, refer to Translating Strings Using XML [page 401].

- **Localization Options in Application Administrator**

Recommended for users who are more comfortable working in an interface than in an XML file or when you are translating a small number of strings. For details, refer to Translating Strings from Application Administrator [page 402]:

When translation is complete, users who select the locale for the translated version will see the translated strings.

Important: String changes are global and impact your entire SBM installation or namespace (on-demand customers.)

Translating Strings Using XML

Use the Export option in Application Administrator to first create an XML file that contains the default English strings. You can then import this file after strings are translated.

Important: Do not modify the structure of the XML file or the values for each category and section. Instead, provide translations as overrides.

Each string is composed of the following elements in the XML:

- **Key**

  Container for each string, including values and tags for all locales.

- **Name**

  The key name for each string.

- **Locale**

  The locale for each key value.

- **Key Value**

  If no override is applied, the text that is shown to users for the specified locale.

- **Override**

  A way to customize a string and maintain the provided value. Overrides, if provided, are always shown to users.

- **Tag**

  Customizable label for each key value.

The following example shows the XML for a key that has an override for the English value, a translated key value, and an override and tag for that translation.

```
<Key>
        <Name>Approvals</Name>
        <KeyValue>
          <Locale>en_US</Locale>
          <Value>Approvals</Value>
          <Override>Votes</Override>
        </KeyValue>
        <KeyValue>
          <Locale>fr</Locale>
          <Value>Approbations</Value>
          <Override>Agréments</Override>
```

```
    </KeyValue>
    <Tag>First Translation</Tag>
  </Key>
```

To translate strings using XML:

1. In Application Administrator, click the **Localization** icon on the **Administrator Portal**.
2. Select the **Export** tab.
3. Select the category of strings to export.
4. Select the locale you want to export.
5. Click **Export** and save the file.
6. Open the file of exported strings in an XML or text editor.
7. Use search and replace to change the *<Locale>* value for each key.
8. Add your translation to the override tag for each string.

   Important: For on-demand customers, you must use the `<Override>` element to override or translate an existing key. You cannot import new keys, and if you attempt an import and you specify a new value for a key, it will be ignored.
9. In Application Administrator, select the **Import** tab, and then import the file.

Translating Strings from Application Administrator

Use the **Values** page to provide new translated values for languages other than the default English (United States) or other languages that have translations.

To modify strings:

1. Select language locales to use for translation on the **Predefined Locales** page.
2. Deploy the process app that you want to translate.
3. In Application Administrator, click the **Localization** icon on the **Administrator Portal**.
4. Select the **Values** tab.
5. Choose one of the following:
   - To modify design object strings, select a primary or auxiliary table category.
   - To modify global design object strings, select the Global Design Objects category.
   - Otherwise, select the Work Center or Request Center category.
6. Select a section that contains strings you want to translate. For example, to translate transition names for a primary table, select the **Transition Name** section.
7. Navigate to or search for the string you want to modify.

8. *On-premise* – Click in the **Value** column, and then provide the value that should be shown to users for each predefined locale. *On-demand* – Click in the **Override** column, and then provide the value that should be shown to users for each predefined locale.
9. Optionally, click in the **Tag** row and provide a label or comment for the string value.
10. Save your changes.

String Localization Settings

The following sections discuss localization settings.

- String Import Settings [page 403]
- String Export Settings [page 403]
- String Value Settings [page 404]
- Predefined Locales [page 406]

String Import Settings

Use the Import feature to import an XML file of translated or modified strings. For best results, use the Export feature to create the XML file that will be modified and then imported.

For details, refer to Translating Strings [page 400] and About Localization [page 397].

The following settings are available on the **Import** page:

- **Import**

  Click to import the selected XML file.

- **Discard**

  Click to discard changes made on the page.

- **XML File**

  Navigate to the XML file you want to import.

String Export Settings

Use the Export feature to export an xml file of strings available for translation.

For details, refer to Translating Strings [page 400] and About Localization [page 397].

The following settings are available on the **Export** page:

- **Export**

  Click to download and save strings for the selected category.

- **Discard**

  Click to discard changes made on the page.

- **Category**

Select the set of strings you want to export to a single file. Examples of available strings include:

- **<All>**

  Export all strings available for modification or customization.

- ***TableName***

  Export only strings for the selected table.

- **Work Center**

  Export only strings used in Serena Work Center.

- **Request Center**

  Export only strings used in Serena Request Center. This option is only available if Serena Service Manager is installed.

- **Locale**

  Select the locale to export.

String Value Settings

The following settings are available on the **Values** page.

For details, refer to About Localization [page 397].

Categories/Sections Settings

Strings are organized into:

- **Categories**

  Design object strings that are associated with primary and auxiliary tables from a deployed process app, or a full feature set, such as strings for Work Center or Request Center.

- **Sections**

  A grouping of strings within a category. For example, the **main** section in the Request Center contains strings from the main Request Center page. The **transition** section in a primary table contains transition name strings.

Navigate through the list of categories and sections or use the **Search** option to highlight a specific category or section.

Select a section to filter the content pane to strings in that section.

Value Settings

Use these options to manually modify or translate strings.

Toolbar Options

- **Add**

Click to add a value for a language other than the default, which is English (United States).

Tip: You must use the **Add** button to add locales and translations for strings in the **Global Design Object Strings** category. Predefined locales are not added for global design objects automatically.

- **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.

- **Language**

  Filter the list of strings by the selected language.

- **Search**

  Choose to search keys, values, or tags.

- **Modified**

  Select a date to list strings that have been modified since that date.

String Column Descriptions

Click a column header to sort the list.

- **Key**

  Depending on your filter, each key can show all values, languages, overrides, and tags for each string.

  Editable?

  No.

- **Language**

  Shows the language (locale) for a key.

  Editable?

  No.

- **Value**

  Shows the default key value for each language.

  Editable?

  No, for default strings. Yes for other locales (on-premise only).

- **Override**

  Shows changes to the default key value.

  Editable?

Yes. Click in the row to edit the value. On-demand users can translate strings using the **Override** column. Not applicable to default string values.

- **Section**

  Shows the category and section for each key.

  Editable?

  No.

- **Tag**

  Shows a label for each key, if defined. Tags enable you to provide comments as you work with strings. You can then search for keys by tags.

  Editable?

  Yes. Click in the row to edit the tag.

- **Last Modified**

  Shows the last date and time a key value was updated.

  Editable?

  No.

For more information, refer to Translating Strings Using XML [page 401].

Predefined Locales

Use the **Predefined Locales** page to select the language locales that should be defined for a process app when it is deployed. The locales that you select on the **Predefined Locales** page appear on the **Values** page for each design object string after a process app is deployed. Temporary values are supplied for all predefined locales until you translate them. Predefined locale selections are unique per namespace (on-demand customers).

To use predefined locales:

1. Select one or more predefined language locales.
2. Deploy a process app that contains design object strings that you want to translate.
3. After the process app is successfully deployed, export and import a translated XML file, or use the **Values** page to translate strings using your predefined language locales.

Note the following important information regarding predefined locales and process app deployment and promotion:

- The list of predefined locales is additive; a deploy activity will not remove predefined locales.
- When a process app is deployed, default string values are always overwritten; string values for predefined locales are not overwritten.
- You must use one of the methods described in step 3 above to modify the string value for a predefined locale.

- When a process app is promoted from one environment to another, default strings and translations that exist for predefined locales are overwritten in the target environment.

About Resources

Resources enable you to manage resource team assignments, scheduling, job functions, skills, and other attributes of employees in your organization. This information can be used for planning purposes.

To help coordinate availability and scheduling, you can assign an SBM calendar to each resource.

Use these elements to manage resources:

- **Resources**
  There are two types of resources:
  - **SBM User**

    Ideally, each resource is associated with an SBM user account. This enables you to assign work items to these resources once work has been planned.

  - **User**

    There may be cases where you do not need to associate a resource with an SBM user account. For example, you may create teams that mimic your organization's reporting structure. CEOs or vice presidents may not be assigned work items, but you may want to set them as team managers or track their contributions to planning processes.

  You can add resources manually or import them from a spreadsheet. For details, refer to Importing and Exporting Resources [page 410].

- **Resource Teams**

  A resource team is a collection of resources who are dedicated to the team either full time or for a percentage of time. This enables resources to be associated with multiple resource teams while ensuring that they are not over-allocated.

  In addition, when you assign resources to a team, their job functions and skills are automatically associated with the resource team.

  You can organize resource teams in a hierarchical structure that makes sense for your organization. For example, you may want to organize resource teams based on management reporting structure or by function.

- **Business Units**

  You can define business units that exist in your organization, and then associate them to resources. Each resource is assigned to a single business unit, such as Sales, Marketing, or R&D.

- **Departments**

  You can define departments that exist under each business unit in your organization, and then associate them to resources. Each resource is assigned to a single department, such as "Inside Sales" or "Software Development".

- **Job Functions**

  You can add job functions to your system, and then associate them with resources. Each resource is assigned a single job function, such as software developer or software tester. You can also specify the resource's **Title Group** and **Manager** as part of the job function. When a resource is assigned to a resource team, the resource's job function is automatically associated with the team.

- **Skills**

  To help ensure that resources are allocated where they are most needed, you can add various skills to your system, and then assign them to resources as they apply. For example, a developer resource may be competent in several programming languages, such as Java, C++, and Perl. You can add each of these languages as a skill, and then assign them to the resource. When a resource is assigned to a resource team, the resource's skills are automatically associated with the team.

- **Title Groups**

  You can add title groups to your system, and then associate them as part of a resource's job function. Each resource can have a single title group defined as part of its job function, such as "Front Line Managers" or "Executive Staff".

- **Types**

  You can add types to your system, and then associate them with resources. Each resource is assigned a single type, such as "Full Time", "Part Time", or "Contractor".

Resources and Reporting

You can create SBM reports that return data based on resource teams.

For example, you may want to report on items owned by resource "Team A." To do this, create search criteria that contains the condition "Owner contains any Members of Team A." This returns items that are owned by any member of Team A.

The "Members of: *Team Name*" value is at the bottom of the **Field Values** list when you create your report search specification. If there are more than 250 values available, you can search for the team name to return the "Members of: *Team Name*" value.

About Working Hours, Capacity, and Scheduling

When you assign resources to resource teams, you specify the percentage of time each resource is allocated to each team. The actual amount of time allotted to each resource team depends on the business calender assigned on the **General** tab for each resource.

For example, a Web Developer resource who works 40 hours is assigned to a calendar for full-time employees. This resource is assigned to two resource teams: IT Ops for 75 percent of the time and Marketing for 25 percent of the time. Therefore, the resource works with the IT Ops team for 30 hours and the Marketing team for 10 hours.

A Data Analyst resource may be assigned to the same two resource teams for 50 percent of the time, but is assigned to a business calendar for part-time employees who work 30 hours per week. In this case, the Data Analyst works with the IT Ops and Marketing teams for 15 hours a week.

Resource	SBM Calendar	Marketing Team Allocation	IT OPs Team Allocation
Web Developer	Full-time (40 hours)	75% (30 hours)	25% (10 hours)
Data Analyst	Part-time (30 hours)	50% (15 hours)	50% (15 hours)

Business calendars are created in SBM Application Administrator and assigned to each resource on the **General** tab. For details on managing SBM calendars, refer to About Calendars [page 390].

Process for Adding Resources

You can choose one of three methods to add resources to your system:

1. Import resources from a spreadsheet. This is useful if you want to export resource information from an identity store, such as LDAP. You can then import that information into a spreadsheet, quickly modify information for resource team assignments, skills and job functions, and more, before you import the spreadsheet into SBM. For details, refer to Importing and Exporting Resources [page 410].

2. Add multiple resources based on SBM user accounts. For details, refer to Adding Multiple Resources from SBM User Accounts [page 414].

3. Manually add resources, following the steps in the following section.

Regardless of the method you select, you should first create business calendars that reflect the working hours of your different resources. For example, you may have separate calendars for employees based in different countries so you can track holidays. For information about using calendars with resources, refer to About Working Hours, Capacity, and Scheduling [page 408].

Steps for Manually Creating Resources

Use these steps to manually add resources to Application Administrator.

1. Create business calendars that reflect the working hours of your resources. For details, refer to About Calendars [page 390].

