Table of Contents

Chapter 1: Welcome to Serena® Business Manager ................................................ 7
  Audience and Scope ......................................................................................... 7

Chapter 2: Pre-installation ................................................................................ 9
  Overview ........................................................................................................ 9
    SBM Components ......................................................................................... 9
  About the Suite Installer .............................................................................. 10
  Pre-installation Checklist .......................................................................... 11
  Installation Considerations ........................................................................ 13
    About Environments .................................................................................. 14
    Single Environment Setting ..................................................................... 14
    Multi-Environment Setting ...................................................................... 15
  Hardware Requirements ............................................................................. 15
  Preparing Your Database ........................................................................... 16
    SQL Server Checklist .............................................................................. 17
    Oracle Checklist ....................................................................................... 19

Chapter 3: Single Environment Installation ...................................................... 21
  Overview ...................................................................................................... 21
  Running the Installer .................................................................................. 23
  Configuring SBM in Wizard Mode .............................................................. 24
  Initializing the Databases .......................................................................... 26
  Finishing the Configuration ....................................................................... 28
  Verifying Installation ................................................................................ 29
  Next Steps .................................................................................................. 30

Chapter 4: Multi-Environment Installation ....................................................... 31
  Overview ...................................................................................................... 31
  Installing SBM in Multiple Environments .................................................. 34

Chapter 5: Configuring SBM .......................................................................... 39
  About SBM Configurator ........................................................................... 39
  General Settings .......................................................................................... 41
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Servers</td>
<td>41</td>
</tr>
<tr>
<td>About Data Sources</td>
<td>43</td>
</tr>
<tr>
<td>About Windows Authentication</td>
<td>44</td>
</tr>
<tr>
<td>Component Servers</td>
<td>45</td>
</tr>
<tr>
<td>Clustering Server Components</td>
<td>49</td>
</tr>
<tr>
<td>IIS Server</td>
<td>54</td>
</tr>
<tr>
<td>Tomcat Server</td>
<td>59</td>
</tr>
<tr>
<td>License Server</td>
<td>62</td>
</tr>
<tr>
<td>Authentication</td>
<td>63</td>
</tr>
<tr>
<td>General Settings</td>
<td>63</td>
</tr>
<tr>
<td>About Single Sign-On (SSO)</td>
<td>66</td>
</tr>
<tr>
<td>Why Use Single Sign-On (SSO)?</td>
<td>66</td>
</tr>
<tr>
<td>Single Sign-On (SSO) Components</td>
<td>67</td>
</tr>
<tr>
<td>Customizing the SSO Login Page</td>
<td>68</td>
</tr>
<tr>
<td>About Windows Domain Authentication</td>
<td>68</td>
</tr>
<tr>
<td>Configuring Windows Domain (NTCR) Authentication</td>
<td>69</td>
</tr>
<tr>
<td>About LDAP Authentication</td>
<td>72</td>
</tr>
<tr>
<td>Configuring LDAP Authentication</td>
<td>73</td>
</tr>
<tr>
<td>Preparing LDAP for SBM</td>
<td>76</td>
</tr>
<tr>
<td>About Third-Party Authentication</td>
<td>77</td>
</tr>
<tr>
<td>Configuring External Identity Provider Settings</td>
<td>77</td>
</tr>
<tr>
<td>Password Restrictions</td>
<td>79</td>
</tr>
<tr>
<td>Custom Authentication Settings</td>
<td>80</td>
</tr>
<tr>
<td>Configuring Authenticators</td>
<td>81</td>
</tr>
<tr>
<td>Configuring Identity Transformers</td>
<td>82</td>
</tr>
<tr>
<td>Using Smart Card Authentication with SBM Composer</td>
<td>83</td>
</tr>
<tr>
<td>Other Settings</td>
<td>85</td>
</tr>
<tr>
<td>Mail Services</td>
<td>87</td>
</tr>
<tr>
<td>About the Notification Server</td>
<td>88</td>
</tr>
<tr>
<td>Configuring the Notification Server</td>
<td>88</td>
</tr>
<tr>
<td>About the Mail Client</td>
<td>99</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Creating an Environment</td>
<td>148</td>
</tr>
<tr>
<td>Chapter 7: Client Installation</td>
<td>149</td>
</tr>
<tr>
<td>The Client Installer</td>
<td>149</td>
</tr>
<tr>
<td>Installing SBM Composer</td>
<td>149</td>
</tr>
<tr>
<td>Silent Installation</td>
<td>149</td>
</tr>
<tr>
<td>Chapter 8: Troubleshooting</td>
<td>151</td>
</tr>
<tr>
<td>Configuring Internet Information Services (IIS)</td>
<td>151</td>
</tr>
<tr>
<td>Settings for IIS 7 and IIS 8</td>
<td>151</td>
</tr>
<tr>
<td>Enabling the Web Server (IIS) Role and Role Services</td>
<td>151</td>
</tr>
<tr>
<td>Modifying Application Pool Options</td>
<td>152</td>
</tr>
<tr>
<td>Granting Permissions to the Database and File Structure</td>
<td>154</td>
</tr>
<tr>
<td>Enabling the ISAPI Filter</td>
<td>155</td>
</tr>
<tr>
<td>Changing the Primary SBM Application Engine Web Server</td>
<td>156</td>
</tr>
<tr>
<td>Additional Troubleshooting Tips</td>
<td>156</td>
</tr>
<tr>
<td>Appendix 9: Additional Information</td>
<td>159</td>
</tr>
<tr>
<td>Core Database Elements</td>
<td>159</td>
</tr>
<tr>
<td>Customizing E-mail Templates</td>
<td>161</td>
</tr>
<tr>
<td>E-mail Template Tags</td>
<td>162</td>
</tr>
<tr>
<td>Base Global Template Tags</td>
<td>165</td>
</tr>
<tr>
<td>Base Item Template Tags</td>
<td>168</td>
</tr>
<tr>
<td>Adding Custom Spell Check Dictionaries</td>
<td>173</td>
</tr>
<tr>
<td>Using Web Queries with SBM Session Cookies</td>
<td>174</td>
</tr>
<tr>
<td>Performing a Silent Installation</td>
<td>174</td>
</tr>
<tr>
<td>Silent Install Options</td>
<td>175</td>
</tr>
</tbody>
</table>
Chapter 1: Welcome to Serena® Business Manager

This document describes how to install and set up Serena Business Manager (SBM), a product of Serena Software, Inc.

SBM is a full-featured process app management tool that enables you to create process apps that pull and manage information and work-tracking items from different sources. Similarly, you can use SBM to manage orchestrations for your business processes, including access to other Web services and third-party applications.

Audience and Scope

This guide is intended for administrators who will install and configure SBM for use in a production environment. The entire installation and configuration process that you must follow in order to successfully use SBM is covered herein.

For steps that guide you through installing SBM for testing, demo, or trial purposes, refer to the SBM Quick Start Guide at the Documentation Center.
Chapter 2: Pre-installation

This chapter describes the tasks that you perform before you install SBM.

- Overview [page 9]
- Pre-installation Checklist [page 11]
- Installation Considerations [page 13]
- Hardware Requirements [page 15]
- Preparing Your Database [page 16]

Overview

The exact process for installing and configuring SBM depends on a variety of factors, such as the number of environments that you intend to establish, your database hosting strategy, and more. Before you begin planning for the installation, familiarize yourself with the various SBM server components.

SBM Components

The following components comprise a complete SBM installation. All of the components listed below are installed by the suite installer with the exception of Serena License Manager. Note that you will use the client installer to install SBM Composer on each client machine in your organization.

<table>
<thead>
<tr>
<th>SBM Application Engine</th>
<th>The component in SBM that executes applications. It powers Serena Work Center, SBM User Workspace, and SBM Application Administrator (the interface administrators use to work with applications).</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBM Orchestration Engine</td>
<td>The component in SBM that executes system workflows defined in orchestrations. Using SBM Composer, a designer can include Web services in an orchestration, which can then be executed in response to an event or by transitions in applications.</td>
</tr>
<tr>
<td>SBM Application Repository</td>
<td>A Web-based component that is responsible for the deployment and promotion of process apps to runtime environments. It also stores versions of process apps and their design elements as they are published or checked in using SBM Composer.</td>
</tr>
</tbody>
</table>
### Single Sign-On (SSO)

Refers to Serena-installed software that enables a user to log in to a Web-based component of SBM and be recognized on subsequent accesses to that component or other Web-based components of SBM. Also enables security tokens to be used in an orchestration, allowing Web services to be called without requiring the user to provide credentials at inconvenient times.

### SBM Common Services

Powers SBM’s Smart Search, Agile services for Work Center backlogs, and the REST Grid and PDF widgets.

### SBM Mail Services

Consists of the Notification Server and Mail Client services. The Notification Server sends notifications and e-mail messages to SBM users. The Mail Client enables the E-mail Submission and the E-mail Recorder features.

### SBM Logging Services

Powers solution usage reports in Serena Work Center and performs active diagnostics, which capture SBM Application Engine Web Server events that occur without requiring you to stop the IIS services. Once you start the SBM Logging Services service, all activities and events that are processed by the SBM Application Engine Web Server are logged, including the end-to-end processing of workflow activities that fire orchestrations.

### SBM Composer

A Windows client application that designers can use to create, edit, and deploy process apps.

### SBM System Administrator

A Windows application that administrators use to configure SBM Application Engine. SBM System Administrator is used to configure system settings and run database utilities, such as the Data Import Wizard.

### Serena License Manager

Serena License Manager (SLM) is a separate component that allows administrators to centralize license management across multiple software tools. The Serena License Manager helps administrators keep track of active licenses.

### SBM Configurator

Enables you to define the distribution of the SBM server components and configure a variety of important SBM installation settings. SBM Configurator is launched automatically when you finish the suite installer and click **Configure**. You can also launch SBM Configurator any time after the install to re-configure settings as necessary.

---

### About the Suite Installer

The SBM suite installer delivers all of the SBM Server components. You will run the suite installer on one or more servers to install SBM.
When you are ready to install SBM, download the SBM installer zip file, extract the contents, and open the resultant folder. From here, navigate to the \Suite directory, and then launch the executable. You must launch the executable from within the \Suite folder in order to properly run the installer. Alternatively, if you are installing from a DVD, you can use the index.html file instead of running the executable directly. The index.html page provides an easy-to-read Web page from which you can launch the various installers.

**Important:** If you copy the suite installer to a particular location and the path to that location includes certain characters, such as an exclamation point (!) or pound sign (#), the installer fails to install the suite components. Run the suite installer directly from the extracted folder instead.

You can also install SBM silently. For information, see Performing a Silent Installation [page 174].

**Repairing Your SBM Installation**

You use the repair option in the suite installer to replace missing or corrupt files, shortcuts, and registry entries in your SBM installation.

**To repair your installation:**

1. Execute the suite installer.

2. The "Welcome to the Install Wizard for Serena Business Manager" message appears. Click Next.

3. Select the Repair option. Click Next.

4. Click Finish when the repair operation is complete.

**Uninstalling SBM**

**To remove your installation:**

1. Execute the suite installer.

2. The "Welcome to the Install Wizard for Serena Business Manager" message appears. Click Next.

3. Select the Remove option. Click Next.

4. Click Finish when the remove operation is complete.

The uninstall process might not remove every file in the SBM installation directory. If you have added any custom files or if a file is locked during the uninstall process, you must manually remove or delete the files that remain in order to clear the directory completely.

**Pre-installation Checklist**

The following checklist describes the tasks that you need to perform before you begin the SBM install process.

- Review Installation Considerations [page 13] to determine which type of installation to implement. Decide how you will distribute the SBM server components in your installation.
• Verify that your servers meets the minimum recommended hardware requirements. For more information, refer to Hardware Requirements [page 15].

• Determine which DBMS you will use with SBM and complete the corresponding database checklist:
  ▪ SQL Server Checklist [page 17]
  ▪ Oracle Checklist [page 19]

For a list of databases and operating systems that are supported with SBM, refer to the Platform Matrix on the My Downloads tab at http://www.serena.com/support.

• Install Serena License Manager 2.2 and decide on a licensing strategy. For guidance, contact your sales consultant.

• Confirm the Internet Protocol version on each server. SBM is certified against Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). Note that SBM requires that both IPv4 and IPv6 stacks are present on each server, though IPv4 can be disabled.

• Install IIS on the server that will host SBM Application Engine if it is not installed already. SBM requires that you enable the Web Server (IIS) role and a specific set of role services for IIS 7 and IIS 8. If you have not added the Web Server (IIS) role, add it using the Windows Server Manager.

  **Tip:** On Windows 2008, the Add Roles Wizard prompts you to install the Windows Process Activation Service. Click Add Required Features to install the service. Click Next to continue.

Once the Web Server (IIS) role is enabled, enable the following role services:

  • Common HTTP Features – Select all, except WebDAV. WebDAV blocks important operations that are used by Serena Release Control.

  • Application Development – ASP.NET, .NET Extensibility, CGI, ISAPI Extensions, ISAPI Filters.

  • Health and Diagnostics – HTTP Logging.

  • Security – Basic Authentication, Windows Authentication.

  • Performance – None.

  • Management Tools – None.

• Disable the User Access Control setting before you install SBM on Windows 2008 or 2008 R2. To disable this setting, perform the following steps:

  1. From the Windows Start menu, open the Control Panel, and then select User Accounts.

  2. In the User Accounts window, click Turn User Account Control on or off.

  3. Clear the Use User Account Control (UAC) to help protect your computer check box.

  4. Click OK.
5. Reboot the server.

After the SBM install is finished, you can enable UAC; however, you must disable it again if you attempt to uninstall SBM.

- Install Microsoft .NET Framework 4.0 or higher on all Windows machines if it is not installed already. If it is not detected, the .NET Framework is installed by SBM. To save download and installation time, install version 4.0 or higher prior to running the SBM installer. If you will not have Internet access during the install, download and install version 4.0 or higher beforehand.

- Install the Adobe Flash Player on all client machines that will access Application Administrator. If the Flash Player is not installed or enabled in a supported browser, users will be prompted to install or enable it when they open Application Administrator.

### Installation Considerations

How you choose to install and configure SBM ultimately depends on how you plan to use SBM and whether or not you want to create multiple SBM environments. Review the following topics after you read the questions below.

- **About Environments** [page 14]
- **Single Environment Setting** [page 14]
- **Multi-Environment Setting** [page 15]

Prior to running the installer, try to determine:

- **Do I want to use a single production instance of SBM?**
  If you do not plan to complete user acceptance testing before pushing changes to production, or if you do not need to make design changes in a test environment before making changes in directly production, you can install and configure SBM in a single production environment. For more information, see **Single Environment Setting** [page 14].

- **Do I want to create multiple SBM environments in order to promote design changes between test, staging, and production instances of SBM?**
  If your system will require user acceptance testing, or if you need cannot make changes directly to production, you will want to establish a multi-environment installation that supports the "path to production" model. For more information, see **Multi-Environment Setting** [page 15].

- **Do I want to set up new environments and grow my current production instance of SBM into a path to production system?**
  If you are already using SBM in a production environment, but you want to add environments for testing or staging, you can move to a path to production system. Before you move to a path to production system, review the steps described in solution **S140642**, and visit **Serena Central** to learn more about using multiple environments with SBM.
About Environments

An environment is a named group of servers and services to which you can deploy process apps. Each environment has one Application Engine server and one or more other target servers and endpoints.