2. Create business units that reflect specific business functions in your company. Examples are "Sales" or "Research and Development". For details, refer to The Business Units View [page 425].

3. Create departments that belong to each of your business units. Examples are "Inside Sales" or "Software Development". For details, refer to The Departments View [page 426].

4. Create job functions that reflect the positions that resources hold in your organization. Examples are "Manager" or "Web Developer." For details, refer to The Job Functions View [page 427].

5. Create skills that reflect the expertise of individual resources. Examples are "Java" or "Web Services." For details, refer to The Skills View [page 428].

6. Create title groups for your organization. Examples are "Front Line Managers" or "Executives". For details, refer to The Title Groups View [page 430].
7. Create types for your resources. Examples are "Full Time", "Part Time", or "Contractor". For details, refer to The Types View [page 431].
8. Create resource teams to group sets of resources. Examples are "US IT Operations" or "Web Development." For details, refer to The Resource Teams View [page 421].
9. Create resources, assign them to resource teams, and assign attributes to each resource. For details, refer to The Resources View [page 415].
10. Edit the resource teams, and set start and end dates and shared percentages for each member. You can also specify one resource as the team lead.

For example, you could create a resource record for SBM user Bill, who is responsible for Web development, as follows:

Resource Attribute	Value
Business Unit	Research and Development
Department	Software Development
Job Function	Web Developer
Skills	HTML, Web services
Title Group	Developers
Type	Full Time

Importing and Exporting Resources

To ease the process of adding resources and resource teams to your system, you can import them from a spreadsheet. The information in the spreadsheet can come from an external system, such as an Active Directory store or other Lightweight Directory Access Protocol (LDAP) providers, or you can manually create a spreadsheet as long as it meets the requirements discussed in the following sections.

Use the import feature to:

- Add new resource teams as parent teams or within a team hierarchy
- Add new resources
- Add resources to resource teams
- Assign skills and job functions to resources
- Assign a resource's manager
- Add skills and job functions to the system

- Add other attributes such as department, business unit, type, and title group to the system
- Assign new skills to existing resources
- Assign a job function to an existing resource who is not already assigned an existing job function
- Assign new resource teams to existing resources

Steps for Importing Resources

Use these basic steps to import resources:

1. In Application Administrator, click the **Resources** icon on the Administrator portal, and then click **Import/Export**.
2. Export a resource spreadsheet template. For details, refer to Export Resources Page [page 432].
3. Add data to the spreadsheet using the information in:
   - Spreadsheet Requirements [page 411]
   - Preparing the Resources Sheet [page 411]
   - Preparing the Teams Sheet [page 413]
4. Select the **Import** tab, and then import the spreadsheet.
5. Review the import log. For details, refer to Import Log [page 433].

Spreadsheet Requirements

The spreadsheet used to import resource teams and resources must adhere to certain requirements:

- Only files of type .xls can be imported. If you have an .xlsx file or any other type of spreadsheet file, you must convert it to .xls.
- The spreadsheet must contain exactly two sheets: one called Resources and one called Teams.
- Use care when adding data to the spreadsheet. In some cases, such as resource names, rows are skipped if data already exists in the system. In other cases, such as skills, new entries are added if data is similar but not identical. For example, "C++ (Level 1)" and "C++ (Lvl 1)" are considered separate skills.

Tip: The easiest way to prepare a spreadsheet is to first perform an export. You can use the empty spreadsheet as a starting point for meeting the following requirements.

Preparing the Resources Sheet

Each column represents a resource attribute. The information in this section describes the relationships between those attributes, as well as guidance on which are required, which are used for uniqueness checking, and data rules.

Each row represents a resource. Each resource may have multiple rows, depending on the number of teams the resource is assigned to.

Use the following information to prepare the **Resources** page of the spreadsheet.

Note: Rows that contain invalid date are skipped during the import process. Review the log for details regarding skipped rows.

- **Required Columns for Resources**
  - **Resource Name**

    For SBM User types, the resource name must be identical to that in the SBM user account.

  - **Type**

    Must be either User or SBM User.

  - **Login ID**

    For resources set as SBM User types, you must provide a login ID that matches the user's SBM login ID.

- **Uniqueness Checking**
  A combination of the following columns are used to determine if a resource already exists:
  - Resource Name
  - Type
  - Login ID (for SBM User types only)

  If row data is not unique for these columns, a new resource is added.

  For identical matches, resources are not added, but new attributes can be assigned to the resource if they were not already assigned to the resource.

- **Manager Information for Resources**
  - If the manager is not already a resource, you must add the manager as a row and import it with the resource.
  - You must indicate whether the manager type is User or SBM User.
  - For managers set as SBM User types, you must provide a name and login ID that matches those in SBM.

- **Importing Team Assignments for Resources**
  - Resource teams must exist in the system or be imported with resources before they can be assigned to resources during an import. Resource teams are imported on the **Teams** sheet of the spreadsheet.
  - A resource can be assigned to multiple resource teams. Create a row for each team to which a resource will be assigned, and specify start dates, end dates, and shared percentages for each team.

- A start date is required for all resource team assignments, but an end date is optional. Start dates must be in MM/DD/YYYY format.
- Shared percentages must be specified in integers only. For example, to indicate that a resource is assigned to a resource team for half of the time, use 50 and not 50%.
- If the shared percentage column is empty for a row, it is imported as 0.
- To assign a resource to a resource team in the hierarchy, use this format in the **Team** column:

  parent/child/child

  To prevent import errors, resource team names should not include a forward slash (/).

- **Importing Attributes**
  - If a resource attribute in the spreadsheet row does not exist in the system, it is added and assigned to the resource. If the attribute in the spreadsheet row exists in the system, it is assigned to the resource.
  - Skills and job functions require a level, which must be specified in parentheses after the skill or job function name. A space is required between the skill name and the parenthesis. For example, a job function might be "C++ (Senior)."
  - You can only specify one job function per row.
  - You can add multiple skills for a resource by separating them with commas. For example, "C++ (Senior), Java (Advanced)."
  - You can only specify one department, business unit, type, and title group per row. All of these attributes are optional.
- **Data Rules**
  - Data matching is case-insensitive. For example, USER, User, and user in the **Type** column is always interpreted as User.
  - Data in the **Start Date** and **End Date** columns must be in MM/DD/YYYY format.

Preparing the Teams Sheet

Resource teams must exist in the system or be imported with resources before they can be assigned to resources during an import.

Columns represent general resource team settings: name, description, and parent. Each row represents a single resource team.

Use the following information to prepare the **Teams** page of the spreadsheet.

- **Team Name**

  Required for imports.

- **Description**

  Optional for imports. The import process does not update the description for existing resource teams, however.

- **Parent**

  If no parent is specified, the resource team is added at the top of the team hierarchy. To import a resource team as a child, add the parent team by name to this row. Separate hierarchy levels with a foward slash (/) as follows:

  parent/child/child

The Team Name and Parent columns are used for uniqueness checking. If data does not match existing resource team records for both columns, a new team is added. If row data exactly matches existing data for both columns, the row is skipped.

Adding Multiple Resources from SBM User Accounts

Use these steps to quickly add multiple resources based on SBM user accounts:

1. From the **Administrator portal**, hover over the **Resources** icon, and then click the second **Resources** icon.
2. Click **Create from SBM Users**.
3. To copy the calender assignment and attributes of an existing resource to the new resources, search for the resource by name, and then select the resource from the results list.
4. Select one or more users from the list of available users, and then use the arrows to move them to the **Selected SBM Users** list. You can also drag and drop selected users to move them.
5. Click **Save**. Resources are created for the selected users.

Resource Settings

The following sections describe the options and settings available for resource management.

- The Resources View [page 415]
- The Resource Teams View [page 421]
- The Business Units View [page 425]
- The Departments View [page 426]
- The Job Functions View [page 427]
- The Skills View [page 428]
- The Title Groups View [page 430]
- The Types View [page 431]
- Export Resources Page [page 432]
- Import Resources Page [page 432]
- Import Log [page 433]

The Resources View

Use the **Resources** view to view, update, and delete resources in your system. Click the column headers to sort the list by name, job function, or resource type.

The following options are available on the **Resources** view:

- **Add**

  Click this button to add a resource.

- **Details**

  Select a resource, and then click this button to view or modify it.

- **Delete**

  Select a resource, and then click this button to delete it. (You must remove a resource's team or manager assignments before you can delete the resource.)

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Create from SBM Users**

  Click this button to open the **Create Resources** page, which enables you to create multiple resources based on SBM user accounts at one time.

- **Search**

  Search for resources by name, job functions, or skills.

The following information may be listed for each resource:

- Name
- Teams
- Job Function
- Skills
- Description
- Type

Tips for Using the Resources View

- If you need to add more than a few resources, consider importing them or using the **Create from SBM Users** option. For details, refer to Importing and Exporting Resources [page 410] or Adding Multiple Resources from SBM User Accounts [page 414].
- To see which resources have a specific skill or job function, search for the skills or job function.

- Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

General Resource Settings

Use the **General** page to define attributes for each resource.

The following options are available:

- **Type**
  Select one of the following resource types:
  - **SBM User**

    Selected by default, this option associates the resource with an SBM user account. Use this type for resources who will be assigned work items.

  - **User**

    Select this option to add a resource for a user who does not have an SBM account. This is useful for tracking resources who are part of a resource team, but who will not be assigned work items. This might include executives or project stakeholders, for example.

- **Name**

  For resources who are SBM users, search for the user by name or login ID. For other resources, provide a unique name.

- **Description**

  Optionally, provide a description for the resource.

- **Location**

  Optionally, provide a location for the resource.

- **Calendar**

  Select the SBM calendar to use for capacity calculations. If a calendar is not selected, the resource's capacity is calculated as zero. For details, refer to About Working Hours, Capacity, and Scheduling [page 408].

- **Employee ID**

  If the resource is an employee, enter his or her employee ID number.

- **Start Date**

  If the resource is an employee, enter his or her employment start date.

- **End Date**

  If the resource is an employee, enter his or her employment end date.

- **Type**

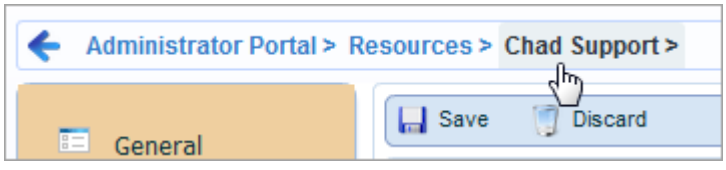
  Select the type of employment that applies. You can add and assign types by clicking the **Add** button. For example, you might define employees as "Full Time" or "Part Time".

- **SBM User Information**

  When you associate a resource associated with an SBM user account, the user's login ID, e-mail address, product-access type are shown here. The **Status** field shows if the SBM has been deleted. Click the user's login ID to view user account details.

Tips for Working with General Resource Settings

- You can only create one resource for each SBM user account.
- SBM calendars are used for several other features, so consider adding a set of calendars specifically for resource calculations. To learn more about calendars, refer to About Calendars [page 390].
- If you click a resource's SBM login ID to view user account details, you can click the user's name in the breadcrumb to return to the **Resources - General** page.



Organization Settings for Resources

Use the **Organization** page to assign a department, business unit, and manager to a resource.

The following settings are available:

- **Department**

  Search for a department for the resource, and then select it from the results list. The list includes selections added on the **Departments** page. For details, refer to The Departments View [page 426].

- **Add and assign a new department**

  Click this button to add a department and assign it to the resource.

- **Business Unit**

  Search for a business unit for the resource, and then select it from the results list. The list includes selections added on the **Business Units** page. For details, refer to The Business Units View [page 425].

- **Add and assign a new business unit**

  Click this button to add a business unit and assign it to the resource.

- **Manager**

  Optionally, search for the resource's manager, and then select it from the results list. All resources are available as managers.

Team Settings for Resources

Use the **Resource Teams** page to perform the following team tasks for an individual resource:

- View and set resource team assignments
- Set shared percentages for each of the resource's team assignments
- Specify start and end dates for each resource team assignment
- Set the resource as a team lead
- Remove a resource from a team
- View resource team details

Changes made for the resource are automatically applied to the resource teams and can be viewed on the **Resource Team - Resources** page. For details, refer to Resource Settings for Teams [page 422].

The following options are available:

- **Manage Resource Teams**

  Click this button to open the **Manage Resource Teams** dialog box and add or remove team assignments for the resource. For details, refer to Team Management for Resources [page 419].

- **Resource Team Details**

  Select a resource team in the list, and then click this button to view and modify settings for the team.

- **Current Resource Teams**

  Select this check box to list only resource teams to which the resource is assigned for the current time frame. Clear this check box to list all resource teams to which the resource is assigned.

- **Search**

  Search for resource teams to which the resource is assigned. Note that the **Current Resource Teams** setting affects search results. If the check box is selected, for example, only resource teams to which the resource is assigned for the current time frame are returned.

- **Resource Team Name**

  Shows the name of each resource team.

- **Shared Percentage**

  Shows the percentage of time the resource is allocated to each resource team for the specified start and end dates. Use the slider bar to set the shared percentage for each resource team. You receive a warning message if a resource is over-allocated.

- **Start Date/End Date**

  Specify the start and end dates that the resource is allocated to each resource team.

- **Team Lead**

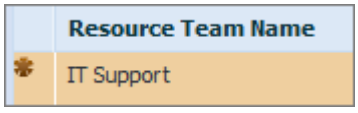
  Select the check box for each team the resource will serve as the lead.

- **Remove**

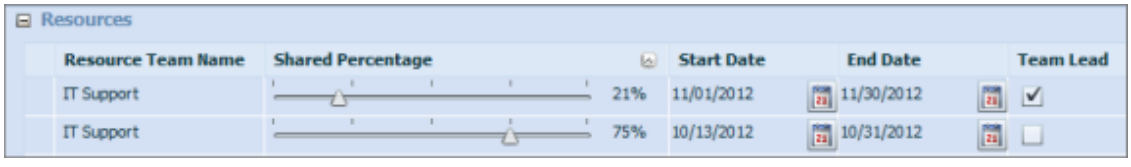
  Click the trash can icon to remove a resource team assignment from the resource.

Tips for Working with Team Settings for Resources

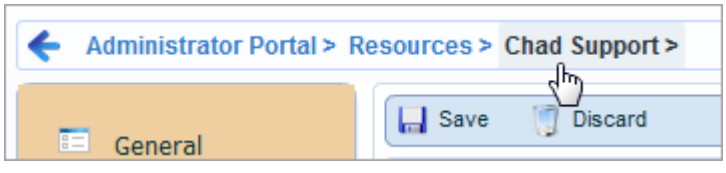
- If you change a setting for a resource's team, an asterisk appears in the far left column. Save your changes to remove the asterisk.



- You can define different shared percentages for multiple time periods for a single resource. To do so, add the multiple references of a team to the resource, and then set different start and end dates and shared percentages. You can also use this feature to set the resource as a team lead for specific time periods.



- If you manage teams for a resource, click the user's name in the breadcrumb to return to the **Resources - Teams** page.



Team Management for Resources

Use the **Manage Resource Teams** dialog box to manage team assignments for an individual resource.

To select team memberships for a resource, navigate to or search for a resource team, and then:

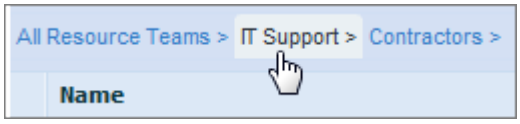
- Use the arrows to move a team to the **Selected Resource Teams** pane.
- Select a team in the list, and then drag it to the **Selected Resource Teams** pane.

Tip: Use the CTRL or SHIFT keys to select and move multiple resource teams.

The following options are available:

- **Available Resource Teams**

  By default, all parent teams in the system are listed along with a description and placement in the team hierarchy. The parent team icon () indicates that a team has child teams, or sub-teams. Expand or collapse the hierarchy, or double-click the icon to view the child teams; use the breadcrumb links to navigate through the team hierarchy.



- **Selected Resource Teams**

  Lists the teams to which the resource is assigned.

- **Arrows**

  Use the arrows to add or remove resource team memberships for the resource.

- **Search**

  Search for resource teams by name.

Job Functions for Resources

Use the **Job Function** page to assign a job function to a resource. The job function is then automatically associated with each resource team to which the resource is assigned.

The following settings are available:

- **Job Function**

  Search for a job function for the resource, and then select it from the results list. The list includes selections added on the **Job Functions** page. For details, refer to The Job Functions View [page 427].

- **Add and assign a new job function**

  Click this button to add a job function and assign it to the resource.

- **Title Group**

  Search for a title group for the resource, and then select it from the results list. The list includes selections added on the **Title Groups** page. For details, refer to The Title Groups View [page 430].

- **Add and assign a new title group**

  Click this button to add a title group and assign it to the resource.

Skill Assignments for Resources

Use the **Skills** page to associate skills with a resource. The skills are then automatically associated with each resource team to which the resource is assigned.

The list of available skills comes from those added on the **Skills** page. You can search for skills by name, sort the columns by name or level, or use the navigation buttons at the bottom of the page to browse the skills list.

To assign existing skills to a resource, select the check box to the right of each applicable skill.

If you cannot find the skills you need to associate with a resource, click the **Add and assign a new skill** button. After you add a new skill, it is automatically assigned to the resource you are adding or editing.

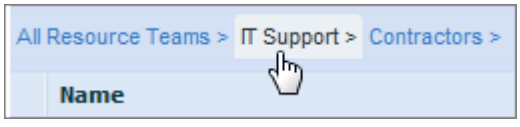
The Resource Teams View

Use the **Resource Teams** view to view, update, and delete resource teams in your system. Click the column headers to sort the list by name. You can also view the hierarchy position for the listed resource teams.

The following options are available:

- **Available Resource Teams**

  By default, all parent teams in the system are listed along with a description and placement in the team hierarchy. The parent team icon ( ) indicates that a team has child teams, or sub-teams. Expand or collapse the hierarchy, or double-click the icon to view the child teams; use the breadcrumb links to navigate through the team hierarchy.

- **Add**

  Click this button to add a resource team. If you need to add more than one or two resource teams, consider importing them. For details, refer to Importing and Exporting Resources [page 410].

- **Details**

  Select a resource team, and then click this button to view or modify it.

- **Delete**

  Select a resource team, and then click this button to delete it. (You must remove a team's resource assignments or child teams before you can delete the resource team.)

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for resource teams by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each resource team:

- Name
- Description
- Hierarchy (parent team is indicated)

General Team Settings

Use the **General** page to define a name, parent resource team, and description for each team. You can also view the team lead, if one has been set for the team.

The following options are available:

- **Name**

  Provide a name for the team. Team names do not need to be unique as long as the teams reside in different levels of the hierarchy. The team name cannot contain a forward slash (/).

- **Parent Resource Team**

  If the team will be the child of a higher-level team, select the parent team from the drop-down list. This is useful for handling organizational hierarchies with your team. For example, the parent team may be a large business unit, and child teams might be departments within that business unit. You can create multiple hierarchical levels for your teams.

- **Description**

  Optionally, provide a description for the team.

- **Team Lead**

  If a team lead has been set on the **Team - Resources** page, it is shown here, but only for the current time period.

Resource Settings for Teams

Use the **Resources** page to perform the following resource tasks for a resource team:

- View and modify resource assignments
- Set shared percentages for each resource
- Specify start and end dates for each resource
- Specify a lead for the resource team
- Remove a resource from a team
- View details for individual resources

Changes made for each resource on a team can be viewed on the **Resource - Teams** page. For details, refer to Team Settings for Resources [page 417].

The following options are available:

- **Manage Resources**

  Click this button to open the **Manage Resources** dialog box and add resources to the team. For details, refer to Resource Management for Teams [page 424].

- **Resource Details**

  Select a resource in the list, and then click this button to view and modify settings for the resource.

To return to the **Resource Teams - Resources** page, click the team name in the breadcrumb.

- **Current Resources**

  Select this check box to list only resources assigned to the team for the current time frame. Clear this check box to list all resources assigned to the team.

- **Search**

  Search by name for a resource in the team. Note that the **Current Resources** setting affects search results. If the check box is selected, for example, only resources assigned to the team for the current time frame are returned.

- **Resource Name**

  Indicates the name of the resource.

- **Shared Percentage**

  Shows the percentage of time each resource is allocated to the team for the specified start and end dates. Use the slider bar to set the shared percentage for each resource. You receive a warning message if resources are over-allocated.

- **Start Date/End Date**

  Specify the start and end dates that each resource is allocated to the resource team.

- **Team Lead**

  Select the check box for the resource who will serve as the lead. You can only have one lead per team for a specific time period.

- **Resource Teams**

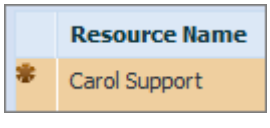
  Indicates the number of teams each resource is assigned to.

- **Remove**

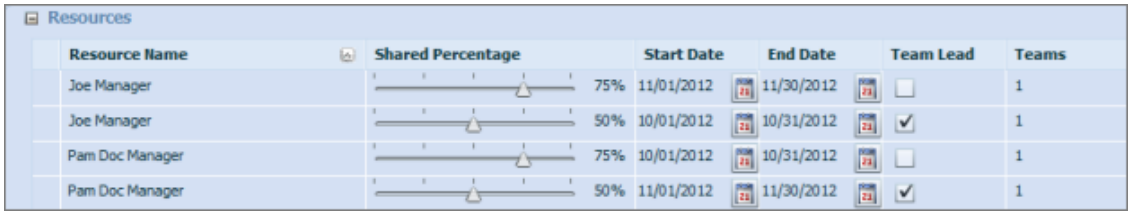
  Click the trash can icon to remove a resource assignment from the team.

Tips for Working with Resource Settings for Teams

- If you change a setting for a team's resource, an asterisk appears in the far left column. Save your changes to remove the asterisk.



- You can define different shared percentages for multiple time periods for a single resource assigned to the team. To do so, add the multiple references of a resource to the team, and then set different start and end dates and shared percentages. You can also use this feature to change the team lead for specific time periods.



Resource Management for Teams

Use the **Manage Resources** dialog box to manage resource assignments for an individual resource team.

To select resources for a team, navigate to or search for a resource, and then:

- Use the arrows to move a resource to the **Selected Resources** pane.
- Select a resource in the list, and then drag it to the **Selected Resources** pane.

Tip: Use the CTRL or SHIFT keys to select multiple resources in the **Available Resources** list.

The following options are available:

- **Available Resources**

  By default, all resources in the system are listed, along with the resource's type, job function, skills, and a description. Click the Name, Type, and Job Function column headers to sort the list as needed.

- **Selected Resources**

  Lists the resources that are assigned to the team.

- **Arrows**

  Use the arrows to add or remove resource assignments for the team.

- **Search**

  Search for resources by name, job function, or skill.

Job Functions by Resource Team

The **Job Functions** page lists an aggregated view of all job functions assigned to the resource team. The totals are calculated based on the job function assigned to each resource in the resource team.

For details, refer to Job Functions for Resources [page 420].

Skills by Resource Team

The **Skills** page lists an aggregated view of all skills assigned to the resource team. The totals are calculated based on the skills assigned to each resource in the resource team.

For details, refer to Skill Assignments for Resources [page 420].

The Business Units View

The **Business Units** view lists the business units that have been added to your system. You can assign a single business unit to each resource.

Click the column headers to sort the list of business units by name or internal name.

The following options are available on the **Business Units** view:

- **Add**

  Click this button to add a business unit.

- **Details**

  Select a business unit, and then click this button to view or modify its details.

- **Delete**
  Select a business unit, and then click this button to delete it.

  Tip: You cannot delete business units that are assigned to resources. You must remove the business unit from each resource first, and then return to the **Business Units** view and delete the business unit.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for a business unit by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each business unit:

- Name
- Internal Name
- Description

General Business Units Settings

Use the **Business Units - General** page to provide basic information about each business unit.

- **Name**

  Provide a name for the business unit, such as Sales or Marketing.

- **Internal Name**

  Provide an internal name for the business unit (for LDAP imports).

- **Description**

Optionally, provide a description of the business unit.

Tip: Use the **Save and Add Another** button to quickly add multiple business units.