Environments enable you to define logical groupings of runtime servers. For example, you can separate a group of runtime servers for use in a production environment from the runtime servers used in staging.

**Important:** Each separate environment must use the same version of SBM. In other words, you cannot promote or deploy process apps from one version of SBM to another.

In addition to defining a group of servers, an environment stores the history of the process apps that are deployed and promoted to it. The environment also shows the process apps currently running on the Application Engine server.

Each environment contains a host Application Engine instance that is used to restrict access to the environment. For example, a user might be allowed to deploy process apps to a staging environment but restricted from deploying to the production environment.

When you install Application Repository, a Default environment is created with the primary Application Engine. Application Repository uses the primary Application Engine to authenticate Application Repository users. If the primary Application Engine does not authenticate your users using internal SBM passwords (for example, if it uses LDAP to authenticate instead), Application Repository still uses it to determine the privileges that control whether a user can access certain views and perform certain operations.

You can further organize environments into "environments sets". Environment sets are collections of environments to which you deploy process apps and among which you promote process apps. For example, an environment set might include test, staging, and production environments that comprise a single SBM system (and each set uses the same version of SBM). Your company might have multiple environment sets. You name the environment set when you initially create the SBM database in SBM System Administrator. Note that each environment in the environment set requires a different name.

Single Environment Setting

In a single environment setting, application designs and changes are deployed directly into your SBM production environment without promoting changes from a development or staging environment first. Consider implementing SBM in a single environment setting if you are not concerned with user acceptance testing prior to pushing changes to users in the production environment.

In a single environment installation, you can enable all of the SBM components on a single server; however, to optimize performance, Serena recommends that you distribute the components on separate servers using SBM Configurator.

If you know that you will routinely need to develop applications in a test environment before you deploy them to your production environment, install SBM in multiple environments according to Chapter 4: Multi-Environment Installation [page 31]. Note that if you do not create multiple environments now, you can still take advantage of the following options:
With a single environment installation, you can still design your initial applications in a test database prior to launching production. For details, refer to Chapter 3: Single Environment Installation [page 21].

If you decide later on that you want to grow your single SBM environment into a path to production system, review the steps described in solution S140642, and visit Serena Central to learn more about using multiple environments with SBM.

**Multi-Environment Setting**

In a multi-environment setting, application designs and changes are deployed into test and staging instances of SBM before they are promoted into production. Consider installing SBM in a multi-environment setting if you plan to complete user acceptance testing prior to pushing changes to users in the production environment.

In this type of installation, you establish separate SBM environments to enable the promotion of process app design changes, user information, groups, projects, and reports from testing to staging, and then into production. The combination of these environments is considered an environment set.

Within each environment in the set, you might choose to distribute the SBM components among separate servers, though typically only your production instance will benefit from a distributed installation.

Note the following important details about setting up a multi-environment installation:

- Each separate environment must use the same version of SBM. In other words, you cannot promote or deploy process apps from one version of SBM to another.

- One instance of Application Repository will be shared by all environments. Do not create separate Application Repository databases for each environment.

If you do not intend to develop applications in a test environment before you deploy them to your production environment, install SBM in a single environment according to Chapter 3: Single Environment Installation [page 21].

**Hardware Requirements**

Hardware requirements for the SBM application and database servers are as follows.

**Table 1. Recommended Hardware Requirements**

<table>
<thead>
<tr>
<th>Server Type</th>
<th>CPU</th>
<th>Cores and Threads</th>
<th>RAM</th>
<th>NIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>IIS / Tomcat</td>
<td>Intel Xeon CPU E5-2620 2.00 GHz</td>
<td>6 Cores, 12 Threads</td>
<td>16 GB</td>
<td>1 Gbps</td>
</tr>
<tr>
<td>Database</td>
<td>Intel Xeon CPU E5-2620 2.00 GHz</td>
<td>6 Cores, 12 Threads</td>
<td>16 GB</td>
<td>1 Gbps</td>
</tr>
</tbody>
</table>

**Table 2. Minimum Recommended Hardware Requirements**
### Important: In addition, note that the SBM server install itself requires at least 2 GB of free disk space. You must ensure each SBM server that you add has at least 2 GB of free disk space.

If you enable all SBM components on one machine, the recommended requirements enable SBM to have an average response time under a normal load. With the minimum requirements, the response time will be much slower; however, SBM will continue to run. You can improve performance and accommodate greater usage by scaling your system.

### Preparing Your Database

Before you install SBM, plan your database hosting strategy. You can host the various SBM databases in one or more database spaces; however, the best practice is to use multiple database spaces. Before you install SBM, create empty databases in your DBMS to host the SBM databases.

A complete SBM system consists of the following databases:

<table>
<thead>
<tr>
<th>Database Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Engine</td>
<td>Contains system, primary, and auxiliary tables. The Application Engine database contains deployed process apps and the runtime data entered by administrators and users.</td>
</tr>
<tr>
<td>Orchestration Engine</td>
<td>Contains runtime data related to the Orchestration Engine and its use.</td>
</tr>
<tr>
<td>Application Repository</td>
<td>Stores design elements and published process apps with version management history. SBM Application Repository connects to the repository database.</td>
</tr>
<tr>
<td>Common Log</td>
<td>Stores logging information that you can view in SBM Application Repository to debug or verify activities related to deployed applications or orchestrations.</td>
</tr>
<tr>
<td>Configuration Settings</td>
<td>Stores centralized configuration settings from each instance of SBM Configurator in your installation. Each instance of SBM Configurator can connect to this database to apply changes and perform updates.</td>
</tr>
</tbody>
</table>
The Orchestration Engine database can share the same database space with the Application Engine database; this is acceptable because SBM Orchestration Engine use of the database is minimal and will have little effect on the overall performance. You can create separate databases for the remaining components. This separates the runtime data (created by the Application Engine and orchestrations) from the rest of the SBM data.

Serena recommends that you create a total of four separate empty database spaces for your production SBM environment before you begin the installation. This provides the following benefits:

- The data entered by users is kept separate from the data used to build and describe process apps and other design artifacts.
- Storing data in separate databases allows more resources to be dedicated to each database or schema.
- This is the most manageable configuration for systems that use Application Repository to promote process app changes between development, test, and production environments. For more information about creating databases for multiple environments, refer to Database Setup [page 33].

**SQL Server Checklist**

Before you install SBM, consult your SQL Server DBA if necessary and complete the following tasks.

<table>
<thead>
<tr>
<th>Checklist Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read solution S140514 for information on recommended database clients and drivers.</td>
</tr>
<tr>
<td>Create database spaces to host the SBM databases.</td>
</tr>
</tbody>
</table>
Grant the database user account sufficient privileges to alter the database. For details, refer to solution S138590. The schema/owner account used to create the database is also used by the **Create Database Wizard** to create the SBM tables and metadata. (If you are using the SQL Server system administrator account, the tables will have "dbo" ownership.) The schema/owner owns all SBM tables created by the database wizard.

Ensure that the database user password does not contain a semicolon; the ODBC connection fails if the password contains a semicolon.

Ensure that the database name does not contain a period; if the database name contains a period, an error may occur when the database is upgraded.

Create the database using the appropriate collation setting for the server locale that you are using. The collation setting determines how text data is compared, which affects searching and sorting when symbols from the locale are used to name objects in SBM (such as orchestrations). For more information about collation settings, refer to solution S139874.

Select a collation that is case insensitive when you create the database.

**Important:** Do not use a case sensitive collation (containing either _CS or _BIN in the name). This leads to problems with future database upgrades and loss of some SBM functionality (for example, Mass Update reports).

Set the file size auto-growth numbers to large fixed sizes for the data and logs rather than a percentage. Specifying a fixed size allows for more efficient allocation in terms of disk space. Using a percentage is more likely to create greater fragmentation.

Install the SQL Server client on the SBM Application Engine machine if it is not already installed. For information on recommended database clients and drivers, refer to solution S140514.

Confirm that your database has TCP/IP enabled. Refer to the SQL Server documentation for enabling the TCP/IP protocol.

If you are using an existing Microsoft SQL Server instance, verify that the SQL Server Browser service is running. This service is required to verify the database connection in SBM Configurator.
Verify that your database user account can connect to SQL Server. To use SQL Authentication, ensure that the **SQL Server and Windows Authentication mode** option is enabled in SQL Server. To use Windows Authentication, configure SQL Server to allow either **Windows Authentication** or **SQL Server and Windows Authentication**. For more information on using Windows Authentication with SQL Server, refer to About Windows Authentication [page 44].

Gather the following connection information. You will enter this information in SBM Configurator later:

- Database server name
- Database server port number
- Database names
- Database user name and password
- Database instance name

### Oracle Checklist

Before you install SBM, consult your Oracle DBA if necessary and complete the following tasks.

<table>
<thead>
<tr>
<th>Checklist Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read solution S140514 for information on recommended database clients and drivers.</td>
</tr>
<tr>
<td>Create schemas to host the SBM databases.</td>
</tr>
<tr>
<td>Grant the Oracle user account sufficient roles and privileges. For details, refer to solution S133641.</td>
</tr>
<tr>
<td>Ensure that the database user password does not contain a semicolon; the ODBC connection fails if the password contains a semicolon.</td>
</tr>
<tr>
<td>Set the NLS_CHARACTERSET for the database instance to either AL32UTF8 or UTF8. (AL32UTF8 is preferred because it supports 4 byte UTF-8 character sequences, whereas UTF8 only supports 3 byte sequences). <strong>Tip:</strong> If you are performing an upgrade from TeamTrack, the NLS_NCHAR_CHARACTERSET must be AL16UTF16. Once the upgrade from TeamTrack to SBM is complete, the NLS_NCHAR_CHARACTERSET value is ignored; therefore, it no longer has to be set to AL16UTF16.</td>
</tr>
<tr>
<td>Set the tablespace blocksize to at least 8k. Application Repository fails to launch on Oracle systems if the tablespace blocksize is less than 8k.</td>
</tr>
<tr>
<td>---</td>
</tr>
<tr>
<td>Verify that you can connect to Oracle. Make sure that you have the correct Oracle service name.</td>
</tr>
<tr>
<td>Gather the following connection information. You will enter this information in SBM Configurator later:</td>
</tr>
<tr>
<td>• Database server host name</td>
</tr>
<tr>
<td>• Database server port number</td>
</tr>
<tr>
<td>• Database user name and password</td>
</tr>
<tr>
<td>• Service name</td>
</tr>
</tbody>
</table>
Chapter 3: Single Environment Installation

This chapter describes how to install SBM in a production environment. Before you begin, complete the tasks described in the Pre-installation Checklist [page 11].

- Overview [page 21]
- Running the Installer [page 23]
- Configuring SBM in Wizard Mode [page 24]
- Initializing the Databases [page 26]
- Finishing the Configuration [page 28]
- Verifying Installation [page 29]
- Next Steps [page 30]

Overview

The following sections provide recommendations for installing SBM in a production environment. To help you prepare for the install, review the information below about server and database setup, and then proceed to Running the Installer [page 23].

Server Setup

Before you install SBM, ensure that you have allocated the correct number of servers. You should have a basic understanding of the SBM components, and a plan for distributing them on separate servers.

You will define the component distribution in SBM Configurator after you install SBM on each server.

In a typical single environment installation, the SBM server components are distributed as follows:

<table>
<thead>
<tr>
<th>Server</th>
<th>Server Type</th>
<th>SBM Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 1</td>
<td>Web server (IIS)</td>
<td>SBM Application Engine</td>
</tr>
<tr>
<td>Server 2</td>
<td>Application server (Tomcat)</td>
<td>SBM Orchestration Engine</td>
</tr>
</tbody>
</table>
### Table 3.1: Server Types and Components

<table>
<thead>
<tr>
<th>Server</th>
<th>Server Type</th>
<th>SBM Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 3</td>
<td>Application server (Tomcat)</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Common Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Mail Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Logging Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single Sign-On (SSO)</td>
</tr>
</tbody>
</table>

- This means that you will run the SBM suite installer on three separate servers.
- An additional server can be allocated to create another instance of SBM Mail Services for failover or performance reasons.
- SBM Logging Services can be installed on a dedicated server if you plan to use TRACE level logging. For details, refer to Active Diagnostics [page 136].
Database Setup

The recommended database hosting strategy for a production environment is discussed in Preparing Your Database [page 16]. To review, in a typical production environment, you will create the following database spaces:

<table>
<thead>
<tr>
<th>Database</th>
<th>SBM Databases</th>
<th>Production</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database 1</td>
<td>Application Engine</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Orchestration Engine</td>
<td></td>
</tr>
<tr>
<td>Database 2</td>
<td>Application Repository</td>
<td>✔</td>
</tr>
<tr>
<td>Database 3</td>
<td>Common Log</td>
<td>✔</td>
</tr>
<tr>
<td>Database 4</td>
<td>Configuration Settings</td>
<td>✔</td>
</tr>
</tbody>
</table>

**Important:** If you plan to design applications in a test database prior to launching production:

- Use the backup and restore tools that are native to your DBMS to copy your test database that contains the SBM Application Engine and SBM Orchestration Engine tables immediately after running the **Create Database Wizard** (described later in this chapter), but prior to beginning any development work.

- When you are ready to launch production, you will promote your changes from the test database into this copy. This copy will then become your production database.

- This process ensures that you do not have any test data or incomplete development work in your production database (which would need to be removed prior to launch).

- This recommendation assumes that you will not implement a true environment set (comprised of separate test, staging, and production environments). If you plan to create an environment set, install SBM according to the steps in Chapter 4: Multi-Environment Installation [page 31].

Running the Installer

This section describes the steps that you perform in the suite installer to install SBM on a server.
Prerequisites:
When you run the installer, ensure that you do not run the installer as an administrator. This can potentially cause issues with deleting log files later on.

To install SBM:

1. Launch the SBM suite installer executable on the IIS server that will host SBM Application Engine.
2. The "Welcome to the Install Wizard for Serena Business Manager" message appears. Click Next to continue.
3. Accept the license agreement. Click Next to continue.
4. Provide the location in which to install SBM. Click Next to continue.
5. If either the Microsoft SQL Native Client or Microsoft ODBC Driver 11 for SQL are not detected on your server, the installer provides you the option to install SQL Express in case you want to evaluate SBM. For details on installing SQL Express and using the sample database for evaluation purposes, refer to the SBM Quick Start Guide at the Documentation Center. Click Install to begin the installation process.
6. Allow the install to complete, and then click Configure to launch SBM Configurator.

SBM Configurator collects important database connection and configuration information. For details, continue to Configuring SBM in Wizard Mode [page 24].

Configuring SBM in Wizard Mode

This section describes the steps that you perform in SBM Configurator immediately after you finish the suite installer. The steps assume that you are following the recommended component distribution that is described earlier in this chapter.

To configure SBM in wizard mode:

1. Launch SBM Configurator on the server that will host SBM Application Engine. The "Welcome to SBM Configurator" page appears.
2. Read the Welcome page, and decide if you will use the Configuration Settings database or not. Serena recommends that you use this database because it eases installation and administrative duties and keeps configuration settings across your entire SBM installation in sync. Click Next to continue.
3. On the Database Servers page, select the type of DBMS you are using, and then enter your database server connection information. In the table of databases, enter the database names and user credentials that you established in your DBMS earlier. Click Test to verify the connection for each database. Click Next to continue.
4. On the Component Servers page, define the distribution of the SBM server components.
   a. Right-click Orchestration Engine, and then select Move to new server. The Orchestration Engine component appears on Server 2.
b. Right-click Application Repository, and then select **Move to new server.** The Application Repository component appears on **Server 3.**

c. Drag and drop the remaining server components to **Server 3**, except for Application Engine (which stays on **this machine**). **Server 3** should now list all components except for Orchestration Engine and Application Engine.