Tips for Managing Business Units

- Before you add business units, determine naming and level standards for all business units in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

The Departments View

The **Departments** view lists the departments that have been added to your system. You can assign a single department to each resource.

Click the column headers to sort the list of departments by name or internal name.

The following options are available on the **Departments** view:

- **Add**

  Click this button to add a department.

- **Details**

  Select a department, and then click this button to view or modify its details.

- **Delete**
  Select a department, and then click this button to delete it.

  Tip: You cannot delete departments that are assigned to resources. You must remove the department from each resource first, and then return to the **Departments** view and delete the department.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for a department by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each department:

- Name
- Internal Name
- Description

General Departments Settings

Use the **Departments - General** page to provide basic information about each department.

- **Name**

  Provide a name for the department, such as Software Development or QA.

- **Internal Name**

  Provide an internal name for the department (for LDAP imports).

- **Description**

  Optionally, provide a description of the department.

Tip: Use the **Save and Add Another** button to quickly add multiple departments.

Tips for Managing Departments

- Before you add departments, determine naming and level standards for all departments in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

The Job Functions View

The **Job Functions** view lists the job functions that have been added to your system. You can assign a single job function to each resource, and then that job function is associated with the resource team to which each resource is assigned.

Click the column headers to sort the list of job functions by name or level.

The following options are available on the **Job Functions** view:

- **Add**

  Click this button to add a job function.

- **Details**

  Select a function, then click this button to view or modify its details.

- **Delete**
  Select a job function, and then click this button to delete it.

  Tip: You cannot delete job functions that are assigned to resources. To determine which job functions are assigned, go to the **Resources** view, and then search for the job function. A list of resources who are assigned to the job function is returned. You can remove the job function from each resource, and then return to the **Job Functions** view and delete the job function.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

Search for a job function by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each job function:

- Name
- Level
- Internal Name
- Description

General Job Functions Settings

Use the **Job Functions - General** page to provide basic information about each job function.

- **Name**

  Provide a name for the job function, such as IT Analyst or Tester.

- **Internal Name**

  Provide an internal name for the job function. Used for imports from LDAP.

- **Description**

  Optionally, provide a description of the job function.

- **Level**

  Select or add a level of experience that is applicable to the job function in your organization. For example, you may have various levels for IT analysts, such as junior and senior.

Tip: Use the **Save and Add Another** button to quickly add multiple job functions.

Tips for Managing Job Functions

- Before you add job functions, determine naming and level standards for all positions in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

The Skills View

The **Skills** view lists the skills that have been added to your system. You can assign multiple skills to each resource, and these skills are then associated with the resource team to which each resource is assigned.

Click the column headers to sort the list of skills by name or level.

The following options are available on the **Skills** view:

- **Add**

  Click this button to add a skill.

- **Details**

  Select a skill, and then click this button to view or modify its details.

- **Delete**
  Select a skill, and then click this button to delete it.

  Tip: You cannot delete skills that are assigned to resources. To determine which skills are assigned, go to the **Resources** view, and then search for the skill. A list of resources who are assigned to the skill is returned. You can remove the skill from each resource, and then return to the **Skills** view and delete the skill.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for a skill by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each skill:

- Name
- Level
- Description

General Skills Settings

Use the **Skills - General** page to provide basic information about each skill.

- **Name**

  Provide a name for the skill, such as C++ or Perl.

- **Description**

  Optionally, provide a description of the skill.

- **Level**

  Select or add a level of experience that is applicable to the skill in your organization. For example, you may have various skill levels for C++ programmers, such 1 for junior programmers and 5 for advanced programmers.

Tip: Use the **Save and Add Another** button to quickly add multiple skills.

Tips for Managing Skills

- Before you add skills, determine naming and level standards for all skills in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

The Title Groups View

The **Title Groups** view lists the title groups that have been added to your system. You can assign a single title group to each resource.

Click the column headers to sort the list of title groups by name or internal name.

The following options are available on the **Title Groups** view:

- **Add**

  Click this button to add a title group.

- **Details**

  Select a title group, and then click this button to view or modify its details.

- **Delete**
  Select a title group, and then click this button to delete it.

  Tip: You cannot delete title groups that are assigned to resources. You must remove the title group from each resource first, and then return to the **Title Groups** view and delete the title group.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for a title group by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each title group:

- Name
- Internal Name
- Description

General Title Groups Settings

Use the **Title Groups - General** page to provide basic information about each title group.

- **Name**

  Provide a name for the title group, such as "Front Line Managers" or "Executives".

- **Internal Name**

  Provide an internal name for the title group (for LDAP imports).

- **Description**

  Optionally, provide a description of the title group.

Tip: Use the **Save and Add Another** button to quickly add multiple title groups.

Tips for Managing Title Groups

- Before you add title groups, determine naming and level standards for all title groups in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

The Types View

The **Types** view lists the types that have been added to your system. You can assign a single type to each resource.

Click the column headers to sort the list of types by name or internal name.

The following options are available on the **Types** view:

- **Add**

  Click this button to add a type.

- **Details**

  Select a type, and then click this button to view or modify its details.

- **Delete**
  Select a type, and then click this button to delete it.

  Tip: You cannot delete types that are assigned to resources. You must remove the type from each resource first, and then return to the **Types** view and delete the type.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Search**

  Search for a type by name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

The following information is listed for each type:

- Name
- Internal Name

- Description

General Types Settings

Use the **Types - General** page to provide basic information about each type.

- **Name**

  Provide a name for the type, such as "Full Time" or "Part Time".

- **Internal Name**

  Provide an internal name for the type (for LDAP imports).

- **Description**

  Optionally, provide a description of the type.

Tip: Use the **Save and Add Another** button to quickly add multiple types.

Tips for Managing Types

- Before you add types, determine naming and level standards for all types in your organization. This will help prevent duplicate entries and ensure consistency across resource management and planning activities.

Export Resources Page

Use the **Export** page to export existing resources and resource teams to a spreadsheet.

If you have not yet imported resources, you can also use this page to create empty spreadsheets that are compatible with the **Import Resources** feature. For details on preparing the spreadsheet for importing resources and resource teams, refer to Importing and Exporting Resources [page 410].

To export resources:

1. Select one or more of the following entities:
   - Resources
   - Resource Teams
2. Click **Export**.
3. Select a location for the spreadsheet, and then click **Save**.

Import Resources Page

Use this page to select a spreadsheet that contains resource teams and resources to import. Click **Import** to start the import process.

Important: Be sure to carefully read the information about spreadsheet requirements in Importing and Exporting Resources [page 410] before you perform an import.

Import Log

Use the import log to view:

- **Import Errors**

  An import will fail if the spreadsheet is formatted improperly or contains invalid row data. Use the log to view these errors. You can then modify the spreadsheet to provide valid data, and run the import process again.

- **Import Successes**

  If the import process succeeds, the log lists the imported resource teams and resources, as well as those that were skipped. Information about skipped rows is added to the log.

You can filter the log to show:

- **All**

  Select to list all warnings and errors.

- **Warnings**

  Select to list only rows that were skipped during a successful import.

- **Errors**

  Select to show only errors that caused the import to fail.

The log is only available for the most current import process. To retain logging information, you can copy the log to your clipboard and then paste it into a separate document.

For guidelines on spreadsheet and data requirements, refer to Spreadsheet Requirements [page 411].

Chapter 11: E-mail Setup

Use e-mail setup features to:

- Manage mailboxes used for e-mail submission. For details, refer to Mailboxes and E-mail Submission [page 435] and Mailbox Settings [page 439]
- Customize templates used for various e-mail messages sent by SBM. For details, refer to E-mail Template Tags [page 444].

Mailboxes and E-mail Submission

SBM enables e-mail messages sent to a specific address to be submitted as primary items. The Mail Client, which is configured in the SBM Configurator in on-premise systems, processes e-mail submissions.

There are three types of e-mail submission:

- **E-mail Submission by Users**

  Users with valid SBM accounts can submit primary items by e-mail as long as their account contains at least one e-mail address. For details, refer to Preparing Your System for E-mail Submission [page 435].

- **XML E-mail Submission**

  You can automate item submission from external tools by sending properly formatted XML in e-mail messages to a specified e-mail address. For details, refer to Preparing Your System for E-mail Submission [page 435] and Using XML E-mail Submission [page 438].

  Note: Support for development efforts for writing or modifying XML is provided by Professional Services. Questions regarding XML operations as documented will be handled by Serena Customer Support.

- **Cross-database Posting**
  Uses the Mail Client, Notification Server, and external post transitions to submit items into external databases. For details, refer to the *SBM System Administrator Guide*.

  Note: In general, orchestrations are the preferred method for automating submission of items. For guidance on using orchestrations, refer to *SBM Orchestration Guide*.

For details, refer to Preparing Your System for E-mail Submission [page 435].

Preparing Your System for E-mail Submission

Several steps must be taken to prepare your system to accept e-mail submission of primary items:

1. Configure the Mail Client in SBM Configurator (on-premise customers). For details, refer to the *SBM Installation and Configuration Guide*.

The Mail Client is pre-configured for on-demand customers.

2. Create dedicated mail accounts for e-mail submissions. For details, refer to Creating Dedicated Mail Accounts [page 436].
3. Prepare the workflow in SBM Composer. For details, refer to Preparing Workflows [page 436].
4. Prepare projects in SBM Application Administrator. For details, refer to Preparing Projects [page 0].
5. Create a mailbox for each project that will accept e-mail submissions. For details, refer to Creating Mailboxes [page 437].
6. Prepare user accounts in SBM. For details, refer to Preparing User Accounts [page 437].

Creating Dedicated Mail Accounts

For each project that will accept e-mail submissions, you or a network administrator must dedicate a mail account that uses a mail protocol supported by SBM. For example, you might use ITRequests@yourcompany.com to handle IT requests submitted by e-mail.

You can create multiple mailboxes for each project, as long as the mailbox name is unique.

For on-premise customers, the mail account must adhere to the protocol set for the Mail Client in SBM Configurator.

For on-demand customers, a POP3 mail account must be used.

The administrator who configures e-mail submission in SBM Application Administrator must know the mailbox name and password for these mailboxes; users who will submit through e-mail must only know the e-mail address for applicable mailboxes.

Preparing Workflows

Each project that allows e-mail submission must contain a transition that originates in the E-mail state. This transition is defined in SBM Composer and inherited by projects assigned to the workflow in SBM Application Administrator.

Consider the following best practices when you prepare workflows for e-mail submission:

- Only one transition coming from the E-mail state to another state is allowed per project. This single transition can be used to submit items by users, XML email submission, and cross-database posting.
- For best results, provide default values for required fields in the E-mail submit transition to avoid unexpected failures.
- Consider creating an "E-mail Submit" item type to make e-mail submissions easier to identify in the SBM. Item types are defined in SBM Composer.
- Included attachments are added to the newly created item in SBM; however, they are added asynchronously. This means that the item is created first, and then the attachments are added afterwards. If you have a script that parses the attachment, it might not succeed if the attachments are not added to the item yet. To work around this problem, consider using an escalation notification to execute the script a

few minutes after the item is created. This should allow the system enough time to add the attachments to the item.

Follow these steps in SBM Application Administrator to prepare your projects for e-mail submission:

1. Verify that the **Allow new items to be submitted** option is set on the project's **General** page.
2. Verify that the project contains an enabled transition that originates in the E-mail state.
3. Review required fields for the E-mail transition and either remove the requirement or set default values for these fields.

Creating Mailboxes

Each project that accepts e-mail submissions must have its own mailbox. You can create mailboxes while you are editing a project or from the global **Mailboxes** page.

To create a mailbox:

1. Do one of the following:
   - From the **Administrator portal**, select the **Mailboxes** icon.
   - Edit a project, select the **Mailboxes** tab.
2. Click **Add**.
3. Configure the mailbox, using the information in Mailbox Configuration Settings [page 440] for guidance.
4. For user e-mail submissions, map e-mail fields to project fields. Refer to Mailbox Field Mapping [page 441].
5. Prepare confirmation and success e-mail templates. Refer to Working with E-mail Submission Templates [page 438]

   Note: Templates used by e-mail submission are stored in the SBM database and must be modified in SBM Application Administrator.