**Tip:** When you move the Orchestration Engine, move the entire component to a new server. By moving the entire component, you keep the Event Manager and BPEL Engine sub-components on the same server, which optimizes performance for orchestrations. Note that when you enter a host name for the Orchestration Engine, the host name cannot contain an underscore "_". Only Latin characters (a-z and A-Z), digits 0-9, and hyphens are permitted, as described in RFC 952. Deployments will fail if the host name contains an underscore.

5. Enter connection information for each server on the **General** sub-tab:
   - Enter the host name for each server.
   - Use the default HTTP port 80 for IIS on the Application Engine server.
   - Use the default HTTP port 8085 on each Tomcat server for now.
   - Use the default TCP port 27017 for Active Diagnostics on server 3.

Click **Next** to continue.

6. On the **IIS Server** page, select an IIS Web site in the drop-down list. The **Default Web Site** is selected by default. Click **Next** to continue.

7. On the **Tomcat Server** page, accept the default port values for now. Click **Next** to continue.

8. Click **Next** on the **License Server, Authentication, and Mail Services** pages. These settings are stored in the Application Engine database, which must be initialized by the Create Database Wizard first.

9. Click **Finish** on the **Summary** page. SBM Configurator will attempt to stop any services that must be stopped. Click **Yes** when you are prompted to continue. Wizard mode is now complete on the Application Engine server.

10. Update the configuration on the other servers by performing the following steps.

   a. On the **Database Servers** tab, enter the connection information for your DBMS, and connect to the same **Configuration Settings** database that you specified on the SBM Application Engine server.

   b. Click the **Update From Database** button at the bottom of SBM Configurator. This updates the local machine with all of the configuration settings that you defined earlier on the Application Engine server.

   c. Click **Next** until you finish wizard mode on each server.

   **Note:** If you declined to use the Configuration Settings database, you must manually configure these servers or export and import snapshot files to ensure they all have the same database connection information.
Each server should now have the same updated configuration information and wizard mode should be finished on each server.

Next, you will launch SBM System Administrator on the Application Engine server and run the **Create New Database** wizard to initialize the database. For details, continue to Initializing the Databases [page 26].

### Initializing the Databases

After you finish wizard mode in SBM Configurator, initialize the SBM databases by following the steps in the topics below. This populates the databases with the required tables and core elements.

- Initializing the Application Engine Database [page 26]
- Initializing the Remaining Databases [page 28]

### Initializing the Application Engine Database

This section provides the steps that you will perform in SBM System Administrator to initialize the Application Engine database.

The information below provides the basic steps that you will follow to populate the Application Engine database and prepare it for initial use.

- For detailed information about the **Create New Database** wizard and its options, start the wizard, and then click the **Help** button on each page.

- To learn more about core database elements that are added by the wizard, see **Core Database Elements** [page 159].

**To initialize the database:**

1. On the server that hosts SBM Application Engine, launch SBM System Administrator. Click **OK** when the warning message appears. Click **Cancel** on the **Connect** dialog box.

2. From the SBM System Administrator menu bar, select **Tools**, and then select **Create New Database**.

3. A message appears that states that the target database will be overwritten. For new databases, this message can be safely ignored because there is no data to overwrite yet. Click **Yes** to continue.

4. The **Welcome** dialog box opens. Click **Next**.

5. In the drop-down list that appears, select the **SBM** data source. Click **Next**.

6. Enter the Application Engine database user **Login ID** and **Password**.
   - When you connect to an Oracle database, Oracle always uses the database specified by the user name at logon time, not what was originally specified in the data source.
   - For Microsoft SQL Server, the schema/owner account that you specify is used to create the database tables. If you are using the SQL Server system administrator...
account, the tables will have dbo ownership. The schema/owner owns all SBM tables created by the wizard.

Click **Next**.

7. Complete the following fields in the **System Settings** dialog box:
   - **System Administrator Login ID** – Enter a login ID for the person who will serve as the primary administrator for your system. An account with basic administrative privileges will be created for this user, who can then log in to SBM Application Administrator and grant additional privileges to his or her account and create accounts for other users. You must provide this information to continue.
   - **Password/Confirm Password** – Enter a password for the primary administrator, and then confirm that password.
   - **Environment Set** – Specify an environment set name for the database you are creating. An environment set is a collection of related environments, such as development, testing, and production environments, for a single SBM system. If you are only creating a single production environment, enter a name like **Production**.

   Note the following information about environment set names:
   - If you will have multiple environment sets, each set should have a unique name (to ease deployment and promotion activities).
   - You can change the environment set name later in SBM System Administrator.
   - All environments within an environment set should use the same environment set name.
   - Each environment should have a unique name within one environment set.
   - **License Server Host Name** – Provide the host name or IP address of your License Server machine or the name and location of the license file provided by Serena. If you provide a host name or IP address, use the IP address of the machine or the host name that is found in the Domain Name Server (DNS). If you use a license file, this file should be stored on a network location accessible to the SBM Application Engine Web Server.

8. Click **Next** to add the recommended set of custom fields to the **Companies** and **Contacts** tables that are included in every Application Engine database. If you do not want one or more of the fields created for a particular table, clear the corresponding check box, and then click **Next**.

9. Click **Finish** to initialize the database. When the process is finished, the **Connect** dialog box appears. Click **OK** to connect SBM System Administrator to your database.

The Application Engine database is now initialized and ready for use; however, additional database elements for the remaining databases must be created using SBM Configurator.
Initializing the Remaining Databases

After you run the Create New Database wizard in SBM System Administrator, follow the steps below to initialize the remaining databases.

The Application Repository, Orchestration Engine, and Common Log database tables are created once SBM Configurator is connected to each database and the SBM Tomcat service is started for the first time.

To initialize the databases:

1. Open SBM Configurator on the server that hosts SBM Orchestration Engine or SBM Application Repository.

2. On the Database Servers tab, verify that the database connection information is correct for each database.

3. Open the Manage Services tab, and then start the SBM Tomcat service. The service starts and begins populating the databases with core elements.

The remaining databases are now initialized and ready for use. There are a couple more steps to perform to finish the configuration. For details, continue to Finishing the Configuration [page 28].

Finishing the Configuration

After the databases have been initialized, use SBM Configurator to enter settings that could not be saved until the database was established. For example, connection information for the license server is stored in the database; therefore, it must be set after the database has been initialized by SBM System Administrator.

To finish the configuration:

1. On the server that hosts SBM Application Engine, open SBM Configurator and enter your license server information on the License Servers tab.

2. On the server that hosts SBM Common Services, open SBM Configurator and enter the attachments directory location as specified in SBM System Administrator on the SBM Application Engine server (Options | Settings | Attachments). For new installations, the default is:

   C:\Program Files\Serena\SBM\Application Engine\attachments

By default, file attachments that are added to items by your users are stored on the file system. If you change this setting in SBM System Administrator and decide to store attachments in the database instead, the Common Services tab automatically recognizes this and you do not need to provide a directory.
3. If you are using the Configuration Settings database (recommended), launch SBM Configurator on the server that hosts Single Sign-On (SSO) and generate new key pairs to properly secure SBM. If you declined to use the Configuration Settings database, you will need to follow the manual steps in Securing SBM [page 118] to secure SBM.

   **Important:** You must generate new key pairs in order to properly secure your SBM installation (even if you do not plan to use SSO to manage user sessions). If you do not generate new key pairs, then the default certificates that the internal Security Server inherently trusts are used.

   a. Click the **Security** tab, and open the **Secure SBM** sub-tab.

   b. Click **Generate All** to create unique certificates.

   c. Click **OK** in the dialog box that appears after the certificates are generated.

   d. Click **Apply** to save and finish.

   e. Click the **Update From Database** button in SBM Configurator on the other servers to secure your entire installation.

4. Open SBM Configurator on each server and start the services on the **Manage Services** tab.

5. Log in to Application Repository using your primary system administrator account. Select **Environments**, edit the **Default Environment**, and then verify that the **BPEL Server** and **Event Manager** were created in the **Target Servers** tab.

The initial SBM installation and configuration is now complete. Next, verify that the system is accessible by following the steps in Verifying Installation [page 29].

### Verifying Installation

After you finish configuring SBM, verify that the following components are accessible.

- **SBM Application Engine**
  Validate SBM Application Engine by using the following URL:

  \[http://servername/workcenter\]

  Log on using your primary system administrator account. You should see the SBM login page. If you do not, then IIS is not started or a problem exists with the workcenter application.

- **SBM Application Engine Web Services**
  Validate that the SBM Application Engine Web Services are available by using the following URL:

  \[http://servername:aePort/gsoap/gsoap_ssl.dll?sbmappservices72\]

  **Note:** The port should be the same TCP port specified by the Default Web site in IIS (typically port 80).
You should see a message like: 'You must use a POST request to get answer from gsoap!'. If not, IIS is not started or a problem exists with the gsoap application.

- **Application Repository**
  Validate that Application Repository is available by using the following URL:

  \[http://serverName:port/mashupmgr\]

  You should see Application Repository logon page. If not, then Tomcat is not running or the database connection is incorrect. Validate that Tomcat is running in SBM Configurator, and check database connection on the **Database Servers** tab.

  If you are not able to log on, then most likely the URL to the primary Application Engine host is incorrect. Application Repository requires a primary Application Engine host in order to validate users and check their privileges. The primary Application Engine is set in the **Component Servers** tab in SBM Configurator.

- **SBM Composer**
  Launch SBM Composer, and then click **Connect Now**. In the **Connection Settings** section, enter the Application Repository **Machine Name** and **Port** (the default is 8085). Enter the User Name and Password of a user that has Application Repository access, and then click **Test Connection**.

**Next Steps**

Congratulations! Your SBM production environment should be up and running. After you finish verifying your installation, review the following topics to learn about configuring advanced settings and preparing the system for your users.

- Review the topics discussed in Chapter 5: Configuring SBM [page 39] and configure important settings as described in the topics on Authentication [page 63] and Mail Services [page 87].

- Prepare the system for use by reviewing the topics in Chapter 6: Post-installation [page 141].
Chapter 4: Multi-Environment Installation

This chapter provides a complete overview of how to install SBM in a multi-environment setting. Before you begin, complete the tasks described in the Pre-installation Checklist [page 11].

The following topics describe how to install SBM in multiple environments.

- Overview [page 31]
- Installing SBM in Multiple Environments [page 34]

Overview

The following sections provide recommendations for installing SBM in multiple environments. To help you prepare for the install, review the information below about server and database setup, and then proceed to Running the Installer and Configuring SBM to complete the initial installation.

Server Setup

Before you install SBM, ensure that you have allocated the correct number of servers. You should have a basic understanding of the SBM components, and a plan for distributing them on separate servers.

You will define the component distribution in SBM Configurator after you install SBM on each server.
In a typical multi-environment installation, the SBM server components are distributed as follows:

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Server Type</th>
<th>SBM Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server 1</td>
<td>Web server (IIS)</td>
<td>SBM Application Engine</td>
</tr>
<tr>
<td>Server 2</td>
<td>Application Server (Tomcat)</td>
<td>SBM Orchestration Engine</td>
</tr>
<tr>
<td>Server 3</td>
<td>Application Server (Tomcat)</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Common Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Mail Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SBM Logging Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Single Sign-On (SSO)</td>
</tr>
</tbody>
</table>

**Important:** Note that SBM Application Repository is included in the production environment. You will use SBM Configurator to enable SBM Application Repository on Server 3 in the production environment. This lone instance of SBM Application Repository will be used by all three environments.

- This means that you will run the SBM suite installer on three separate servers to create your production environment.
- An additional server can be allocated to another instance of SBM Mail Services for failover or performance reasons.
- SBM Logging Services can be installed on a dedicated server if you plan to use TRACE level logging. For details, refer to *Active Diagnostics* [page 136].

To create your staging and test environments, you will run the SBM suite installer on two additional servers. You will use SBM Configurator to disable SBM Application Repository on these servers. This means that you will have a total of five SBM servers when you are finished: three for production, one for staging, and one for test.
Environment Set

When you have finished the install to complete each environment, you will have one complete SBM environment set:

![Environment Set Diagram]

Database Setup

In a typical multi-environment installation, your production environment will have the same database distribution as discussed in Preparing Your Database [page 16]. However, each additional environment should have dedicated databases for the Common Log and Configuration Settings databases. This means that for a typical multi-environment installation, you will create the following database spaces:

<table>
<thead>
<tr>
<th>Database</th>
<th>SBM Databases</th>
<th>Production</th>
<th>Staging</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database 1</td>
<td>Application Engine</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Orchestration Engine</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database 2</td>
<td>Application Repository</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database 3</td>
<td>Common Log</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Database 4</td>
<td>Configuration Settings</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Note the following important information:

- Each environment should have their own database space to host the Application Engine and Orchestration Engine databases.
- The staging and test environments do not have their own Application Repository database. Rather, the lone Application Repository database in production is shared by all environments.
- Each environment has its own Common Log database.
- All three environments share the one Configuration Settings database that is created in the production environment. When you set up and configure the test and staging environments, you will supply unique environment names on the Welcome page in SBM Configurator.

## Installing SBM in Multiple Environments

This section describes the steps that you perform to install SBM in multiple environments to create an environment set that enables the path to production model.

You will create your production environment first. After production is up and running, the rest of the steps guide you through the process of establishing your other environments.

### To successfully implement SBM in a multi-environment setting:

1. Complete all the tasks listed in Pre-installation Checklist [page 11].
2. Allocate the servers and databases for a multi-environment installation as described in Overview [page 31].
3. Create your production environment by following the steps in Chapter 3: Single Environment Installation [page 21], starting with Running the Installer [page 23]. When you are finished, you should have a complete and functional production environment.
4. If you are using the Configuration Settings database (recommended), open SBM Configurator and enter the name for your production environment in the System Settings | Configuration Settings tab, and then click Apply. Use the Update from Database option on each server to flag each production server as part of the production environment.
5. Log in to SBM Application Administrator as the primary system administrator. Ensure that this account has Regular User product access and all "user" privileges. This primary system administrator is now a "super user" who has all the same privileges and capabilities that a managed administrator has, but can also deploy and promote into the production environment. For details on administrative access and privileges, refer to the "Managing Administrators" section of the SBM Application Administrator Guide.
6. In SBM Application Administrator, establish additional user accounts. You can create users as needed later on; however, to establish and test a multi-environment system, consider creating at least three users with the following personas:
   - Designer
Designs process apps in SBM Composer and deploys the process apps to a test environment.

- **Managed administrator**
  Designs or modifies process apps in SBM Composer, but also configures deployed process apps. A typical managed administrator might be responsible for managing user accounts, creating notifications, and setting project overrides in SBM Application Administrator. Also, the managed administrator might have the privilege to deploy into the staging environment or promote from the test environment into staging.

- **End user**
  A typical end user logs into SBM and works with primary and auxiliary items. When you create your initial multi-environment system, you might create at least one end user that does not have any administrative privileges, but can work with items in the browser.