Preparing User Accounts

Users must have valid SBM accounts and:

- Be granted the "Submit New Items" privilege for each project they will submit items into through e-mail.
- Add the e-mail address from which they will submit items to the **E-mail Address** box of their SBM account profile.

  Note: Users can submit items into the system from more than one account. Multiple accounts should be separated by a semicolon.

- If you are using an automated process to submit items through e-mail, including XML email submission, a user account with an e-mail address that matches the

"From" address in the e-mail message must exist in the database. This account must also be granted the "Submit New Items" privilege for the specific project.

Note: For best results, specify an English locale in the user preferences for the SBM user account used for XML e-mail submissions. If not, data may not be parsed as expected. For example, numeric values may be parsed incorrectly for locales that use characters other than a period as a decimal point.

Working with E-mail Submission Templates

You can create and modify templates for e-mail submission confirmations and error messages. You can create text or HTML templates; a WYSIWYG editor is available for formatting HTML templates and quickly adding template tags to text and HTML templates.

Two templates are provided for confirming successful or failed e-mail submission of items.

- Confirmation of successful e-mail submission (EmailSubmitSuccess.txt)
- Notification of failed e-mail submission (EmailSubmitFailure.txt)

You can manage templates from the global Templates view (Global Mailbox View [page 439]) or for a specific project. If you create a global template, you must assign the template to mailboxes for specific projects.

To add or edit e-mail templates for a specific project:

1. From the **Administrator Portal**, select **Projects**.
2. Edit a project for which e-mail submission is enabled.
3. Select the **Mailboxes** tab.
4. Add or edit the mailbox used for e-mail submission for the project.
5. Select the **Use Confirmation Template** or **Use Error Template** check box.
6. Select an existing template from the list and click the pencil icon to edit it, or click the plus sign to add a template. The E-mail Template Editor opens.
7. For new templates, provide a name for new template in the **Template Name** box.
8. Enter text, e-mail template tags, and HTML formatting (if applicable) into the editor, or click **Editor** to open a WYSIWYG editor.

   Tip: Click the **Template Tag** icon () to insert SBM-specific tags into the template. Click the **Fields** icon () to insert fields into the template. The field's values will be returned in the e-mail notification.
9. Save your changes.

Using XML E-mail Submission

E-mail messages, templates, and forms used for XML submission must adhere to the specifications published in the ttemail.xsd XML schema file. On-premise customers can find this file in the *xmlschemas* folder of your SBM Application Engine installation directory. On-demand customers should contact Customer Support for this file.

Data from the following field types are parsed to SBM fields when submitted through XML e-mail submission:

- Date/Time
- Numeric
- Single-Selection
- Text
- User (maps to user's unique database id or login ID, not to user name)

Data from field types other than those listed is added to the submitted item as a note. This includes invalid field selections. Only one note is created, however, so data from multiple fields and selections that cannot be mapped is added to a single note. In addition, you must use database names rather than logical names for tables and fields included in the XML.

CAUTION:

Some e-mail clients may add line breaks or spaces to text in *Text* fields. When added to SBM items, these line breaks or spaces may affect the formatting of the field on forms.

Examples for formatting XML for use with e-mail submission are available at http://www.serena.com/support.

Mailbox Settings

Mailboxes are assigned to projects. Each project can have multiple mailboxes that submit items, but each mailbox must be unique and can only be used for a single project. For example, customer@company.com and employee@company.com can both be used to submit items into a project by e-mail, but these addresses can only be assigned to a single project. For details, refer to Mailboxes and E-mail Submission [page 435].

You can manage mailboxes at the project level or globally.

- Global Mailbox View [page 439]
- Mailbox Configuration Settings [page 440]
- Mailbox Field Mapping [page 441]

Global Mailbox View

Use the global **Mailboxes** page to view and manage mailboxes for all projects in your system. For details on mailboxes, refer to Mailboxes and E-mail Submission [page 435].

Administrators can view and manage mailboxes for projects they have privileges to administer. Click the column headers to sort the list by mailbox login name, mailbox e-mail address, project name, or application name.

The following options are available on the **Mailboxes** page:

- **Add**

  Click this button to add a mailbox.

- **Details**

  Select a mailbox in the list, and then click this button to edit it. If the **Details** button is disabled for a selected mailbox, you do not have privileges to modify the project or its mailbox.

- **Delete**

  Select a mailbox in the list, and then click this button to delete it. If the **Delete** button is disabled for a selected mailbox, you do not have privileges to modify the project or delete its mailbox.

- **Refresh**

  Click to refresh the page to its last saved state or to update the page after a deployment or promotion.

- **Show Only Mailboxes You Can Edit**

  By default, all mailboxes you have privileges to manage are listed. Clear this check box to display all mailboxes in the system.

- **Search**

  Search for mailboxes by login name.

- **Items Per Page**

  Use **Items Per Page** to set the number of items to display on the page. You can use one of the provided amounts or specify your own number under 1,000 items. Use the navigation arrows to move through multiple pages.

Mailbox Configuration Settings

Use **Mailbox** settings to configure mailboxes used for e-mail submissions and cross-database posting.

The following options are available on the **Mailbox Settings** page for projects that are enabled to allow submissions:

- **Account Settings**
  - **Mailbox E-mail Address**

    Type the full e-mail address of the account.

  - **Login Name**

    Enter the login or user name of the mailbox account that will be used for e-mail submission.

  - **Mailbox Password**

    Type the password for the e-mail address, and then verify it. Users submitting items do not need to know this password.

- **Submission Options**
  - **Allow External Postings**

    Select this check box to allow submissions from external SBM databases. *(On-premise only.)*

- **Allow External Post Updates**

  Select this check box to allow updates from external SBM databases to be submitted through this mailbox. This check box must be selected if items in the current system will be posted to an external SBM database. *(On-premise only.)*

- **Response Options**
  - **Project for Submission**

    If you are adding or editing a mailbox for a specific project, the project name is indicated here.

    If you are adding or editing a mailbox from the global **Mailbox** page, navigate to the project you want to use for this mailbox.

  - **Use confirmation template**

    Select this check box to send users a confirmation e-mail message for successful submissions, and then select an e-mail template from the list.

  - **Use error template**

    Select this check box to send users an e-mail message for failed submissions, and then select an e-mail template from the list.

    Note: You can also choose to edit the existing template or add a new one. For details, refer to Working with E-mail Submission Templates [page 438].

  - **Template Reply Address**

    Type an e-mail address that should appear in the **From** address field for confirmations and error messages. User replies to confirmations and error messages will be sent to this address.

- **Mail Mappings**

  Once a project is selected for a mailbox, you can map fields in incoming messages to fields in the project. For details, refer to Mailbox Field Mapping [page 441].

Mailbox Field Mapping

Use the **Mailbox Mapping** page to map fields in the incoming e-mail message to fields in your project.

Note: The settings on this page apply only to user e-mail submissions. For information regarding XML e-mail submissions, refer to Using XML E-mail Submission [page 438].

The following options are available on the **Mailbox Mapping** page:

- **Mapping From**

  Lists header fields from the e-mail message. Drag compatible fields in this list to the **Mail Header Name** column in the **Mapping To (Project)** list.

- **Mapping To (Project)**

  Lists the fields available for mapping. Double-click a field in the list to remove the mapping.

Tip: For best results, verify that no fields in e-mail submit transition are set as required. Required fields must be mapped or e-mail submissions will fail. Auto fields, such as *Submit Date*, do not need to be mapped because these fields are automatically populated by the system.

E-mail Templates

Use the Templates view to customize e-mail templates for the features shown in the following table.

Template Type	Use	Context
E-mail submission replies	Confirmation and failure messages	Project
Notification	E-mails sent to users	Workflow
Scheduled reports	Deliver scheduled reports	Global
Registrations and password changes	External user registration confirmation messages and password change requests	Global (on-premise only)
User e-mail	Messages sent by users from primary and auxiliary items	Global
View sharing alerts	Messages sent to users when a Work Center view is shared with them or when the view is no longer shared with them	Global

Default templates for each of these features are shown on the Templates view. To open this view from the **Administrator portal**, select **E-mails**, and then select **Templates**.

You can then use this page to add new templates and modify or delete existing templates.

You can also search for templates and you can filter the list by template type.

For details on using the e-mail template editor, refer to About the E-mail Template Editor [page 443].

For a list of tags applicable to each template type, refer to E-mail Template Tags [page 444].

About the E-mail Template Editor

The **E-mail Template Editor** provides a simple way to customize the body portion of templates used various features.

HTML and text formats are supported for all types of e-mail templates.

Tip: If users will format text added to fields and e-mail messages they send to other users, use HTML formats for notifications and user e-mail templates. This prevents formatting tags from appearing in the messages sent by the Notification Server.

The following options are available:

- **Name**

  Shows the template file name . When you add templates, you must include an .html or .txt extension.

- **Type**

  Indicates the template type. This cannot be changed after a template has been saved.

- **Usage Options**
  May be available depending on the type of template you are editing.
  - **Self registration options**

    Choose to use the template for external user registration confirmations, external user password requests, user password requests, or LDAP user import notices.

  - **User e-mails**

    Set the current template as the default for e-mail messages sent by users. Only one template can be specified for this feature.

  - **View sharing**

    Set the current template as the default for e-mail messages sent to users when a view is shared with them or when they are removed from a shared view. You can only select one template for each.

- **Locale**

  Select a specific locale for the template. The default locale is en_US.

- **Format Text**

  You can edit the template tags and text in the main pane, or you can click **Format Text** to open a Rich Text Editor.

- **Formatting Options**
  Standard formatting options are available, along with these specific e-mail template options:
  - **Template Tags**

Click this icon ( ) to insert template tags into the editor. For details on specific template tags, refer to E-mail Template Tags [page 444].

- Click this icon ( ) to insert fields into the editor. At runtime, these fields are replaced with appropriate values.

  Note: The fields icon is not available in the global Templates view. If you are working with a mail client or notification template and want to see the list of available fields, modify notification templates from the **Notifications** view or mail client templates from the **Projects** view.

E-mail Template Tags

The following sections discuss the template tags available to you. Tags are organized by type.

Template Type	Supported Tags
Notifications	Notification Base item Base global
E-mail submission replies	E-mail submission replies Base item Base global
Scheduled reports	Scheduled reports
Registration and password changes (On-premise only)	E-mail submission replies Base global
User E-mails	Base item Base global
View sharing alerts	View sharing alerts Base global

- Notification Tags [page 445]
- E-mail Submission Template Tags [page 459]
- Scheduled Report Template Tags [page 462]
- User Registration and Password Template Tags [page 466]

- View Sharing Template Tags [page 467]
- Base Item Template Tags [page 468]
- Base Global Template Tags [page 471]

Notification Tags

Notification tags can only be used in Notification e-mail templates.

Note: All notification tags can be used in Notification e-mail templates for Service Level Agreements (SLAs); however, dynamic SLA-specific information cannot be returned.

Several Notification template tags are conditional tags. The condition for each of these tags is placed between parentheses after the `$IF` statement. The conditional tags can be used with `$ELSE()` and `$ENDIF()` tags to tailor the content of the e-mail message depending on whether the condition is true or false.

$ATTACHMENT()

- **Description**

  Adds all files attached to an item to the e-mail notification.

- **Usage**

  Attachments must be stored in the SBM database and not on the file system. (This setting is applied in SBM System Administrator.)

  Files are not attached to messages if their combined size exceeds the limit specified in SBM Configurator.

  Attachments are only included with a notification if users have privileges to view those attachments in the associated item.

  Note: Use the `$FILEATTACHMENTLINKS()` tag to include links to attachments in the notification rather than actual files.

- **Parameters**

  None.

$ALLRECIPIENTS()

- **Description**

  Adds a comma-separated list of subscribers to the e-mail notification.

- **Usage**

Use this tag to include a list of all the current users that are subscribed to the notification.

Note: To avoid sending a potential large list of subscribers, perform the following steps on the SBM server that hosts the Notification Server:

1. Edit the `config.properties` file located here:

```
installationDirectory\Serena\SBM\Common\jboss405\server\default\deploy\
→notificationsrv.war\WEB-INF\classes
```

2. Search for the `event.allrecipients.maxsize` setting.
3. Enter the maximum number of subscribers that should appear. For example, to display only three subscribers, change the setting as follows:

```
event.allrecipients.maxsize=3
```

In this example, the list in the notification shows the first three subscribers, followed by ellipses:

```
Hans Tester (hans@serena.com), Chad Support (chad@serena.com),
Administrator (admin@serena.com),...
```

4. Save your changes. The new maximum size will take effect after the next JBoss restart.

- **Parameters**

  None.