By establishing these users in production first, you ensure that the same login IDs will be used in each environment. Establishing privileges for these users requires changes in SBM Application Administrator and the Application Repository. For more information about these privileges and some example use cases, see Creating Users and Establishing Privileges [page 141].

7. Create a backup copy of the database that contains the SBM Application Engine and SBM Orchestration Engine tables using the backup and restore tools that are native to your DBMS. This copy will be used as the basis for your SBM Application Engine and SBM Orchestration Engine databases in the test and staging environments.

8. Restore the copied database into a blank database space in the test DBMS and the staging DBMS. This ensures that the same tables and users that you established in the production database earlier are replicated into your test and staging environments.

   **Note:** You must restore the copied production database into the database spaces that are designated for your test and staging databases. If you do not use a copy of the production database as the basis, you will not be able to promote between these environments. You must also ensure that the same licensing model is used for each environment. For example, if your production database uses seat licenses, you must ensure that the other environments have access to seat licenses as well (because the test and staging databases are copies of the production database).

9. Install SBM on the test server and on the staging server.

10. Once the installer is finished, launch SBM Configurator on both servers. Perform the following tasks:

   - Enter an **Environment name** for the test and staging environments on the Welcome page. This assumes that you are using the Configuration Settings database (recommended). Click Next.

   - On the **Database Servers** tab:
11. Log in to SBM Application Repository and create new environments for the test and staging environments. For more information, see Creating an Environment [page 148].

12. Prepare for creating and editing process apps by performing the following tasks:
   • Establish privileges for the rest of your designers and administrators who will create and modify process apps and applications in SBM Composer and deploy them to each environment. See Creating Users and Establishing Privileges [page 141] for details.
   • Get the Global Process App from the newly created SBM Application Engine database to allow designers to include core database elements, such as system auxiliary tables, in their process apps. For more information, see Getting the Global Process App [page 148].
   • Have designers, who will publish and deploy process apps to the SBM Application Engine, install SBM Composer on their machines using the client installer.
   • Provide designers with the configuration information to connect to Application Repository.

13. After setting the appropriate privileges and permissions, create and publish your workflows with the following process:
   a. Design process apps in SBM Composer.
   b. Publish completed process apps to the repository.
   c. Deploy completed process apps to your production server.
This completes the multi-environment install, which results in a single environment set. If you plan to create multiple environment sets, you will perform the same steps to set up each environment set. Keep in mind that each environment set will need its own Application Repository instance. If multiple environment sets share the same Application Repository, you will experience problems with keeping the Global Application synchronized to the correct database.
Chapter 5: Configuring SBM

This chapter describes SBM Configurator and the settings that you configure with the utility. An overview of SBM Configurator is provided first, followed by usage instructions and the tasks that you can perform in each tab.

- About SBM Configurator [page 39]
- General Settings [page 41]
- Advanced Settings [page 113]
- Utilities [page 132]

About SBM Configurator

SBM Configurator is launched automatically once you click **Configure** after the suite installer is finished. You can launch it from the Windows **Start** menu any time after the install is finished as well.

Wizard Mode

SBM Configurator runs in **wizard mode** immediately after the suite installer is finished. In **wizard mode**, you progress through the **General** tabs by clicking **Next**. Click **Back** to return to the previous tab. Once you finish **wizard mode**, SBM Configurator runs in **utility mode**.

- On the **Welcome** page, decide if you will use the **Configuration Settings** database to store your configuration settings in a centralized location. This option is preferred because it eases administrative duties and keeps configuration settings across your entire SBM installation in sync. For details, see **About the Configuration Settings Database** [page 40].

- If you click **Cancel** any time during the wizard, your current changes are discarded. To save your changes, click **Finish** at the end of the wizard. After you finish the wizard, launch SBM Configurator from the Windows **Start** menu to continue configuring your installation.

- Once you click **Finish** at the end of the wizard, SBM Configurator is launched in **utility mode**, which enables you to configure advanced settings that are not available in **wizard mode**.

Utility Mode

In **utility mode**, you can change your existing settings and use advanced options and utilities. You can also synchronize configuration settings across all your servers using the **Update From Database** option.

- When you select a tab in **utility mode**, corresponding details appear in the main pane. Unlike **wizard mode**, you can configure any tab at any time.
• Click **Apply** to save your changes or click **Close** to discard your changes. When you click **Apply**, the IIS and Tomcat services are stopped, and your changes are saved in the **Configuration Settings** database (if used). The IIS and Tomcat services are returned to their prior status once SBM Configurator saves the configuration changes.

  **Tip:** Users might not be able to access the system immediately while the services are restarting. Therefore, consider applying configuration changes at a time when users are not actively using the system.

• Under **System Settings**, you can select the **Use Configuration Settings database** option if you declined it on the **Welcome** page. Alternatively, you can select **Use Configuration Snapshots** if you do not want to use the **Configuration Settings** database any longer. For more information, see **System Settings** [page 133].

### About the Configuration Settings Database

During **wizard mode**, the **Welcome** page prompts you to decide if you will use the **Configuration Settings** database to store your configuration settings in a centralized location. Serena recommends that you use the **Configuration Settings** database because it eases administrative duties and keeps configuration settings across your entire SBM installation in sync.

If you decide to use the **Configuration Settings** database:

• The **Update From Database** button appears at the bottom of SBM Configurator. An icon next to the button indicates if the local configuration is in sync with the database. The date and time that changes were last applied are displayed as well.

• For distributed installations, you will use the **Update From Database** option to update the local configuration with changes that have been saved in the database from another server. SBM Configurator periodically polls the **Configuration Settings** database to ensure the settings on your local machine are in sync with the settings in the database. If changes have been detected in the database, you are prompted to click **Update From Database** to update your local settings.

  **Important:** The update process will discard any current changes you might have made locally that have not been applied. If you have changes on your local machine that must be applied, click **Apply** to commit them before performing an update. This will overwrite the settings in the database using your local configuration instead, so you must confirm this action.

If you decide not to use the **Configuration Settings** database:

• The **Update From Database** button does not appear and your configuration is stored on the file system (not in the database). If you are configuring multiple servers, you will use the **Import Configuration** option to import the configuration snapshot file that you exported from the first server you configured.

• For distributed installations, this means you must export and import configuration snapshot files on each server to keep the system configuration up-to-date or you must perform updates manually on each server (not recommended). These are the only methods that ensure that each distributed server shares the same component server and database connection information if the **Configuration Settings** database is not used.
For example, if you change the IIS port number on the SBM Application Engine server, you must update the configuration settings on the Application Repository and SBM Mail Services machines as well to ensure they can still communicate with SBM Application Engine. (This change is automatically detected if you use the Configuration Settings database to store configuration settings for all servers in a centralized location.)

**General Settings**

From the **General** menu, you provide configuration settings to finish the SBM installation and configuration process in **wizard mode**. The **General** menu tabs are available in both **wizard mode** and **utility mode**.

**Database Servers**

In the **Database Servers** tab, you configure the distribution and connection information for the SBM databases. You typically configure the **Database Servers** tab in **wizard mode** after you install SBM.

Initially, the **Database Servers** tab contains a single server (**Server 1**). By default, all of the SBM databases are listed on this server. You can define additional servers by dragging and dropping SBM databases into the space below **Server 1**. Alternatively, right-click any database and select the option **Move to new server**.

To use the SBM sample database, select the **Use sample database** check box and configure the database server settings for the server that will host the sample database according to the steps in the SBM Configurator help.

- Entering Database Server Information [page 41]
- Entering Database Connection Information [page 42]

**Entering Database Server Information**

To connect to your database server, provide the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Engine ODBC data source</td>
<td>Displays the current ODBC data source that is used to connect to the Application Engine database. Click <strong>Change</strong> to create a new data source, rename the default data source, or select an existing data source. For more information, see About Data Sources [page 43].</td>
</tr>
<tr>
<td>Type</td>
<td>Select the type of DBMS you are using (SQL Server or Oracle). The database type that you select determines which of the following fields appear.</td>
</tr>
<tr>
<td>Windows Authentication</td>
<td>Select this check box to use Windows Authentication instead of SQL Authentication. For more information, see About Windows Authentication [page 44].</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the host name of your database server.</td>
</tr>
</tbody>
</table>
### Entering Database Connection Information

After you enter your database server information, enter connection information for each SBM database. A warning message appears for each required field that is not completed.

For SQL Server systems, use the **Database** column to define which database in SQL Server will host each SBM database. For Oracle systems, use the **Schema/User name** column to define which schema in Oracle will host each SBM database. For recommendations on hosting the SBM databases, refer to *Preparing Your Database* [page 16].

Note the following important information:

- The SBM Mail Services component uses the SBM Application Engine database to store settings and configuration. Therefore, you must ensure that the server or servers that run the SBM Mail Services have access to the correct SBM Application Engine database connection information.

- You must enter database connection information for the Application Engine database (even though the database connection information is in the DSN that is selected in the **Application Engine ODBC data source** field). This ensures that SBM framework elements and components that do not use ODBC can still connect to the database.

To connect your databases, provide the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Enter the name of the database space you created in SQL Server. <strong>Note:</strong> You can specify the same name if one or more components will share the same database. If you plan to have separate databases for each component, consider naming the database after the component. For example, &quot;SBM Application Engine Database.&quot;</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User name</td>
<td>Enter the name of a privileged DBMS user account. Also known as the &quot;schema&quot; in Oracle.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For SQL Server databases, enter a SQL Server user account, not a Windows user account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the user's password.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Enter the password again to confirm.</td>
</tr>
<tr>
<td>Connection</td>
<td>After you have entered the connection information, you can test the connection to the database. If the test fails, review the information and make sure the database is online. You can also test the connection from an outside source like Microsoft's ODBC Data Source Administrator or Oracle's SQLPlus.</td>
</tr>
</tbody>
</table>

**About Data Sources**

Default data sources for the Application Engine and Common Log databases are provided by SBM. For new installations, **SBM_AE** is used for the Application Engine and **SBM_CL** is used for the Common Log database.

- **Application Engine Data Source**
  
  There are two data sources that are used to connect to the Application Engine database: the SBM Application Engine Web Server DSN, which you configure in SBM Configurator, and the SBM System Administrator DSN, which you configure in SBM System Administrator.
  
  **Tip:** If you are upgrading from SBM 10.1.3 or earlier, SBM Configurator will continue to use the **Mashup2009** for the Web server DSN after you upgrade. You can continue to use this DSN, or rename it at any time. If you change the Web server DSN in SBM Configurator, and you want the SBM System Administrator DSN to match, you must manually update the DSN in SBM System Administrator.

- **Common Log Data Source**

  The Application Engine server uses the Common Log data source to connect to the Common Log database. This enables you to use a dedicated ODBC connection for Application Engine to connect to the Common Log database using the connection parameters and security information that are required by your DBMS.

**Configuring Data Sources**

Click the **Change** that appears next to either data source to create, rename, or use an existing data source.
• To create a new data source with default settings, select **Create a new data source**, and then enter a new data source name. The new data source appears on the **Database Servers** tab.

• To rename the data source that is currently being used, select **Rename current data source**, and then enter a different data source name. The renamed data source appears on the **Database Servers** tab.

• To use an existing data source on the server instead of the default data sources that are provided by SBM, click **Select an existing data source**, and then select the existing data source from the **Data source name** drop-down list. The server will use this data source to connect to the database.

  **Important:** You must select the check box that appears below the drop-down list to preserve any custom settings in your existing data source.

  If you select an existing data source that uses an unsupported driver, SBM Configurator warns you about using the driver, and then automatically selects the check box and marks it as read-only in order to prevent any inadvertent changes to the data source.

### About Windows Authentication

For SQL Server installations, you can select the **Windows Authentication** check box to use a Windows user account of your choice to connect to SQL Server (instead of a SQL Server user account). You must ensure that this account can log in to SQL Server and that it has "dbo" permissions over all the tables in the database. This means that you must set SQL Server to allow **Windows Authentication** or both **Windows Authentication** and **SQL Authentication**. For details, refer to your SQL Server DBMS documentation.

**CAUTION:**

If you use **Windows Domain (NTCR)** to authenticate users, Windows authentication requires that your domain users have "dbo" privilege to the database. However, this presents a security risk to your system. Therefore, it is recommended that you clear the **Windows Authentication** check box in SBM Configurator and use **SQL Authentication** with **Windows Domain (NTCR)** instead.

If you select **Windows Authentication** in SBM Configurator, you do not need to enter database credentials in the **User Name** and **Password** columns. Instead, the SBM **Application Pool Identity** and the **Tomcat Log On Identity** are used to connect to the SBM databases.

• **Application Pool Identity** – By default, SBM uses the DefaultAppPool in IIS. The **Identity** specified in the DefaultAppPool is used to connect to the Application Engine database for Windows authentication. Note the following important information:

  • The default **Identity** for the DefaultAppPool is **NetworkService**. If you do not change the default **Identity**, then the **NetworkService** account is used to connect to the Application Engine database, and automatically granted the required Application Engine file system permissions once you click **Apply** in SBM Configurator.
If you want to use a different Windows user account, change the **Identity** from `NetworkService` to the desired account, and then click **Apply** in SBM Configurator. This grants the specified user account the required file system permissions.

If you change the default **Identity** in the DefaultAppPool, you must set the same identity in the gsoap application pool (`gsoap_pool`).

For steps on changing the default Identity, refer to **Modifying Application Pool Options** [page 152].

If you decide to create a new application pool for SBM, the **Identity** in that application pool is used for **Windows Authentication**.

If you install more than one instance of SBM Application Engine, you must ensure that the same Windows user account is specified in the application pool **Identity** on each server.

**Tomcat Log On Identity** – By default, the SBM Tomcat uses the Local System account. Similar to the DefaultAppPool identity, this account is used for Windows authentication unless you change it. Note the following important information:

- If you select **Windows Authentication**, the Local System account is used to connect to the Tomcat databases, and automatically granted the required Tomcat file system permissions once you click **Apply** in SBM Configurator.

- If you want to use a different Windows user account, change the Log On identity to the desired account, and then click **Apply** in SBM Configurator. This grants the specified user account the required file system permissions.

**To change the default Tomcat identity:**

1. Open the Windows Services Manager.
2. Right-click SBM Tomcat and select **Properties**.
3. Click the **Log On** tab.
4. Select **This account** and enter the Windows user account name.
5. Click **OK**.

For distributed installations, you must ensure that the same Windows user account is specified in the Log On tab in the SBM Tomcat service properties on each server.

After you click **Apply** in SBM Configurator, the default DSN (**SBM**) that is used to connect to the Application Engine database is automatically updated to use Windows authentication. If you decide to use a DSN other than the default, you must manually update that DSN to use Windows Authentication.

**Component Servers**

In the **Component Servers** tab, you define the distribution of the SBM server components and enter connection information for each server. You typically configure the **Component Servers** tab in **wizard mode** after you install SBM.
Initially, the **Component Servers** tab contains a single server definition (labeled *(this machine)*) with all of the SBM components listed. You can define additional servers by dragging and dropping SBM components on the design editor. Alternatively, you can right-click any component in the list and select **Move to new server**.

- **Distributing the SBM Server Components** [page 46]
- **Entering Server Connection Information** [page 46]

**Distributing the SBM Server Components**

When you run the SBM installer, all of the SBM server components are installed on the target machine. If you want all of the SBM server components to run on a single server, you can verify the default values in the **General** sub-tab and click **Next** to continue wizard mode.

However, if you want to create a distributed server installation (recommended), you must use the **Component Servers** tab to define additional servers and configure which components are enabled on each server.

**To configure a distributed installation:**

1. Select a component from the list.

2. Drag and drop the component on the design editor or right-click the component and select **Move to new server**.

3. Configure each server as described in **Entering Server Connection Information** [page 46].

When you drag a component to another server, that component is no longer configurable on the local server with the exception of the Notification Server and Mail Client components—these components can be installed and configured on multiple servers within the same environment. Note that when you attempt to drag either component, you are prompted to **Copy** it (which keeps a local copy and designates another copy on a separate server) or **Move** it (which removes the configuration from this server in favor of a remote server).

You might choose the **Move** option if you want to configure and run the Mail Client on a separate server from the Notification Server. You might choose the **Copy** option if you are defining your entire component distribution and you know that you want the Notification Server installed on two servers for failover purposes.

**Entering Server Connection Information**

After you finish distributing the server components in the editor, enter connection information for your local server and any additional servers you defined.
For each server that you define, provide the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the server host name. <strong>Restriction:</strong> The Orchestration Engine BPEL server host name cannot contain an underscore &quot;_&quot;. Only Latin characters (a-z and A-Z), digits 0-9, and hyphens are permitted, as described in RFC 952. Deployments will fail if the host name contains an underscore.</td>
</tr>
</tbody>
</table>
| Use HTTP on port| Select this check box to configure all SBM URLs to use HTTP. The current HTTP ports that are used by IIS and Tomcat appear for informational purposes.  
If you select this option, all SBM components on this server are only accessible using HTTP. Select only the HTTP check box to force all traffic to use HTTP.  
**CAUTION:**  
If you set the **Require Secure Channel** property on the **gsoap** extension in IIS, you must ensure that **Use HTTP** is not selected. |
| Use HTTPS on port| Select this check box to configure all SBM URLs to use HTTPS. The current HTTPS ports that are used by IIS and Tomcat appear for informational purposes.  
If you select this option, all SBM components on this server are only accessible using HTTPS. Select only the HTTPS check box to force all traffic to use HTTPS. |
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use IIS to proxy all server requests           | Select this check box to have IIS proxy all server requests in SBM. This forces all SBM traffic through IIS on port 443 and disables all Tomcat HTTP connectors (8085, 8243, 8343, 8443). Note that if you enable this feature, you must update the following to use port 443:   
  • Endpoints in deployed process apps          
  • Target servers                               
  • Bookmarked URLs                              
  • Client certificate authentication settings (if already configured)                             
  • SmartCard authentication settings            
  After you have updated your target servers and endpoints, you must re-deploy your process apps.  
  **Important:** In addition, you must ensure that the WebDav module in IIS has been removed under Common HTTP Features. This module blocks important HTTP requests that are used by SBM when IIS is used to proxy server requests. |
| Join cluster as a node                         | Select this check box to add this server as a node to a Tomcat or Application Engine cluster. When you select this option, the server group box in the design editor changes from a server to a cluster. For details, see Clustering Server Components [page 49]. |
| TCP port                                       | If SBM Logging Services is on a separate server, enter the TCP port for the Active Diagnostics database (powered by MongoDB) on that server. The default port value is 27017.                                               |
| Beyond firewall                                | Select this check box to configure the external host name and HTTP or HTTPS settings for this server if it is located outside your company's firewall.  
  **Important:** If this server is located outside the firewall, you must enter the External Host name in order for users to access the server. The host name that you enter is the same host name that your users will use to access the server externally.  
  Because the host name and port values for the firewall cannot be detected by SBM Configurator, you must enter valid port numbers manually. The port values that you enter here are dependent on your current firewall settings. Consult your firewall administrator to determine the port values that should be used in combination with the external server host name.  
  These port values are completely independent from the port values that you enter on the following IIS Server and Tomcat Server tabs in SBM Configurator. |
If you select both the **Use HTTP** and **Use HTTPS** check boxes, this preserves the current HTTP or HTTPS configuration of all the URLs in your installation and no changes are made to their current configuration (except for port values you might have set after selecting **Beyond firewall**). Select both check boxes if you have previously manually configured some URLs to use HTTP and some URLs to use HTTPS. By default, both options are selected if you are installing and configuring SBM for the first time.

After you click **Apply**, SBM Configurator verifies the connection information for your local server. If SBM Configurator is unable to reconcile the host name or IP address that you provided with the host name or IP address of the local machine, SBM Configurator prompts you to select which host name represents your local server. Alternatively, you can click the **Select local host** link that appears to specify which machine is the local host.

For example, if you have a distributed installation that uses a load balancer, the host name you enter that corresponds to the load balancer will not match the host name or internal IP address of the local server. In that case, you must confirm which host name represents your local server. In this scenario, you must specify which host name represents the local machine.

### Clustering Server Components

If you plan to create a cluster, Serena recommends that you read this section in its entirety, and then create a schematic to help you organize and plan your system layout and configuration.

- About Clusters [page 49]
- Using Load Balancers [page 49]
- Installation and Configuration Considerations [page 50]
- Creating a Cluster [page 51]

### About Clusters

Establishing one or more SBM clusters provides several benefits to your SBM installation.

- Creating a cluster for SBM Application Engine provides failover in the event one of the servers in your installation fails or loses connection.

- Clustering SBM Orchestration Engine can provide greater scalability for the orchestrations that you create in SBM Composer.

- Using a cluster can improve the overall performance and load handling of SBM.

For example, you can use SBM Configurator to create an Application Repository cluster, where each Application Repository server is an individual node in the cluster that is connected to the same Application Repository database. Multiple users can access the Application Repository cluster, with each request routed to one given Application Repository instance using either a software or hardware load balancer.

### Using Load Balancers

The load balancer has knowledge about the health of the configured servers in the cluster. If one of the servers goes down, the load balancer sends requests to the other servers in the cluster.
Load Balancer Requirements in a Tomcat Cluster

You can use either a software or hardware load balancer, though Serena typically recommends using a hardware load balancer due to better support, statistics, and overall performance. For uninterrupted service, the load balancer should be configured to ensure that sessions are "sticky" or persistent. This ensures that the same HTTP session is always delegated to the same machine, as state information resides on only one Application Repository server. The load balancer can then delegate different sessions to different servers so that multiple sessions can run on different servers.

For more details on configuring your load balancer with a Tomcat cluster, refer to solution S140260.

Load Balancer Requirements in a Application Engine Cluster

In an Application Engine cluster, the load balancer requires session persistence via the "Node Lock" option (also called "Server Affinity" and "Persistence" depending on the load balancer). This option ensures that once a user is directed to a server, they are continuously directed to that server unless there is a long period of inactivity or the server goes down. Data loss can occur if the Node Lock option is not used, in addition to an over consumption of licenses (1 per server that is connected to).

You also need to ensure that the load balancer is configured to properly identify the client. When SBM receives a network packet, it initially scans for X-FORWARDED-FOR: client1, proxy1, proxy2 in the header. If SBM cannot find this header, it uses the source IP address from the packet header instead. A packet that is sent from a load balancer or proxy will contain the load balancer or proxy server's address and not the client address; therefore, you must configure the load balancer header settings to include X-FORWARDED-FOR as SBM expects.

For more details on configuring your load balancer with an Application Engine cluster, refer to solution S138266.

Installation and Configuration Considerations

Review the following important considerations before you configure a cluster.

- You will run the SBM installer on each server that will join the cluster as a node. When the installer is finished, you will use the Component Servers tab on one of the servers to create the cluster and define the nodes.

- The method you use to configure the cluster depends on the following:
  - If you are using the Configuration Settings database (recommended), the entire configuration is saved in a single database and all servers should be in sync. This means after you have installed SBM on each server, you can configure the entire cluster from one server, and then click Update From Database on each server to have them join the cluster as a new node with all the settings that you defined.
  - If you are using configuration snapshots instead of the Configuration Settings database, enter all the configuration information in SBM Configurator on one server (pre-defining all node number and host name pairings at the same time), and then export the data into a snapshot configuration file using the System Settings tab. Once the snapshot is created, import it into SBM Configurator on each server that will become a node in the cluster. This ensures that each server is configured exactly the same.
• There are multiple clustering options available, depending on the number of components that you want to cluster and the number of clusters you want to create. For example:
  ▪ You can create a single cluster for a single Tomcat component (for example, SBM Orchestration Engine).
  ▪ You can create a single cluster for multiple Tomcat components (for example, SBM Orchestration Engine and SBM Mail Services together).
  ▪ You can create multiple clusters each comprised of a single Tomcat component or multiple clusters each comprised of multiple Tomcat components. In either scenario, you must enable the same Tomcat components on each node in the cluster.
  ▪ You can create a single cluster for SBM Application Engine or combine it with Tomcat components in a mixed cluster.

• You will typically create a cluster that contains either a set of Tomcat nodes or a set of SBM Application Engine nodes. If you have nodes with both SBM Application Engine and Tomcat components in one cluster (mixed), you must ensure that the load balancer is configured properly to redirect requests to the correct IIS or Tomcat ports in the cluster (unless you decide to have IIS proxy all server requests, in which case only the IIS ports are used).

• Ensure that you have dedicated servers that meet the minimum hardware requirements as specified in Hardware Requirements [page 15].

• Consult with your network administrator, and ensure that UDP multi-casting is available between all nodes in the cluster. In other words, ensure that all nodes in the cluster exist in a common subnet that supports UDP multi-casting.

• For correct results, you must ensure that the clocks on all the servers are synchronized within one second.

Creating a Cluster
To create one or more clusters, perform the following steps on each server that will join the cluster as a node:

1. On the Component Servers tab, drag and drop one or more SBM components that you intend to cluster to an empty space in the design area. This creates a temporary server definition that represents the entire cluster.

2. Click the new server definition that you just created in the design area.

3. In the General sub-tab, select Join cluster as a node. Enter the following details:
4. On the **Load Balancer** tab, enter the following information:

- **Internal load balancer**

  Used by nodes that are inside the firewall.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select HTTP or HTTPS, depending on which protocol your load balancer is configured to use.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the host name for the internal load balancer.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number that is used to access the nodes through the load balancer.</td>
</tr>
</tbody>
</table>

- **External load balancer**

  Used for connections from outside the firewall.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select HTTP or HTTPS, depending on which protocol your load balancer is configured to use.</td>
</tr>
</tbody>
</table>
### Field Name | Description
--- | ---
Host | Enter the server host name that all incoming requests should use.
Port | Enter the port number that is used to access the nodes through the load balancer.

**Important:** After you enter load balancer details for a Tomcat cluster, you must log in to SBM Application Repository, edit the host environment, and update the target server endpoints with the load balancer host and port information that you entered in SBM Configurator. When you are finished, redeploy your process apps to this environment.

5. On the **Nodes** tab, enter the following information:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 Host</td>
<td>Enter the host name of the first node that you add to the cluster. Click <strong>Add Node</strong> to define additional nodes or <strong>Remove Node</strong> to delete this node from the cluster.</td>
</tr>
<tr>
<td>Node 2 Host</td>
<td>Enter the host name of the second node that you add to the cluster. Click <strong>Add Node</strong> to define additional nodes or <strong>Remove Node</strong> to delete this node from the cluster.</td>
</tr>
</tbody>
</table>

After you have added at least one other node, continue to add nodes for each server that will join the cluster as a new node. You must replicate the same node number and host name pairing on each server in the cluster. For example, if you create the following node number and host name pairing on Server A:

<table>
<thead>
<tr>
<th>Node</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 host:</td>
<td>Server A</td>
</tr>
<tr>
<td>Node 2 host:</td>
<td>Server B</td>
</tr>
<tr>
<td>Node 3 host:</td>
<td>Server C</td>
</tr>
</tbody>
</table>

You must enter the same pairing on the **Nodes** tab on Server B and Server C:

<table>
<thead>
<tr>
<th>Node</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node 1 host:</td>
<td>Server A</td>
</tr>
<tr>
<td>Node 2 host:</td>
<td>Server B</td>
</tr>
</tbody>
</table>
If you remove a node, the following node becomes the node number that you just removed. For example, if you remove node 2 (Server B), then Server C becomes node 2. This means you must update each server again with the correct node number and host name pairing.

6. On the Ehcache tab, review the Ehcache information to ensure each cluster that you configure has a unique subnet address and that there are no port conflicts on the server. You must ensure each cluster is assigned a unique address to avoid problems with identifying clusters if they are in the same subnet.

7. To finish, verify the information on each server that will become a node in the cluster—the same configuration information and the same node number and host pairings should appear for each node that exists in the cluster.

**IIS Server**

In the IIS Server tab, you designate a Web site to host the SBM Application Engine Web server components and configure the ports it will use. You configure the IIS Server settings in either wizard mode or utility mode on the server where you installed the SBM Application Engine component.

If you change any IIS settings while SBM Configurator is open, you must close and reopen SBM Configurator in order to update it with the latest changes that you made in IIS.

If users experience problems accessing SBM, verify and Apply settings in SBM Configurator on the IIS server, and then refer to Chapter 8: Troubleshooting [page 151] for further assistance.

- Web Site Settings [page 0]
- Configuring SSL [page 56]
- Managing Trusted Certificates [page 57]
- Other Settings [page 58]
Web Site Settings
To configure IIS Web site settings, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Application Engine Web site   | Select an IIS Web site in the drop-down list. The **Default Web Site** is selected by default. After you select a Web site and click **Apply**, SBM Configurator performs the following tasks:  
  • Creates the workcenter application in IIS, which hosts Serena Work Center.  
  • Creates the tmtrack application in IIS, which hosts SBM User Workspace.  
  • Creates the gsoap application in IIS, which hosts the SBM Application Engine Web services WSDL.  
  • Creates the sbmconnector application in IIS, which hosts the REST Grid and PDF widgets.  
  • Creates the necessary ISAPI filters for SBM Application Engine to communicate with SBM Common Services.  
  • Sets file system permissions for the Network Service and IUSR accounts and grants access to the SBM Application Engine folder and its sub-folders.  
  • Grants permission to the necessary ISAPI extensions.  
  • Configures the tmtrack and gsoap application pools to use the recommended identity, number of worker processes, and idle timeout. SBM Configurator adjusts the idle timeout and number of worker processes if the recommended settings are not currently used. |
| Web site HTTP port            | Define the HTTP port for the Web site that you selected. This updates the Web site in IIS with a new binding, which means you do not have to open IIS to change the Web site's port value. |
| Web site HTTPS port           | Define the HTTPS port for the Web site that you selected. This updates the Web site in IIS with a new binding, which means you do not have to open IIS to change the Web site's port value. |
### Configuring SSL

You can configure SSL in IIS by generating a new certificate from a well-known certificate authority (CA) or a self-signed certificate generated by your own CA. You can also manage the current SSL configuration by removing or selecting existing SSL certificates.

Before you can configure SSL for IIS, you must specify an HTTPS port in the **Web site HTTPS port** field.

The **IIS Server** tab only appears when you run SBM Configurator on the SBM Application Engine server. If you want to secure end-user connections to IIS in a distributed server environment, you must configure SSL settings on the SBM Application Engine server. Additionally, if you choose to enable SSO, you can secure connections from the browser into the SSO Security Server by selecting **Use HTTPS for SSO login** on the **Security** tab. For details, refer to Securing SSO [page 122].