- **Sample**

  ```
  $ALLRECIPIENTS()
  ```

  Result:

  ```
  Hans Tester (hans@serena.com), Chad Support (chad@serena.com),
  Administrator (admin@serena.com), Bill Admin (bill@serena.com)
  ```

$CHANGEACTION()

- **Descripton**

  Returns the action and user that caused the notification to be generated, along with the date and time the action occurred.

- **Usage**

  Change action examples include state changes, item updates, and attachment additions. Date and time action occurred is also returned.

  Change actions are only sent to users who have privileges to view the change history for the item on which the notification is based. For delayed escalations, changes may not be available.

- **Parameters**

  None.

- **Sample**

```
$BEGINSUBJECT()$NOTIFICATION() - $ITEMNUMBER()$CHANGEACTION()$ENDSUBJECT()
```

  Result:

  subject **Attachment Is Added - ENH000202 2011-10-26 08:18:57: Attachment/Note added by Administrator**

$CHANGES()

- **Description**

  Returns the change history entries for an item.

- **Usage**

  Change history records are only sent to users who have privileges to view the change history for the item on which the notification is based. For delayed escalations, changes may not be available.

- **Parameters**

  Insert the number of change history entries to return between the parentheses. If you do not specify a number in the parameter, all transitions and changed data are returned.

- **Sample**

```
$CHANGES()
```

  Result for HTML template:

Showing last 3 change action(s) of 7

Pass Review by Administrator - 11/16/2012 11:07:24 AM

Field Name	Prior Value	New value
Status Log:		
Tester:	(None)	Chris Tester
Percentage Complete:		100
P4Status:	open	closed
State:	Peer Review	Testing Issue
Last Modified Date:	11/16/2012 10:22:17 AM	11/16/2012 11:07:24 AM
Last State Change Date:	11/16/2012 10:22:17 AM	11/16/2012 11:07:24 AM

Delegate by Administrator - 11/16/2012 11:10:35 AM

Field Name	Prior Value	New value
Tester:	Chris Tester	Melanie Prod Manager
Owner:	Chris Tester	Melanie Prod Manager
Last Modified Date:	11/16/2012 11:07:24 AM	11/16/2012 11:10:35 AM

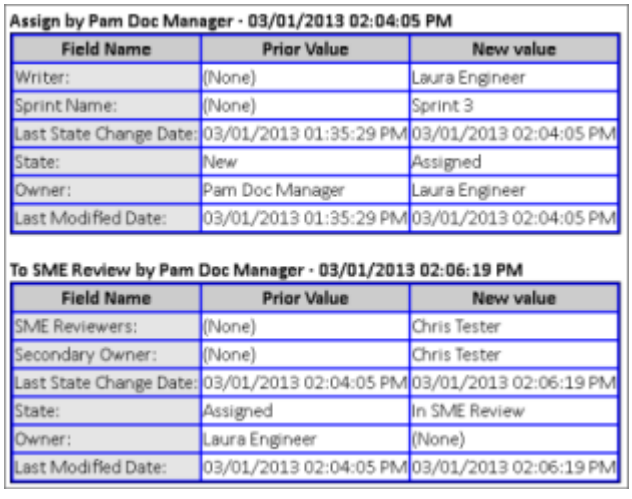
Pass by Administrator - 11/16/2012 11:13:22 AM

Field Name	Prior Value	New value
State:	Testing Issue	Resolved
Owner:	Melanie Prod Manager	(None)
Active/Inactive:	Active	Inactive
Last Modified Date:	11/16/2012 11:10:35 AM	11/16/2012 11:13:22 AM
Close Date:		11/16/2012 11:13:22 AM
Last State Change Date:	11/16/2012 11:07:24 AM	11/16/2012 11:13:22 AM

You can optionally apply a cascading style sheet (CSS) to the $CHANGES() tag. For best results, place the CSS tags before the $CHANGES() tag, and place the $CHANGES() tag at the bottom of the template. For example:

```
<style media="screen" type="text/css">
table.serena_ns_changes_table {border: thin solid black;background-color:#0000ff;}
tr.serena_ns_changes_tr {background-color:#ff0000;}
td.serena_ns_changes_td_field {background-color:#777777;}
td.serena_ns_changes_td {background-color:#ffffff;}
</style>
$CHANGES()
</body>
</html>
```

Result:



Assign by Pam Doc Manager - 03/01/2013 02:04:05 PM

Field Name	Prior Value	New value
Writer:	(None)	Laura Engineer
Sprint Name:	(None)	Sprint 3
Last State Change Date:	03/01/2013 01:35:29 PM	03/01/2013 02:04:05 PM
State:	New	Assigned
Owner:	Pam Doc Manager	Laura Engineer
Last Modified Date:	03/01/2013 01:35:29 PM	03/01/2013 02:04:05 PM

To SME Review by Pam Doc Manager - 03/01/2013 02:06:19 PM

Field Name	Prior Value	New value
SME Reviewers:	(None)	Chris Tester
Secondary Owner:	(None)	Chris Tester
Last State Change Date:	03/01/2013 02:04:05 PM	03/01/2013 02:06:19 PM
State:	Assigned	In SME Review
Owner:	Laura Engineer	(None)
Last Modified Date:	03/01/2013 02:04:05 PM	03/01/2013 02:06:19 PM

$EMAILRESPONSE()

- **Description**

  Returns links that correspond to notification responses, as discussed in E-mail Responses [page 298].

- **Usage**

  Add a tag for each response you have configured for a given notification, using an `href` attribute. Each response tag that you add will appear in the notification message.

- **Parameters**
  For HTML e-mail templates, insert the name of the response, followed by `external` or `internal`. These values correspond to the Web server links that you configure for the Notification Server in SBM Configurator.

  Important: You must enter the same response name that you specified in the **E-mail Responses** tab. For example, if you entered **`Approve`** as an alias for the "Manager Approval" transition, you must enter **`Approve`** in the `$EMAILRESPONSE()` parameter. See the example below.

- **Sample**

```
$BEGINSUBJECT()$NOTIFICATION() - $ITEMNUMBER() $TTID()$ENDSUBJECT()
<meta http-equiv="Content-Type" content="text/html; charset=$GETSETTINGSSTR(CharSet,UTF-8)">
```

```
<title>$NOTIFICATION() - $ITEMNUMBER() $TTID()</title>
<style type="text/css">
a.attachlink:link { color: #0000FF }
a.attachlink:visited { color: #0000FF }
a.attachlink:hover { color: #006600 }
</style>
$IF(AUXTABLE)$ELSE()$ENDIF()
<table>
<tbody>
<tr>
<td><b>$STRING(IDS_EMAIL_DISPLAYVALUE):</b></td>
<td>$ITEMNUMBER()</td>
</tr>
<tr>
<td><b>$SYSFIELDNAME(TS_SYSFLD_TEXT_DISPLAYID):</b></td>
<td>$ITEMNUMBER()</td>
</tr>
<tr>
<td><b>$SYSFIELDNAME(TS_SYSFLD_TITLE):</b></td>
<td>$TITLE()</td></tr>
</tbody>
</table>
<br>Dear $RECIPIENT(),<br><br><p align="left"> This ticket requires your approval.</p>
<p align="left"> To approve, click <a href="$EMAILRESPONSE(Approve, external)"
style="background: #11356D; color: white; display: inline-block; width: auto;
text-align: center;text-decoration:none;border:10px solid #11356D;">Approve</a></p>
<p align="left"> To reject, click <a href="$EMAILRESPONSE(Reject, external)"
style="background: #11356D; color: white; display: inline-block; width: auto;
text-align: center;text-decoration:none;border:10px solid #11356D;">Reject</a></p>
<br>$IF(CANVIEW)$IF(VIEWLINK)
<b>$STRING(IDS_EMAIL_TOVIEW) $ITEMTYPENAME():</b> $LINK( TRUE )$ENDIF()$ENDIF()<br>
<br>$IF(CANVIEW)$FIELDS()$ENDIF()<br>
<br>$FILEATTACHMENTLINKS()
```

In this example, the response names `Approve` and `Reject` are used as aliases for their respective transitions. The second parameter (`external` or `internal`) configures the link for access outside or inside the firewall.

Result:

$FIELDS()

- **Description**

  Returns fields selected on the **Fields** page for each notification, as discussed in E-mail Field Settings [page 297].

- **Usage**

  Asterisks replace field values for users who do not have permission to view fields included in the notification. Fields in the *Not Used* fields section are not included in the e-mail notification.

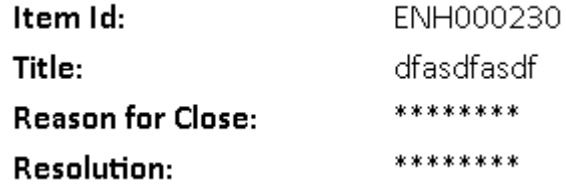
- **Parameters**

  For HTML e-mail templates, insert the number of display columns between the parentheses. If you do not specify the parameter, the default number of display columns is 2. This parameter is ignored for text-formatted e-mail messages.

- **Sample**

```
$IF(CANVIEW)
$FIELDS()
$ENDIF()
```

  Result for user who cannot view specific fields:



$FILEATTACHMENTLINKS()

- **Description**

Adds links to files attached to items associated with the e-mail notification.

- **Usage**

  Links to file attachments appear in the notification only if users have permissions to view those attachments in the associated item. Tag can be included in text-based messages, but links are not clickable.

- **Parameters**

  - `external` - Optional. Add link to attachments in an external instance of SBM.

- **Sample**

```
$FILEATTACHMENTLINKS()
```

  Result:

  File Attachment(s):
  error.png

$IF() Tags

Use with the following parameters and the `$ELSE()` and `$ENDIF()` conditional tags.

Note: All line breaks and spaces are left in the message during template processing. For statements to display as one line in the e-mail message, the conditional statement must not include any line breaks.

- **$IF(auxtable) and $IF(pritable)**

  - **Description**

    Use to specify which information should appear in the e-mail message if the notification is associated with a primary table or auxiliary table.

  - **Sample**

```
$IF(AUXTABLE)(IDS_EMAIL_DISPLAYVALUE):$ITEMNUMBER()
$ELSE()
$SYSFIELDNAME(TS_SYSFLD_TEXT_DISPLAYID):$ITEMNUMBER()
$SYSFIELDNAME(TS_SYSFLD_TITLE):$TITLE()
$ENDIF()
```

    Result (for primary items):

    Item Id: UPLA000147
    Title: Color Palette needs to be more intuitive

    Result (for auxiliary items with Item ID field included in table):

    Display Value: 000231

- **$IF(CANVIEW, fieldname)**

- **Description**

  Use to determine if the subscriber has privileges to view a specific field.

- **Usage**

  Fields specified in this tag must be selected on the **Fields** page for each notification, as discussed in E-mail Field Settings [page 297].

  Use with the `$FIELDVALUE(fieldname)` tag to show the field's current value in the e-mail message.

- **Parameters**

  - `fieldname`

    Returns the logical field name.

- **Sample**

```
Item is assigned to
      $IF(CANVIEW,Doc Lead)
      $FIELDVALUE(Doc Lead)
      $ELSE()
      a Manager
      $ENDIF()
```

  Result for users who can view *Doc Lead* field:

  Item is assigned to Pam Doc Manager

  Results for users who cannot view *Doc Lead* field:

  Item is assigned to a Manager

- **$IF(ITEMTYPE)**
  - **Description**

    Returns information based on the application to which the notification is related.

  - **Usage**

    Parameters are based on table settings, which are available on the **General** tab of the Table property editor in SBM Composer.

  - **Parameters**
    - singular item name
    - application prefix
  - **Sample**

```
$IF(ITEMTYPE, Change Requests)
Send this information about Change Requests
$ELSE()
```

```
Send this information about all other item types
$ENDIF()
```

- **$IF(VIEWLINK)**
  - **Description**

    Returns a link to the item related to the notification to users who have the **Include a Link to the Item** check box selected in their user profile.

  - **Usage**

    Must be used with `$LINK` tag, as shown in the following sample.

    When the `$LINK` tag is included in the template without the `$IF(VIEWLINK)` tag, users who do not have the **Include a Link to the Item** check box selected receive a message stating that the item was created, but they must select the check box in their user profile to receive links to items.

  - **Sample**

    ```
    $IF(VIEWLINK)
     $LINK( TRUE )
     $ENDIF)
    ```

    Result with `$IF(VIEWLINK)` tag:

    http:/yourserver/tmtrack/tmtrack.dll?View&I=43&T=1006

    Result without `$IF(VIEWLINK)` tag:

    The item was created. However, if you would like to link back to this item you will need to go to your User Profile Page and select 'Include a link to the item'.

$ITEMNUMBER()

- **Description**

  Returns the system-generated ID number.

- **Usage**

  For primary items, returns the prefix, if any, and ID number of the item associated with the e-mail notification. For auxiliary items, returns the ID number if the auxiliary table contains the system *Item ID* field. If it does not, the table's display name is returned.

- **Parameters**

  None.

- **Sample (Subject Line)**

  ```
  $BEGINSUBJECT()$NOTIFICATION() - $ITEMNUMBER() $ENDSUBJECT()
  ```

Result:

```
000204 was created. You may connect to this item at
http://YOURSERVER/tmtrack/tmtrack.dll?View&I=11&T=1006

http:///tmtrack/tmtrack.dll?View&I=11&T=1006
```

$ITEMTYPENAME()

- **Description**

  Returns the singular item name for the primary or auxiliary table.

- **Usage**

  The singular item name is specified in SBM Composer and can be viewed in the **General** tab of the Edit Table property editor for the applicable table.

- **Parameters**

  None.

- **Sample**

```
$STRING(IDS_EMAIL_TOVIEW) $ITEMTYPENAME(): $LINK( TRUE )
```

  Result:

  To View Change Request: http:/yourserver/tmtrack/tmtrack.dll?View&I=22&T=1003

$MAILHEADERPARAM()

- **Description**

  Returns custom header information.

- **Usage**

  Use to add information to the e-mail header. For example, you can return sender information in the header.

  For best results, use both the header name and header value parameters, as shown in the sample below.

- **Parameters**
  - **MSG_**

    Use to indicate message headers.

  - **BDY_**

    Use to indicate body headers.

  - **Header Name**

    Use to label header data.

  - **Header Value**

Use to provide header data.

- **Sample**

```
$MAILHEADERPARAM(MSG_SENDER,admin@serena.com)


$MAILHEADERPARAM(BDY_SENDER,admin@serena.com)
```

- **Result**

```
Message-ID: <24102312.30.1323109940609.JavaMail.SERVER$@SERVER>
Subject: D - Any DOC is submitted - DEF000201
MIME-Version: 1.0
Content-Type: multipart/mixed;
        boundary="----=_Part_29_10991923.1323109940542"
X-Envelope-From: pam@cs4161
X-Envelope-To: pam@cs4161
X-FromIP: 10.33.12.18

SENDER: admin@serena.com

------=_Part_29_10991923.1323109940542
SENDER: admin@serena.com
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: 7bit
```

$NOTES()

- **Description**

  Includes notes added to an item by users or by e-mail messages.

- **Usage**

- Individual notes that exceed the character limit specified in SBM Configurator are added to the notification as attachments.

  Notes are only included with a notification if users have privileges to view those notes in the associated item.

- **Parameters**
  - $NOTES() or $NOTES(0) – Displays all notes on the item.
  - $NOTES(N) – Returns the last *N* number of notes on the item. For example, $NOTES(3) returns the last three notes that were added to the item.
  - $NOTES(-N) – Returns the first *N* number of notes on the item. For example, $NOTES(-3) returns the first three notes that were added to the item.

- **Sample**

```
$NOTES()
```

  Result:

Notes:

--- Note 1 ----------
"Need status on this item" by Administrator (Mon Sep 09 20:47:44 GMT 2013)

Please update the status of this item by the end of the week. Thanks!
--- End of note 1 ----------
--- Note 2 ----------
"Follow up" by Administrator (Mon Sep 09 20:47:58 GMT 2013)

Have you had a chance to review the status yet? Thanks!
--- End of note 2 ----------

$NOTIFICATION()

- **Description**

  Returns the name of the notification.

- **Usage**

  The notification name is available on the **General** page when you are adding or editing notifications and escalations.

- **Parameters**

  None.

- **Sample**

```
$NOTIFICATION() - $ITEMNUMBER()
```

$PAUSESTATUS()

- **Description**

  Returns whether the item is paused or unpaused.

- **Usage**

  Use to indicate whether an item is paused or unpaused. If an item has been paused by Serena Demand Manager, the tag returns "Paused".

- **Parameters**

  None.

- **Sample**

```
$PAUSESTATUS()
```

$RECIPIENT()

- **Description**

  Returns the name of the notification recipient.

- **Usage**

  The name specified in the **Full Name** box in the user's profile is used.

- **Parameters**

  None.

- **Sample**

```
To $RECIPIENT():
```

  Result:

  To Allison IT Specialist:

$RECIPIENTEMAIL()

- **Description**

  Returns the e-mail address of the notification recipient.

- **Usage**

  All e-mail addresses specified for a user are returned. Mutiple e-mail addresses are separated by a semi-colon.

- **Parameters**

  None.

- **Sample**

```
To $RECIPIENT() at $RECIPIENTEMAIL():
```

  Result:

  To Allison IT Specialist @allison@serena.com

$REPEATCOUNTER()

- **Description**

  Returns the current number of repeated notifications.

- **Usage**

  Use this tag to display the number of times that the notification has been repeated.

- **Parameters**

  None.

- **Sample**

```
Number of repeated notifications: $REPEATCOUNTER()
```

Result:

```
Number of repeated notifications: 5
```

$TITLE()

- **Description**

  Returns the title of the item associated with the notification.

- **Usage**

  Information provided in the system *Title* field is used.

- **Parameters**

  None.

- **Sample**

```
$SYSFIELDNAME(TS_SYSFLD_TITLE): $TITLE()
```

Result:

Title: Create marquee/scrolling line around pasted image

$TRIGGEREDDATETIME()

- **Description**

  Returns the date and time the notification rule became "true" for an item.

- **Usage**

  Date and time are formatted for the locale set in each user's profile.

- **Parameters**

  None.

- **Sample**

```
This notification was triggered at $TRIGGEREDDATETIME()
```

Result:

This notification was triggered at 07/22/2011 11:42:10 AM

$TTID()

- **Description**

  Returns the identifier ([ttid: table ID, record ID]) required by the E-mail Recorder feature, which attaches replies to the e-mail notification to the item to which it pertains.

- **Usage**

By default, the `$TTID()` tag is enclosed by the `$BEGINSUBJECT()` and `$ENDSUBJECT()` base template tags in the default.txt notification template. This tag must remain in this location for the E-mail Recorder to function properly. If the E-mail Recorder is not configured, this tag is ignored. For details on the E-mail Recorder, refer to the *SBM Installation and Configuration Guide*.

- **Parameters**

  None.

- **Sample**

```
$BEGINSUBJECT()$NOTIFICATION() - $ITEMNUMBER() $TTID()$ENDSUBJECT()
```

  Result:

  CAR - Any Change Request changes state - UPLA000142 [ttid: 1003,19]

E-mail Submission Template Tags

E-mail Submission template tags can only be used with templates used for success and failure confirmation messages sent for e-mail submissions. For details on this feature, refer to Mailboxes and E-mail Submission [page 435].

$ATTACHMENTLIST()

- **Description**

  Returns a list of attachments submitted by the user as part of the e-mail submission.

- **Usage**

  If users do not have privileges to add attachments, an error is included in the message. If attachments are not included with the e-mail submission, this tag is empty.

- **Parameters**

  None.

- **Sample**

```
$ATTACHMENTLIST()
```

  Result:

```
—ConfigurationSteps.txt————————————————————


—Errors.txt———————————————————————————————
```

$FROMEMAIL()

- **Description**

  Returns the name of the user who submitted the item by e-mail.

- **Usage**

  If the user's name cannot be found, returns the user's e-mail address.

- **Parameters**

  None.

$IF(FOUNDUSER)

- **Description**

  Determines if an e-mail submission is received from a valid user based on the submitter's e-mail address specified in the user's SBM account.

- **Usage**

  Use with `$ELSE()` and `$ENDIF()` tags.

- **Parameters**

  None.

- **Sample**

```
$IF(FOUNDUSER)Please contact your administrator. We were
     unable to submit your message.
$ELSE()Thank you for submitting an automated support request. We were
     unable to process your e-mail. We could not find your e-mail address
     within our current records.
$ENDIF()
```

  Result:

  Valid users receive the following:

```
Please contact your administrator. We were unable to submit
      your message.
```

  Invalid users receive the following:

```
Thank you for submitting an automated support request. We were unable to
       process your e-mail. We could not find your e-mail address within our
       current records.
```

$ITEMNUMBER()

- **Description**

  Returns the Item ID for the newly submitted item.

- **Usage**

  Prefix and ID number are returned.

- **Parameters**

  None.

- **Sample**

```
$ITEMNUMBER() was created. You may connect to this item at
$LINK()
```

  Result:

000204 was created. You may connect to this item at
http://YOURSERVER/tmtrack/tmtrack.dll?View&I=11&T=1006

http:///tmtrack/tmtrack.dll?View&I=11&T=1006

$PROJECT()

- **Description**

  Returns the project to which the item was submitted.

- **Usage**

  Project name is returned. Hierarchy information is not included.

- **Parameters**

  None.

- **Sample**

```
$ITEMNUMBER() was created in $PROJECT().
```

  Result:

  000206 was created in the Documentation Errors project.

$RETURNEMAIL()

- **Description**

  Returns the text of the submitted e-mail message.

- **Usage**

  Useful in failure messages to return the original submission to the sender.

- **Parameters**

  None.

- **Sample**

```
Your Message:
<br>
$RETURNEMAIL()
```

  Result:

Your Message: The configuration documentation contains several typos, which are highlighted in the attached document.

Scheduled Report Template Tags

Scheduled report template tags can only be used with templates used for success and failure confirmation messages sent for scheduled reports. For details on this feature, refer to the "Scheduling Reports" topic in the *SBM User's Guide*.

$PROJECT_NAME()

- **Description**

  Returns the name of the project that contains the report.

- **Usage**

  Include this tag to display the project name.

- **Parameters**

  None.

- **Sample**

```
The $PROJECT_NAME() report <b>[$REPORT_NAME()]</b> that was generated on
<b>$REPORT_DATE() is attached to this message</b>.
```

  Result:

```
The Animation Pro report [All Issues I Own] that was generated on
Fri Dec 14 13:02:23 PST 2012 is attached to this message.
```

$REPORT_DATE()

- **Description**

  Returns the date and time at which the report was initially executed.

- **Usage**

  Include this tag to display the date and time.

- **Parameters**

  None.

- **Sample**

```
$REPORT_DATE()
```

  Result:

```
Fri Dec 14 13:02:23 PST 2012
```

$REPORT_NAME()

- **Description**

Returns the name of the report that was executed.

- **Usage**

  Include this tag to display the report name.

- **Parameters**

  None.

- **Sample**

  ```
  $REPORT_NAME()
  ```

  Result:

  ```
  [All Issues I Own]
  ```

$REPORT_URL()

- **Description**

  Returns the URL of the report that was executed.

- **Usage**

  Include this tag to display the report URL.

- **Parameters**

  None.

- **Sample**

  ```
  For the latest results of this report, click <a href="$REPORT_URL()">HERE</a>.
  ```

  Result:

  ```
  For the latest results of this report, click HERE.
  ```

%BEGIN_SUCCESS_SUBJECT% and %END_SUCCESS_SUBJECT%

- **Description**

  Returns a success message in the subject part of the e-mail when a report is successfully executed.

- **Usage**

  The markers cannot be changed but they must be present.

- **Parameters**

  None.