To configure SSL, use the following options:

- **Generate Sample Certificate**

  Creates a new SSL certificate that is based on a sample CA certificate (**Serena Sample CA-2**) installed with SBM. For example, if you have not yet purchased a certificate from a well-known certificate authority (CA), select this option to temporarily secure IIS with a sample certificate.

  - In the **Generate Certificate** dialog box that appears, you can accept the default values to create a new sample certificate with a common name that matches the local server's hostname. By default, the sample certificate is signed by the **Serena Sample CA-2** CA, but you can import and use a different CA cert if necessary.

  - If you clear the **Certificate authority** check box, SBM Configurator generates a self-signed certificate. You can configure additional parameter including the public key size, validity dates, and signature algorithm as needed.

  - You must confirm that you want to add the **Serena Sample CA-2** CA certificate to the Windows truststore (if is not detected there already). This operation deploys the sample CA certificate to the local Windows truststore (which creates a trust for any certificates that are henceforth generated by this CA certificate).

  - Once you click **Yes**, SBM Configurator creates a new SSL certificate (using the sample CA certificate that you just deployed), and imports the new certificate into IIS, which associates it with selected Web site. The newly-generated certificate’s...
common name is generated using the server’s host name. You can view the certificate details in SBM Configurator or in the Web site properties in IIS.

- After the certificate is created, you can export the public key and import it into a third party keystore to establish a trust. To export the certificate, click View more details, select the Details tab, and click Copy to File. Complete the export wizard that appears to generate a DER-encoded certificate.

- Import New Certificate
Imports a well-known or self-signed certificate (in PEM format, which is a base64-encoded DER). For example, if you have purchased a certificate from a well-known CA, select this option to have SBM Configurator import the certificate for you. This operation adds the new certificate to the Windows keystore, imports the certificate into IIS, and associates the certificate with the Web site that is selected in the Web site drop-down list.

- SBM does not support using certificates that contain wildcards.

- If you configure your server for Smart Card authentication, there are restrictions when configuring SSL. Specifically, if you replace the server SSL certificate with a self-signed server certificate, you must create the self-signed certificate using the RSA algorithm. The SSL handshake fails when using a self-signed DSA certificate in earlier FireFox browsers. This is not an issue for Internet Explorer browsers.

- Export Current Certificate
Launches the Export dialog box, from which you can: export the certificate and optionally the private key; export the entire certificate chain plus the certificate; export just the chain without the certificate. Note that the certificate path options are disabled if you are using a self-signed certificate.

- Select Existing Certificate
Selects an existing certificate from the Windows keystore to secure IIS. For example, if you need change the current certificate that is installed, use this option to select an alternative certificate from the keystore. This operation replaces the current certificate (if one is installed) with the certificate that you select.

- Remove Current Certificate
Removes the current certificate from IIS. For example, if the server's hostname changes (which invalidates the current certificate), you use this option to disassociate the current certificate from IIS. This operation disassociates the current certificate from the Web site that is selected in the Web site drop-down list and also provides you the option to remove the certificate from the keystore.

- If you select Yes, the certificate is removed from IIS and the keystore.
- If you select No, the certificate is removed from IIS, but not the keystore. To secure IIS again with an alternative certificate, you can either generate, import, or select a different certificate.

Managing Trusted Certificates
Click Manage Trusted Certificates to launch the Certificates dialog box. This enables you to search for trusted certificates, as well as import, export, or remove trusted certificates from the truststore. In the Certificates dialog box, you can:
• **Import Certificates** – Imports a trusted certificate into the truststore.

• **Export Certificates** – Exports a trusted certificate.

• **Remove Certificates** – Removes one or more selected certificates.

• **View Details** – Select a certificate and click View Details to see more information.

Use the search field to find a certificate in the truststore. You can search for certificates by using any of the details that are listed in the **Certificates** dialog box.

To execute an external Web service call from SBM using SSL, the SBM certificate truststore must contain the external service's public certificate (in the event that the certificate does not already exist in the truststore). Therefore, you must import the service's public certificate into either the Windows or Tomcat truststore—depending on which SBM component performs the call.

For example, if the external Web service call is invoked from a workflow transition, you must add the public certificate to the Windows truststore in the IIS tab on the IIS server. This ensures that SBM Application Engine calls are trusted by the external service. Similarly, you must add the public certificate to the Tomcat truststore to ensure that SBM Orchestration Engine calls are trusted by the external service. For example, if you create an SBM orchestration that contains an external Web service call that is secured by SSL, the public certificate for that service must be added to the Tomcat truststore. The truststore may already contain some public certificates, but if you create your own certificates or use certificates that are newer than those the truststore, the truststore must be updated to successfully complete calls over HTTPS.

**Other Settings**

SBM Configurator also displays the following Application Engine settings:

• **Application pool name** – This is the Application Pool that is assigned to the tmtrack application in IIS. SBM Application Engine powers the runtime environment using this memory space.

• **Application pool identity** – This is the name of the account under which the application pool's worker process runs. By default, application pools operate under the Network Service account, which has low-level user access rights.

• **Number of worker processes** – Should always have a value of "1". This values denotes a single worker process for the application, which disables the Web garden feature. This keeps concurrent licenses from being consumed multiple times by one user session.

• **Recycle worker processes (in minutes)** – This setting is disabled by default. If enabled, IIS will periodically restart. This not only forces an IIS restart at a potentially inconvenient time, but also causes problems for installations that use Single Sign-On (SSO).

• **Idle timeout (in minutes)** – This setting is disabled by default. If enabled, the IIS worker process is shutdown after a specified period of inactivity. This forces IIS to re-cache all the templates and images again, which impacts users on subsequent attempts to access the system.

• **Virtual directory authentication** – This setting denotes the current authentication methods that are selected in the tmtrack and gsoap applications in IIS.
Tomcat Server

In the Tomcat Server tab, you designate ports for the local Tomcat server components and optionally configure Tomcat to use SSL. You configure the Tomcat Server settings in either wizard mode or utility mode on the servers that host the Tomcat server components.

- Server Settings [page 59]
- Configuring SSL [page 59]
- Managing Trusted Certificates [page 61]
- Advanced Settings [page 61]

Server Settings

To configure your Tomcat server, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Connector port</td>
<td>Enter the HTTP connector port that Tomcat will use on this server. If you clear the port value, the connector is no longer used.</td>
</tr>
<tr>
<td>HTTPS Connector port</td>
<td>Enter the HTTPS connector port that Tomcat will use on this server. If you clear the port value, the connector is no longer used.</td>
</tr>
<tr>
<td>HTTPS client certificate port for Smart Card authentication</td>
<td>Enter the HTTPS port that will be used for client certificate authentication, which is used for Smart Card authentication in SBM.</td>
</tr>
</tbody>
</table>

**Note:** The HTTP and HTTPS ports affect the URL that is used to log in to Application Repository. If you change these ports, you will need to notify SBM Composer users.

Configuring SSL

You can configure SSL for Tomcat by generating a sample certificate or importing a new certificate from a well-known certificate authority (CA) or a self-signed certificate generated by your own CA. You can also manage the current SSL configuration by selecting an existing SSL certificate. If SSO is enabled, this creates a secure communication channel between the browser and the SSO Security Server.

The Tomcat Server tab only appears when you run SBM Configurator in utility mode on servers that hosts Tomcat components. If you want to enable SSL in a distributed server environment, you must run SBM Configurator on each Tomcat server and configure these settings.

To configure SSL, use the following options:

- **Generate Sample Certificate**
  Select this option to create a new certificate that is based on the sample CA certificate Serena Sample CA-2 that is installed with SBM. For example, if you have
not yet purchased a certificate from a well-known certificate authority (CA), select this option to secure Tomcat with a sample certificate.

- In the **Generate Certificate** dialog box that appears, you can accept the default values to create a new sample certificate with a common name that matches the local server's hostname. By default, the sample certificate is signed by the **Serena Sample CA-2** CA, but you can import and use a different CA cert if necessary.

- If you clear the **Certificate authority** check box, SBM Configurator generates a self-signed certificate. You can configure additional parameter including the public key size, validity dates, and signature algorithm as needed.

- The newly-generated certificate and the CA certificate that was used to generate the sample certificate are placed in the local Tomcat keystore and truststore, respectively. If an existing certificate is found, SBM Configurator provides you with the option to remove it from the keystore.

- Once the certificate has been created, you can export the public key and import it into a third party keystore to establish a trust. To export the certificate, click **View more details**, select the **Details** tab, and click **Copy to File**. Complete the export wizard that appears to generate a DER-encoded certificate.

**Import New Certificate**

Select this option to import a well-known or self-signed certificate (in PEM format, which is a base64-encoded DER). For example, if you have purchased a certificate from a well-known CA, select this option to have SBM Configurator import the certificate for you. This operation adds the new certificate to the Tomcat keystore.

- SBM does not support using certificates that contain wildcards.

- If you configure your server for Smart Card authentication, there are restrictions when configuring SSL. Specifically, if you replace the server SSL certificate with a self-signed server certificate, you must create the self-signed certificate using the RSA algorithm. The SSL handshake fails when using a self-signed DSA certificate in earlier FireFox browsers. This is not an issue for Internet Explorer browsers.

**Export Current Certificate**

Launches the **Export** dialog box, from which you can: export the certificate and optionally the private key; export the entire certificate chain plus the certificate; export just the chain without the certificate. Note that the certificate path options are disabled if you are using a self-signed certificate.

**Select Existing Certificate**

Select this option to select an existing certificate from the Windows keystore to secure Tomcat. For example, if you need change the current certificate that is installed, use this option to select an alternative certificate from the keystore. This operation replaces the current certificate (if one is installed) with the certificate that you select.

**Change Keystore Password**

Select this option to change the default Tomcat SSL keystore password. Changing the default password updates the SSL keystore and certificates with a password of your choice, which improves security.
To update the default password:
1. Click **Change Keystore Password**.
2. A window appears and displays the current password. (The default is *serena*).
3. Enter a new password and click **OK**.
4. Click **Apply**.

**Managing Trusted Certificates**

Click **Manage Trusted Certificates** to launch the **Certificates** dialog box. This enables you to search for trusted certificates, as well as import, export, or remove trusted certificates from the truststore. In the **Certificates** dialog box, you can:

- **Import Certificates** – Imports a trusted certificate into the truststore.
- **Export Certificates** – Exports a trusted certificate.
- **Remove Certificates** – Removes one or more selected certificates.
- **View Details** – Select a certificate and click View Details to see more information.

Use the search field to find a certificate in the truststore. You can search for certificates by using any of the details that are listed in the **Certificates** dialog box.

To execute an external Web service call from SBM using SSL, the SBM certificate truststore must contain the external service’s public certificate (in the event that the certificate does not already exist in the truststore). Therefore, you must import the service’s public certificate into either the Windows or Tomcat truststore—depending on which SBM component performs the call.

For example, if the external Web service call is invoked from a workflow transition, you must add the public certificate to the Windows truststore in the IIS tab on the IIS server. This ensures that SBM Application Engine calls are trusted by the external service. Similarly, you must add the public certificate to the Tomcat truststore to ensure that SBM Orchestration Engine calls are trusted by the external service. For example, if you create an SBM orchestration that contains an external Web service call that is secured by SSL, the public certificate for that service must be added to the Tomcat truststore. The truststore may already contain some public certificates, but if you create your own certificates or use certificates that are newer than those the truststore, the truststore must be updated to successfully complete calls over HTTPS.

**Advanced Settings**

Configure Tomcat Server **Advanced Settings** in the event that you need to override the maximum HTTP header size for SBM Tomcat requests and responses. Tomcat allocates two buffers with the `maxHttpHeaderSize` per request, which can create out-of-memory problems when SBM Tomcat is handling heavy server traffic. If users are experiencing 400 errors from Tomcat, consider increasing the maximum HTTP header size as appropriate.

For systems that are configured to use Windows Domain authentication with SSO, SBM Configurator automatically doubles the default maximum HTTP header size from 8192 bytes to 16384 bytes.
License Server

In the License Server tab, you configure license server settings for SBM. You configure license settings in utility mode after your database has been initialized.

**Important:** For new installations, the License Server settings are not saved in the Application Engine database until after you run the Create Database Wizard in SBM System Administrator. After you run the wizard and successfully create the database, use SBM Configurator to enter your License Server settings.

Provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use evaluation license</td>
<td>Select this option if you do not currently have licenses, but want to evaluate SBM. SBM Configurator displays the number of days that remain in your evaluation period.</td>
</tr>
<tr>
<td>Use license manager</td>
<td>Select this option to use license keys that you have purchased, and then enter the following information.</td>
</tr>
<tr>
<td>Server</td>
<td>Enter the hostname or IP address of the server on which Serena License Manager is installed. To specify a port number for the server, use the @ symbol before the host name. For example, if your license server uses port 81, enter 81@license server name.</td>
</tr>
<tr>
<td>Override for this machine</td>
<td>Select this option if your system uses multiple license servers and you want to override the license server for a specific SBM Application Engine Web Server. When the check box is cleared, the license server host name applies to all Web servers.</td>
</tr>
</tbody>
</table>

You can specify multiple host names separated by a semi-colon to establish license server redundancy (in case one license server is shut down or fails). For example, you can concatenate server names in this format:

```plaintext
licenseServer1;licenseServer2
```

If `licenseServer1` should fail, then licenses from `licenseServer2` would still be available.

**Important:** Concatenating license server host names for redundancy purposes fails if your license server is not running on the default port. This means you can not specify an alternate port before the host name (such as `7000@licenseServer1;7000@licenseServer2`). Therefore, do not concatenate license server host names if you are not using the default port.

Additional licensing information including the database identifier (which is used to confirm whether or not a copied database is identical to another database) and license usage logging settings are available in the License Options tab in SBM System Administrator.
Authentication

In the Authentication tab, you configure SBM authentication settings. You can configure authentication settings in utility mode after your database has been initialized.

Important: For new installations, the Authentication settings are not saved in the Application Engine database until after you run the Create Database Wizard in SBM System Administrator. After you run the wizard and successfully create the database, use SBM Configurator to configure your Authentication settings.

If your installation uses multiple Web servers with different authentication settings for each server, select the Override authentication settings for this server check box and configure the authentication settings for your local server. Clear the check box if all servers will use the same authentication settings.

General Settings

In the General Settings tab, you configure the following authentication settings.

- Browser Sessions [page 63]
- Browser Authentication [page 63]
- Authentication Sources [page 64]
- User Session Time-Out [page 65]
- Enable Login Form [page 66]

Browser Sessions

To begin configuring SBM authentication, select the method SBM will use to manage user sessions.

- Single Sign-On (SSO)
  
  SSO enables users to provide their login credentials once, receive a security token in return, and then use this token again to access other SSO-enabled tools without logging in again. Because SSO offers a single point of access to SBM that enhances the end-user experience, consider selecting this option to manage SBM user sessions. For more information, refer to About Single Sign-On (SSO) [page 66].

- SBM Session Cookies
  
  Optimizes the performance of log in and log out features and is recommended for browsers that support cookies.

  - If you select one of the LDAP authentication options and SBM Session Cookies to manage sessions, select the Allow legacy access check box to allow access for the SBM API. Enter your domain name on the Windows Domain tab.

  - You must select Allow legacy access if you use integrations, such as SourceBridge, or to allow connections for other programs that use the SBM API.

Browser Authentication

After you determine how SBM will manage user sessions, select which option to use to obtain browser user credentials.
• **SBM Login Form**
  Displays a login form in the Web browser to gather user credentials.

• **Windows Authentication**
  Credentials of the user logged in to the workstation are used to log in automatically.
  Note the following important information about using Single Sign-On with Windows Authentication:
  • If you select Single Sign-On with Windows Authentication, you must configure your authentication settings on the Single Sign-On (SSO) server in order for SBM Configurator to successfully update the SSO configuration files.
  • Select the Enable Login Form check box to display a login page if user validation fails.

• **Third Party Authentication System**
  Browser user credentials are collected and authenticated by a SAML2 identity provider or another identity management system. You will configure additional settings on the External Identity Provider tab that appears.

• **Smart Card Login**
  Enables users to log in using Smart Cards. To set up Smart Card authentication, you must configure how authentication is handled and how user identities are managed on the Custom Authentication tab. For details, refer to Custom Authentication Settings [page 80].
  Optionally, select Do not use login form on first login attempt if you do not want users to view a login form and have to click the Smart Card Login button on their first login attempt.

When you select either Windows Authentication or Third Party Authentication System, browser users are validated externally and logged in automatically without a login form. In the following section, you will determine which authentication source to use for validating Web service and API calls in these scenarios.

**Authentication Sources**

Finally, select the authentication source that SBM will validate credentials against. If you selected Windows Authentication or Third-Party Authentication System to collect identities, this selection determines how Web service calls and connections from the SBM API are authenticated.

• **Internal SBM Database**
  Uses SBM login IDs and internal SBM passwords to authenticate users.

• **LDAP**
  Validates users against LDAP using SBM Application Engine.

• **LDAP then Internal**
  Validates users against LDAP using SBM Application Engine first, and then against the internal SBM database if the user is not found in LDAP.

• **SSO LDAP**
Validates users against LDAP using SSO.

- **SSO LDAP then Internal**
  Validates users against LDAP using SSO first, and then against the internal SBM database if the user is not found in LDAP.

- **Windows Domain**
  Uses the Windows security system for authentication. User login IDs and passwords are authenticated against your Windows domain.

  The domain that is used for validation differs as follows depending on the session management option that you select:

  - If you select **Single Sign-On** to manage sessions, domain user IDs and passwords are validated against the domain of the SSO machine for browser authentication requests. Domain user IDs and passwords are validated against the domain of the IIS machine for Web service calls that do not have a security token.

  - If you select **SBM Session Cookies** to manage sessions, domain user IDs and passwords are validated against the domain that you specify on the **Windows Domain** tab. If you do not provide a domain, the domain that the IIS server is installed on is used.

**CAUTION:**

When users are logged in automatically by using either **Windows Authentication** or a **Third-Party Authentication System** for browser authentication, selecting **Internal SBM Database** for Web services authentication potentially allows users to:

- Access the repository from SBM Composer by specifying only the login ID with no password
- Log in to SBM Application Repository by specifying only the login ID with no password
- Make SBM Web service calls by specifying only the login ID and no password

By default, users in SBM are created without a password, which means any user that has not explicitly changed his or her password can log in by specifying a blank password. Therefore, either consider using SSO instead of session cookies or set passwords in SBM for every user.

**User Session Time-Out**

Depending on the authentication source and session management options that you select, you can optionally designate a **User session time-out** period.
This setting forces users to re-authenticate if they have not actively used the system for a specified number of minutes. Enter a positive integer to have SBM automatically log out users who are inactive for the specified number of minutes. This feature does not apply when browser user identities are collected via Windows Authentication.

**Note:** The User session time-out setting is unrelated to licensing. Rather, you use the User session time-out setting to enhance the security of your system. This setting prevents data from inadvertently being exposed in end-user interfaces for an indefinite period of time.

When this setting is enabled, the Web client polls the server once a minute to determine if the configured timeout has been exceeded. If no activity has occurred in the browser and the configured timeout has been exceeded, the client disconnects the session and returns a message that indicates that the session has timed out. If the timeout is exceeded and the user attempts to make a change in the browser before the next polling period after the timeout period has lapsed, then the session is immediately disconnected and the user is prompted to log in again.

If the connection to the server is lost or the server cannot be reached, the existing session is automatically disconnected after the first unsuccessful poll between the client and the server. Note that any data that is entered in a transition form that is not completed when the session timeout occurs is lost and will need to be re-entered in the transition form again when the user logs back in.

**Enable Login Form**

If you are not using the SBM Login Form option, select the Enable Login Form check box to display a login page if user validation fails with Windows Authentication, Third-Party Authentication, or Smart Cards. Clear the check box if you do not want the page to appear.

**About Single Sign-On (SSO)**

Single Sign-On (SSO) enables users to log in to a Web-based component of SBM and be recognized on subsequent connections to that component or other Web-based components in SBM.

Additionally, SSO enables users with a valid e-mail address to request a password change from the SSO login page. After users request a password change, responses are sent to their e-mail address by the Notification Server.

You can modify SSO security settings on the Security tab. For details, refer to Securing SSO [page 122].

The following sections provide detailed information about the SSO framework.

- Why Use Single Sign-On (SSO)? [page 66]
- Single Sign-On (SSO) Components [page 67]
- Customizing the SSO Login Page [page 68]

**Why Use Single Sign-On (SSO)?**

Single Sign-On (SSO) provides several benefits to your SBM system. This section describes why you should consider using SSO.

- **SSO offers a seamless integration**
SSO makes it possible for users to provide their login credentials once, receive a security token in return, and then use this token again to access other SSO-enabled tools without logging in again. SSO offers a single point of access to SBM, which enhances the end-user experience.

- **SSO is a standards-based solution for interoperability**
  SSO is a secure solution for interoperability that is based on the following well-established industry standards:
  - WS-Trust
  - WS-Federation Passive Requestor Profile
  - WS-Security

  The SSO framework relies on these standards and the use of a SAML 1.1 token to convey user identity information between the various components in an SBM environment. Because SSO is based on proven standards, the solution is both secure and reliable. These standards have been adopted across the industry, which makes the solution interoperable with other products.

- **SSO offers integrations with third-party authentication systems**
  You can configure SSO to work with third-party authentication methods such as NT Challenge Response. You might decide to enable SSO and use it in combination with a third-party authentication system if you want to seamlessly integrate SBM with other products.

- **Smart Card authentication**
  SBM can be configured to authenticate users through Smart Cards that utilize the Single Sign-On (SSO) framework. Smart Card authentication is a secure and reliable authentication method that allows users who have a current Smart Card (containing valid certificates and identity information) to gain access to a Smart Card-enabled SBM system once the proper PIN is provided.

**Single Sign-On (SSO) Components**

SSO includes the following components:

- **Gatekeeper**
  The Gatekeeper is a servlet filter that rejects incoming messages that lack proper user credentials. The Gatekeeper acts an agent that sits in front of Application Repository and SBM Application Engine (each has its own gatekeeper), allowing requests to pass through if they have the proper authentication, or rejecting them if they do not.

- **Security Server**
  The Security Server (also known as the Identity Provider or "IDP") presents a login page that requests credentials. Every login request comes through the Security Server to challenge the user for credentials.

  The Security Server also receives requests for security tokens and issues them if the requesting user is properly authenticated. The Security Server generates and signs security tokens (also known as SAML tokens) with its own private key for
authenticated users. There are two entities within the Security Server: the Identity Attribute Service (IDAS) and the Context Provider.

- **Identity Attribute Service (IDAS)**
  
The Identity Attribute Service is an abstraction layer that contacts the authentication source (in conjunction with the Context Provider) to authenticate a user’s credentials and return verification to the Security Server. The IDAS allows the Security Server to operate with identity stores on a high level, so that the Security Server does not have to know a particular LDAP directory and its structure or the SBM Application Engine and its structure.

- **Context Provider**
  
The Context Provider is an adapter to an authentication source, such as an LDAP directory. The authentication source could be LDAP or SBM internal passwords within the SBM Application Engine database. SBM supplies LDAP and SBM Application Engine context providers as part of the installation.

- **Identity Store**
  
The Identity Store is the actual LDAP directory or database that holds the user identity (ID and password).

**Customizing the SSO Login Page**

You can customize the SSO login page to notify users of upcoming system maintenance. Edit the `loginnotice.jsp` file in the following location.

```
installDir\Common\Tomcat 7.0\server\default\webapps\idp\jsp
```

Insert HTML in the following section to notify your users:

```
<%-- Insert HTML here to display a notice on the SSO login page
Example:
<div align="center" style="padding-top: 55px;">
  <div class="title-error">System Unavailable Tonight</div>
  <table>
    <tr>
      <td class="header" style="padding-bottom: 18px; padding-top: 15px;">
        The system will be down at 5PM PST for maintenance.
      </td>
    </tr>
  </table>
</div>
--%>
```

**Tip:** It is not necessary to restart SBM Tomcat after saving your changes.

**About Windows Domain Authentication**

*Windows Domain* authentication relies on the Windows network security system for SBM authentication. To validate users via this method, SBM login IDs must match each user’s network login ID.
In the **Other Settings** tab, you can specify an IIS application that is configured with anonymous access in the **IIS application for external authentication** field. This enables external users access to SBM without having to log in to your domain. For details, see **Other Settings** [page 85].

You can validate users against a **Windows Domain** with or without **Single Sign-On**:

- If you want to take advantage of SSO for user authentication, select **Single Sign-On** and authenticate browser users via **Windows Authentication**. SBM Configurator automatically updates the SSO configuration files with the required settings to authenticate users against your Windows domain when you click **Apply**.

- If you want IIS to authenticate users, select **SBM Session Cookies** and authenticate browser users via **Windows Authentication**. SBM Configurator automatically updates IIS with the required application settings to authenticate users against your Windows domain when you click **Apply**.

**Configuring Windows Domain (NTCR) Authentication**

SBM Configurator performs all the necessary set up tasks in IIS or SSO to authenticate users against your Windows domain. However, if your IIS settings are inadvertently or mistakenly changed, consult with your IIS administrator and manually configure either IIS or SSO according to the steps in the following sections. Note that the steps differ slightly depending on which session management option you select.

- **Windows Authentication (IIS) Manual Configuration Steps** [page 69]
- **Windows Authentication (SSO) Manual Configuration Steps** [page 70]

**Windows Authentication (IIS) Manual Configuration Steps**

This section describes how to manually configure **Windows Authentication** when IIS is used to manage user authentication (non-SSO). You will configure the following settings on the machine that hosts SBM Application Engine:

1. Open Internet Information Services (IIS).

2. On the **tmtrack** application:
   - Enable **Windows Authentication** (IIS 7 and higher)
   - Disable **Anonymous Authentication** (IIS 7 and higher)

   If you intend to use integrations, such as SourceBridge, enable **Basic Authentication**.

3. On the **workcenter** application:
   - Enable **Windows Authentication** (IIS 7 and higher)
   - Disable **Anonymous Authentication** (IIS 7 and higher)

   **Important:** The **workcenter** application authentication settings must match the tmtrack application authentication settings.

4. Enable only **Anonymous Authentication** on the following applications:
   - **Default Web Site** (or **Web Sites**)
This ensures that the REST grid widget, PDF widget, and Serena Request Center work properly. The REST Widget fails in FireFox browsers if SBM uses **Windows Domain (NTCR)** authentication. This issue does not occur in Internet Explorer browsers.

**Important:** In a distributed installation, configure the SBM Tomcat service to use a Windows domain account (or create a local user on both the Tomcat and IIS servers with the same password). This ensures that the PDF widget has access to the tmtrack application.

5. Stop and start IIS.

6. Launch SBM Configurator, and then open the **Authentication** tab.

7. On the **General** tab, set the following:
   - **Browser sessions** – **SBM Session Cookies**
   - **Browser authentication** – **Windows Authentication**
   - **Web services authentication** – **Internal SBM Database**

8. On the **Windows Domain** tab, enter the correct Windows domain in the **Domain** field. If a domain is not specified, then the domain that the IIS server machine is installed on is used for user validation.

   **Note:** This domain is used by SBM Application Engine to verify the user’s credentials with the domain controller when Windows authentication materials do not accompany the authentication request (for example, when SBM Application Engine receives a Web service request). Basic authentication materials should accompany the call in that case; therefore the proper domain is required. Be aware that user passwords are sent in clear text unless secured through SSL in this scenario.

9. Configure password restrictions for external users (if any) on the **External Passwords** tab. For details, refer to **Password Restrictions** [page 79].

10. If you want users to access SBM without logging in to your network domain, type the name of an application in IIS with anonymous authentication in the **Virtual Directory for external authentication** field on the **Other Settings** tab. For more information, refer to **Other Settings** [page 85].

11. Click **Apply** in SBM Configurator.

**Windows Authentication (SSO) Manual Configuration Steps**

This section describes how to manually configure **Windows Authentication** when SSO is used to manage user authentication. You will configure all of the IIS settings on the machine that hosts SBM Application Engine and the steps involving SBM Configurator on the server that hosts SSO.

1. Open Internet Information Services (IIS).

2. On the **tmtrack** application:
• Enable Anonymous Authentication (IIS 7 and higher)
• Disable Windows Authentication (IIS 7 and higher)

If you intend to use integrations, such as SourceBridge, enable Basic Authentication.

3. Enable and disable the same authentication settings (except for Basic Authentication, if you enabled it) on the following directories:
   • Default Web Site (or Web Sites)
   • gsoap
   • sbmconnector
   • workcenter
   
   **Important:** The workcenter application authentication settings must match the tmtrack application authentication settings.

This ensures that the REST grid widget, PDF widget, and Serena Request Center work properly. The REST Widget fails in FireFox browsers if SBM uses Windows Domain (NTCR) authentication. This issue does not occur in Internet Explorer browsers.

   **Important:** In a distributed installation, configure the SBM Tomcat service to use a Windows domain account (or create a local user on both the Tomcat and IIS servers with the same password). This ensures that the PDF widget has access to the tmtrack application.

4. Stop and start IIS.

5. Launch SBM Configurator, and open the Authentication tab.

6. On the General tab, set the following:
   • Browser sessions – Single Sign-On
   • Browser authentication – Windows Authentication
   • Web services authentication – Internal SBM Database

Select the Enable Login Form check box if you want to display a login page to users when user validation fails. Clear the check box if you do not want the page to appear.

7. Configure password restrictions for external users (if any) on the External Passwords tab. For details, refer to Password Restrictions [page 79].

8. If you want users to access SBM without logging in to your network domain, type the name of an application in IIS with anonymous authentication in the Virtual Directory for external authentication field on the Other Settings tab. For more information, refer to Other Settings [page 85].

9. Click Apply in SBM Configurator.
About LDAP Authentication

LDAP authentication enables you to validate users through a central directory via the Lightweight Directory Access Protocol (LDAP). There are several options for LDAP authentication, including:

- **LDAP**
  Validates users against LDAP using SBM Application Engine.

- **LDAP then Internal**
  Validates users against LDAP using SBM Application Engine first, and then against the internal SBM database if the user is not found in LDAP.