- **Sample**

```
%BEGIN_SUCCESS_SUBJECT%
Report [$REPORT_NAME()] was created on $REPORT_DATE().
%END_SUCCESS_SUBJECT%
```

Result:

```
Report [All Issues I Own] was created on Fri Dec 14 13:02:23 PST 2012
```

%BEGIN_ERROR_SUBJECT% and %END_ERROR_SUBJECT%

- **Description**

  Returns an error message in the subject part of the e-mail when a report fails.

- **Usage**

  The markers cannot be changed but they must be present.

- **Parameters**

  None.

- **Sample**

```
%BEGIN_ERROR_SUBJECT%
ERROR: Report [$REPORT_NAME()] failed to run on $REPORT_DATE().
%END_ERROR_SUBJECT%
```

Result:

```
ERROR: Report [All Issues I Own] failed to run on Fri Dec 14 13:02:23 PST 2012.
```

%BEGIN_EMAIL_FROM% and %END_EMAIL_FROM%

- **Description**

  Contains the content of the From field.

- **Usage**

  The markers cannot be changed but they must be present.

- **Parameters**

  None.

- **Sample**

```
%BEGIN_EMAIL_FROM%
NotificationServer@serena.com
%END_EMAIL_FROM%
```

Result in the From field of the e-mail message:

```
NotificationServer@serena.com
```

%BEGIN_SUCCESS_CONTENT% and %END_SUCCESS_CONTENT%

- **Description**

  Returns a success message in the body part of the e-mail when a report is successfully executed.

- **Usage**

  The markers cannot be changed but they must be present.

- **Parameters**

  None.

- **Sample**

```
%BEGIN_SUCCESS_CONTENT%
Hello,
</br>
</br>
The SBM report <b>[$REPORT_NAME()]</b> that was generated on <b>$REPORT_DATE() is
attached to this message</b>.
</br>
</br>
Note that if the report contains drill-down options, you can click them in the PDF.
The drill-down links launch the report and display the current results, and not
necessarily the results that appeared when the report was initially generated. This
means there may be a difference between the results listed in the report and the results
that appear when you click the drill-down option.
</br>
</br>
For the latest results of this report, click <a href="$REPORT_URL()">HERE</a>.
%END_SUCCESS_CONTENT%
```

Result:

```
Hello,

The SBM report [All Issues I Own] that was generated on Fri Dec 14 13:02:23 PST 2012 is
attached to this message.

Note that if the report contains drill-down options, you can click them in the PDF. The
drill-down links launch the report and display the current results, and not necessarily
the results that appeared when the report was initially generated. This means there may
be a difference between the results listed in the report and the results that appear when
you click the drill-down option.

For the latest results of this report, click HERE.
```

%BEGIN_ERROR_CONTENT% and %END_ERROR_CONTENT%

- **Description**

  Returns an error message in the body part of the e-mail when a report fails.

- **Usage**

The markers cannot be changed but they must be present.

- **Parameters**

  None.

- **Sample**

```
%BEGIN_ERROR_CONTENT%
Hello,
</br>
</br>
Your SBM report <b>[$REPORT_NAME()]</b> failed to run on <b>$REPORT_DATE()</b>.
</br>
</br>
The report might have failed for any of the following reasons:
</br>
1)  - The report does not exist.
</br>
2) - The user lacks sufficient privileges to run the report.
</br>
3) - The report encountered a system exception.
</br>
</br>
To verify that you can access and run the report,
click <a href="$REPORT_URL()">HERE</a>.
</br>
</br>
If the scheduled report fails to run, contact your SBM administrator.
%END_ERROR_CONTENT%
```

Result:

```
Hello,

Your SBM report [All Issues I Own] failed to run on Fri Dec 14 13:02:23 PST 2012.

The report might have failed for any of the following reasons:
1) - The report does not exist.
2) - The user lacks sufficient privileges to run the report.
3) - The report encountered a system exception.

To verify that you can access and run the report, click HERE.

If the scheduled report fails to run, contact your SBM administrator.
```

User Registration and Password Template Tags

User registration and password tags can only be used for external user registration confirmations and password change messages. In addition, SBM includes Base template tags that can be used in all these e-mail templates.

$LOGINID

- **Description**

Returns the user's SBM login ID.

- **Usage**

  Use the $USERDISPLAYNAME() to return the user's name.

- **Parameters**

  None.

$NEWPASSWORD()

- **Description**

  Returns a system-generated password.

- **Usage**

  When a user receives a new password via an e-mail using this tag, the user's SBM account is updated to reflect the new password.

- **Parameters**

  None.

$USERDISPLAYNAME()

- **Description**

  Returns the user's name.

- **Usage**

  Use the $LOGINID() tag to return the user's login ID.

- **Parameters**

  None.

View Sharing Template Tags

View sharing template tags can only be used with e-mail templates used for informing users when a view has been shared or unshared with them in Work Center.

You can also use Base Global template tags in view sharing e-mail templates.

$VIEWNAME()

- **Description**

  Returns the name of the activity view.

- **Usage**

  Use in subject line or in template body.

- **Parameters**

  None.

$VIEWDESCRIPTION()

- **Description**

Returns the description of the activity view.

- **Usage**

  Useful for sending details about the view to users.

- **Parameters**

  None.

$VIEWLINK()

- **Description**

  Returns a link to the view.

- **Usage**

  Link is valid only for users who own a view or with whom a view is shared. For best results, do not include this tag in the template used to notify users that a view is no longer shared with them.

- **Parameters**

  None.

Base Item Template Tags

Base Item template tags can be used to customize templates used for e-mail submissions, notifications, and e-mails sent from items.

$FIELDVALUE()

- **Description**

  Returns the value of a specified field.

- **Usage**

  Asterisks replace field values for users who do not have permission to view fields included in the message. Fields in the *Not Used* fields section are not included in the e-mail notification.

- **Parameters**

  - `FIELD_NAME` - Insert the database field name between the parentheses. Be sure to omit the TS_ prefix.
  - `PROJECTID` - Returns the name of the project in which the primary item associated with the e-mail message resides.
  - `PROJECTID, FULL` - Returns the full path of the project in which the primary item associated with the e-mail message resides.
  - `USER_FIELD_NAME` - For *User* and *Multi-User* fields, returns the name and a link to the e-mail address (HTML templates only) of the users associated with the field.
  - `(USER_FIELD_NAME, NO_EMAIL)` - For *User* and *Multi-User* fields, returns the name of the user associated with the field.

- **Sample**

```
$FIELDVALUE(DOC_LEAD)
<br>
<br>
$FIELDVALUE(PROJECTID)
<br>
<br>
$FIELDVALUE(PROJECTID, FULL)
<br>
<br>
$FIELDVALUE(SUBMIT_DATE)
<br>
<br>
$FIELDVALUE(WRITER, NO_EMAIL)
```

Result:

Pam Doc Manager

Serena Service Manager

Base Project:Documentation Project:Serena Service Manager

05/13/2011 01:09:42 PM

Allison Tech Writer

$LINK()

- **Description**

  Returns a text link to the primary or auxiliary item to which the e-mail pertains.

- **Usage**

  Use the `$LINK()` tag without additional parameters for text templates.

- **Parameters**
  - `TRUE` - Applies only to HTML templates and returns a hyperlink to the primary or auxiliary item to which the e-mail pertains.
  - `TRUE, link description` - This tag applies only to HTML templates and returns a customizable hyperlink to the primary or auxiliary item to which the e-mail message pertains.

- **Sample**

```
$STRING(IDS_EMAIL_TOVIEW) $ITEMTYPENAME():</b> $LINK(TRUE, Click here.)
```

Result:

To View Change Request: Click here.

$RECORDID()

- **Description**

  Returns the database ID for the primary or auxiliary item to which the e-mail pertains.

- **Usage**

  Useful for providing users with the internal identifier for specific items.

- **Parameters**

  None.

$SYSFIELDNAME()

- **Description**

  Returns the logical field name for specific system fields.

- **Usage**

  Useful for providing a label in the message for system field names that may be different in various applications.

- **Parameters**

  - `TS_SYSFLD_TEXT_DISPLAYID` - Returns the logical field name for the *Item ID* field.
  - `TS_SYSFLD_TITLE` - Returns the logical field name for the system *Title* field.
  - `TS_SYSFLD_DESC` - Returns the logical field name for the system *Description* field.

- **Sample**

```
<b>$SYSFIELDNAME(TS_SYSFLD_TEXT_DISPLAYID):</b> $FIELDVALUE(Item ID)
<br>
<br>
<b>$SYSFIELDNAME(TS_SYSFLD_TITLE):</b> $FIELDVALUE(Title)
<br>
<br>
<b>$SYSFIELDNAME(TS_SYSFLD_DESC):</b> $FIELDVALUE(Description)
```

Result:

Item Id: 000135

Title: Allow Image Builder to display 32X32 bit icons.

Description: We should allow Image Builder to display 32X32 bit icons.

$TABLEID()

- **Description**

  Returns the database ID for the primary or auxiliary table to which the e-mail pertains.

- **Usage**

  Useful for providing users with the internal identifier for specific tables.

- **Parameters**

  None.

Base Global Template Tags

Base global template tags can be used in all types of SBM e-mail templates, except for scheduled reports.

$BASEURL()

- **Description**

  Returns the URL for the User Workspace login page.

- **Usage**

  Use this tag to display the User Workspace URL. To provide links to specific items, use the `$LINK()` tag.

- **Parameters**

  None.

- **Sample**

  ```
  To view all items you own, log in to $BASEURL().
  ```

  Result:

  To view all items you own, log in to http://yourserver/tmtrack/tmtrack.dll?.

$BEGINSUBJECT(), $ENDSUBJECT()

- **Description**

  Use to customize the subject line of the e-mail message.

- **Usage**

  For HTML e-mail templates, the subject tags should precede all HTML formatting, as shown in the following sample. For text e-mail templates, the subject tags should be on the first line of the template.

- **Parameters**

  None.

- **Sample (for HTML template)**

```
$BEGINSUBJECT()$NOTIFICATION() - $ITEMNUMBER() $TTID()$ENDSUBJECT()
<html>
<head>
```

Result:

subject **CAR - Any Change Request changes state - UPLA000142 [ttid: 1003,19]**

$GETSETTINGSSTR()

- **Description**

  Returns data from specified settings in the TS_SYSTEMSETTINGS table.

- **Usage**

  Use this tag to return system data, such as field section labels or the system administrator's e-mail address.

- **Parameters**

  Setting name as specified in the SBM *Database Schema Reference*.

- **Sample**

```
For assistance, contact $GETSETTINGSSTR(AdminEmailToolbar)
```

Result:

For assistance, contact SBMAdministrator@serena.com

$KNOWLEDGEBASE()

- **Description**

  Provides a link to anonymous use page of the SBM Knowledge Base.

- **Usage**

  Applies to on-premise only.

  The link is valid only if you have enabled anonymous access to the SBM Knowledge Base in SBM System Administrator.

- **Parameters**

  None.

- **Sample**

```
For assistance, refer to:
<br>
$KNOWLEDGEBASE()
```

Result:

For assistance, refer to:
http:// server /tmtrack/tmtrack.dll?AnonymousUse&template=knowhome

$SENTBY()

- **Description**

  Returns the value specified as the mail sender in the SBM Configurator. By default, "SBM Notification Service" is returned.

- **Usage**

  Use to indicate the sender of the e-mail message either in the subject or body.

- **Parameters**

  None.

- **Sample**

  ```
  Sent by $SENTBY()
  ```

  Result:

  ```
  Sent by ACME Notification Service
  ```

$STRING()

- **Description**

  Returns text specified as the root value for records in the *String IDs* system auxiliary table. You can use existing string IDs or create your own. For details, refer to the "Customizing and Translating SBM User Workspace Strings" section of the *SBM System Administrator Guide*.

- **Usage**

  Using strings rather than text messages in your templates is recommended if your system includes multiple languages, such as English and Japanese. The `$STRING()` tag returns translated text based on the user's preferred language setting in his or her user profile.

- **Parameters**

  String ID name.

- **Sample**

  ```
  $STRING(IDS_EXIT_THANKYOU)
  ```

  Result:

  Thank you for using Serena Business Manager.

$TEMPLATENAME()

- **Description**

  Returns the file name of the template used for the notification.

- **Usage**

  This tag can be useful if your system contains a large number of e-mail templates or for troubleshooting.

- **Parameters**

  None.