- **SSO LDAP**
  Validates users against LDAP using SSO.
  - Using SSO provides better performance and more security options than the Application Engine-based LDAP options. When you configure SSO LDAP, all browser authentication requests are performed against LDAP by SSO, and only Web service authentication requests that do not have a security token are performed by Application Engine.
  - If you select this option, continue the configuration on the server that hosts the Single Sign-On (SSO) component. You must configure SSO LDAP on the Single Sign-On (SSO) server in order for SBM Configurator to successfully update the SSO configuration files.
  - You cannot use the Auto Add from LDAP feature with SSO LDAP. If you plan to configure SBM to automatically add users from LDAP upon successful authentication (Auto Add from LDAP), you must use LDAP or LDAP First, then Internal for user validation.

- **SSO LDAP then Internal**
  Validates users against LDAP using SSO first, and then against the internal SBM database if the user is not found in LDAP.
  - If you select this option, continue the configuration on the server that hosts the Single Sign-On (SSO) component. You must configure SSO LDAP on the Single Sign-On (SSO) server in order for SBM Configurator to successfully update the SSO configuration files.
  - You cannot use the Auto Add from LDAP feature with SSO LDAP. If you plan to configure SBM to automatically add users from LDAP upon successful authentication (Auto Add from LDAP), you must use LDAP or LDAP First, then Internal for user validation.

**Important:** If you use the LDAP then Internal authentication option, user passwords must match in SBM and LDAP.
Configuring LDAP Authentication

To configure LDAP authentication for SBM:

1. On the **General** tab, select a browser session option. If you select Single Sign-On (SSO), you can use **SSO LDAP** or **SSO LDAP then Internal**.

2. In the **Browser authentication** drop-down list, select the option that you want to use for gathering user credentials. If you select **Windows Authentication**, users are logged in automatically upon successful authentication against LDAP.

3. Select one of the following options in **Authenticate against** (or **Web services authentication** if you are not using the **SBM Login Form** option):
   - **LDAP**
   - **LDAP then Internal**
   - **SSO LDAP**
   - **SSO LDAP then Internal**

   The **LDAP** sub-tab appears.

4. On the **LDAP** sub-tab, enter the following information:
   - **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.

• Click **Managed Trusted Certificates** to launch the **Certificates** window and import, export, or remove trusted certificates from the Java truststore (cacerts file). This enables you to manage multiple certificates in the Java truststore. This option only applies if you are using **SSO LDAP**.

    **Note:** You manage your trusted certificates on the server that hosts Single Sign-On (SSO). For distributed installations, ensure that you configure the LDAP security settings for **SSO LDAP** on the **Single Sign-On** server. This is where the cacerts file is stored.

• **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**

  The search filter is used differently depending on if you are working with LDAP users or LDAP groups.

  • **For LDAP users:**

    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 `j smith` 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.

  • **For LDAP groups:**

    Enter a search string that will act as a filter against the group membership attribute. For example:
(&{objectClass=user})

This is used to ensure that the group membership search result is an actual user account and not a sub-group or other non-user LDAP object.

- **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 cannot 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.

- **Test Connection**
  - **User name**
    Type the SBM login ID of a user account to test the provided connection and search parameters settings.
Chapter 5: Configuring SBM

- **Password**
  Type the LDAP password of the user account specified in the **User name** box.

  Click **OK** to test the connection and search parameter settings. If your authentication test fails, an error message appears and explains the settings that need to be modified.

  **Note:** You can test connection and search parameter settings without applying them to the database.

5. Configure password restrictions for external users (if any) on the **External Passwords** tab. For details, refer to **Password Restrictions** [page 79].

6. If you want users to access SBM without logging in to your network domain, type the name of an application in IIS with anonymous authentication in the **Virtual Directory for external authentication** field on the **Other Settings** tab. For more information, refer to **Other Settings** [page 85].

7. Click **Apply**.

**Preparing LDAP for SBM**

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.
About Third-Party Authentication

Using a Third-Party Authentication System enables you to designate an external entity that will perform user authentication for SBM. This option configures SBM to accept authenticated user credentials from an External Identity Provider such as Tivoli, SiteMinder, or Oracle Identity Manager.

You can choose to manage user sessions with or without SSO. SSO enables you to configure authentication settings for an external identity provider that uses SAML2. For details, refer to Configuring External Identity Provider Settings [page 77].

Configuring External Identity Provider Settings

You can enable SBM to accept authenticated users using an external identity provider. If you are using SSO to manage user sessions, select one of the following options:

- Use Third-Party Service Provider
- Use SAML2 Service Provider

Otherwise, if you are not using SSO, enter the Custom HTTP header that is used by the identity provider to pass the user ID to SBM. The default value is REMOTE_USER.

For more information on these options, refer to the corresponding topics below.

Using a Third Party Service Provider

You can configure authentication settings for a third-party service provider with or without SSO. Details on configuring settings with SSO are provided below.


2. In the Browser authentication drop-down list, select Third Party Authentication System. The External Identity Provider tab appears.


4. Select the Enable Login Form check box to display a login page to users when user validation fails. Clear the check box if you do not want the page to appear.

5. Enter the Custom HTTP header that is used by the identity provider to pass the user ID to SBM. The default value is REMOTE_USER.

6. Select Configure custom authentication filter to enter your own custom filter for the external identity provider.

    For example:

```
<filter>
  <filter-name>MySample3rdPartyFilter</filter-name>
  <filter-class>com.acme.authentication.MySample3rdPartyFilter</filter-class>
  <init-param>
    <param-name>param1</param-name>
    <param-value>value1</param-value>
  </init-param>
  <init-param>
    <param-name>param2</param-name>
  </init-param>
</filter>
```
7. Click **Apply** to save your changes.

**Using a SAML2 Service Provider**

SAML2 requires a trust relationship between the identity provider and the service provider via an exchange of metadata between the two entities. On the SSO server, you will use SBM Configurator to retrieve the service provider metadata (which includes a unique entity ID) and you will use it to register the SSO server with your identity provider. You will then obtain metadata from the identity provider and enter it into SBM Configurator to establish the trust.

If you have multiple SSO servers (as you would in a multi-environment installation), depending on the identity provider requirements you might need to register the entity ID from each SSO server individually with the identity provider.

The following steps describe how to perform a typical metadata exchange.

1. On the **General** tab, in the **Browser sessions** drop-down list select **Single Sign-On**.

2. In the **Browser authentication** drop-down list, select **Third Party Authentication System**. The **External Identity Provider** tab appears.

3. On the **External Identity Provider** tab, select **Use SAML2 Service Provider**.

4. If Tomcat is configured to use HTTPS, the **Use HTTPS for endpoints** check box is selected by default. Clear this check box if HTTPS is not used or not desired by SBM as the service provider.

5. In the **Identity Provider** section, click **Edit Metadata**. Click **Import** or paste the metadata that you obtain from the identity provider. Click **OK** when you are finished.

6. In the **Service Provider** section, click **Generate Certificate** to add a self-signed certificate. This creates a certificate with a private key and adds the x509 certificate information to the service provider metadata that you will send to the external identity provider.

7. In the **Service Provider** section, click **View Metadata**. In the dialog box that appears, click **Export** or **Copy** and save the data that appears to a text file. Use this metadata to register with the identity provider.

   **Tip:** Depending on the policies of your identity provider, HTTPS URLs might be required for the service provider bindings. If you configure SSL on the IIS and Tomcat tabs in SBM Configurator, the bindings in the service provider metadata are automatically created using HTTPS as well.

8. Click **Apply** to save your changes.
The exchange of metadata is now complete and the trust relationship between SBM and your external identity provider has been established.

**Password Restrictions**

The **Password Restrictions** tab enables you to determine system settings for user passwords. You can override system password settings for individual users in SBM Application Administrator.

Users with an invalid password who attempt to log in are immediately directed to the **Change Password** page and must provide a valid password before logging in. For example, if a user's password expires, that user must provide a new password before he or she can log in to the system.

SBM maintains a count of the invalid login attempts that occur per user ID while the server is running. However, the number of invalid log in attempts that occur over a period of time is not recorded. In other words, time does not play a role with respect to the number of invalid login attempts. If the server is restarted for any reason, the invalid login count is reset to zero for all user IDs. Also, the count for invalid login attempts for a user is reset after the next successful log in.

- **Internal Password Expiration Options** [page 79]
- **Internal Password Complexity Options** [page 79]

**Internal Password Expiration Options**

Configure expiration settings for user passwords. If you choose not to set a password expiration time, you can prevent users from changing their passwords.

Select one of the following options:

- **Passwords do not expire and cannot be changed**
  Select this option if you do not want to set a password expiration period and you want to prevent users from changing their passwords.

- **Passwords do not expire**
  Select this option if you do not want to set a password expiration period.

- **Passwords expire after \((n)\) days**
  Select this option to set a password expiration period. Specify the number of days that passwords are valid, after which users must create new passwords. The range is 1 to 999.

**Internal Password Complexity Options**

You can specify certain requirements for passwords, such as a minimum length, special characters, or uniqueness from a certain number of past passwords.

By default, the **No minimum length** option is selected. To specify a minimum number of characters for passwords, select the **Minimum length of** option, and then specify the minimum number of required characters in the **characters** field.

- **Must include a number**
  Select this option to require passwords that include at least one number.

- **Must include an uppercase letter**
Select this option to require passwords that include at least one uppercase letter.

- **Must include a lowercase letter**
  Select this option to require that passwords include at least one lowercase letter.

- **Must include special characters**
  Select this option to require that passwords include special characters.
  - By default, internal user passwords do not require special characters. To require users to create a password with a specific number of special characters, select the **Must include** option, and then specify the minimum required number of special characters in the **special characters** field. Special characters include punctuation marks, the percent sign, and currency symbols. Special characters can appear in any sequence in the password.

The first three options evaluate passwords separately from the special characters option. For example, you do not need to require users to provide special characters in their passwords to require them to include a number.

Depending on the version of SBM you are using, these 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** options.

By default, the **No historical validation** option is selected. To require users to create unique passwords, select the **Cannot match last** option, and then specify the number of passwords that must be unique in the **passwords** field.

### Custom Authentication Settings

The **Custom Authentication** tab appears when you select Single Sign-On (SSO). In the **Custom Authentication** tab, you can customize authentication settings or configure Smart Card authentication.

A Smart Card is a secure token carrier that contains X.509 v3 certificates. Smart Card authentication is a secure and reliable authentication method that allows users who have a current Smart Card (containing valid certificates and identity information) to gain access to a Smart Card-enabled SBM system once the proper PIN is provided.

**Note:** Smart Card users log in by selecting a certificate with their PIN; there is no need to enter an SBM password when logging in via Smart Card authentication. However, if SBM is configured to authenticate transitions or require electronic signatures, Smart Card users must create a Smart Card password to complete transition authentication requests. For more information, see "Overriding Authentication Options for Transitions" in the *SBM Application Administrator Guide*.

To start configuring custom authentication settings, select the context provider you want to use:

- **Application Engine**
  Select **Application Engine** as the context provider if your users are in SBM.

- **Other**
Select **Other** as the context provider if your user accounts are stored in an external application that can use SBM Single Sign-On (SSO).

For example, if you want users in Dimensions CM to authenticate against LDAP using SBM’s Single Sign-On (SSO) engine, select **Other** as the context provider and add an LDAP authenticator that points to the LDAP store that contains your Dimensions CM users.

If you want to override the default authentication settings, select **Enable authenticators and identity transformers** and configure authenticators and identity transformers. Note that this option is selected by default when you select the **Smart Card Login** for browser authentication on the **General** tab.

Refer to the following sections for help with customizing authenticators and identity transformers.

- Configuring Authenticators [page 81]
- Configuring Identity Transformers [page 82]

**Configuring Authenticators**

In the **Authenticators** section, you manage predefined or custom authenticators. You can configure authenticators for each source that your users should be authenticated against.

To get started, click **Add New**, and then select one of the following:

- Configuring Predefined Authenticators [page 81]
- Configuring Custom Authenticators [page 82]

**Configuring Predefined Authenticators**

Select this option to use one of the predefined authenticators that are provided by SBM. Use the provided tooltips for guidance when configuring an authenticator.

Select the **Explicit** checkbox to force an authenticator to reject any incompatible credentials that are received. For example, an x509 authenticator will deny any requests that contain a user name and password if this option is selected.

The following predefined authenticators are available:

- **Default authenticator**
  
  Provided for testing purposes only.

- **Compound authenticator**
  
  Compound authenticizers enable you to implement multiple authenticators using logical operators like OR and AND. After you add a compound authenticator, define additional authenticators as needed, and then drag and drop them into the compound authenticator container.

- **NTLM authenticator**
  
  Authenticate credentials against a Windows domain.

- **Application Engine authenticator**
Authenticate credentials against Application Engine. No additional configuration is necessary.

- **LDAP authenticator**
  Authenticate credentials against LDAP. This is analogous to configuring SSO LDAP.

- **x509 Base authenticator**
  Authenticate credentials using client-side certificates.

- **x509 LDAP authenticator**
  Authenticate credentials from x509 certificates against LDAP.

  **Note:** The x509 LDAP authenticator assumes that the user's distinguished name is contained in the certificate's subject value. If certificates issued by your certificate authority do not have the distinguished name or have additional parameters included in the subject, authentication fails. In this case, you can modify the sample LDAP authenticator and use it as a custom authenticator.

- **x509 CRL authenticator**
  Authenticate credentials from x509 certificates against a certificate revocation list (CRL). A CRL is a certificate authority–managed list of certificates that have been revoked or are no longer valid.

  **Important:** Authentication is assumed for certificates that are not in the CRL. This means that if authentication does not occur prior to accessing SBM, you must set up and configure an authenticator that performs the actual identity check. For example, you can configure the LDAP authenticator to enforce authentication against LDAP, and then validate the certificate against the CRL.

- **x509 OCSP authenticator**
  Authenticate credentials from x509 certificates against using Online Certificate Status Protocol (OCSP).

**Configuring Custom Authenticators**

Select **Custom authenticator** to enter XML that describes for your custom authenticator. Click **Reindent** to fix any indentation problems in the XML and improve readability. Click **Validate** to check that the XML is valid.

**Configuring Identity Transformers**

After you define one or more authenticators, configure how user identities are managed using one or more identity transformers. You can configure both pre-authentication and post-authentication transformers.

For example, after a user selects his or her certificate when prompted, an x509 base authenticator validates the certificate and passes the certificate information to the Identity Store. The certificate contains a common name (CN) in the form:

\[ CN=LASTNAME.FIRSTNAME.MIDDLE.10DIGITNUMBER \]
If the login ID in SBM does not match the common name, authentication fails. Most SBM login IDs do not contain the entire CN value; therefore, a server-side JavaScript **pre-authentication identity transformer** can convert the common name into the required login ID format. Once the CN value is transformed, the user identity is authenticated against the Identity Store.

To get started, click **Add New**, and then select one of the following:

- Configuring Predefined Identity Transformers [page 83]
- Configuring Custom Identity Transformers [page 83]

### Configuring Predefined Identity Transformers

Select **Predefined identity transformer** to use one of the predefined identity transformers that are provided by SBM. Use the provided tooltips for guidance.

The following predefined identity transformers are available:

- **Default identity transformer**
  Provided for testing purposes only.

- **Decorator identity transformer**
  A simple transformer that enables you to prepend or append a string to a username. For example, you can specify a suffix like @acme.com to transform a username like jdoe into an e-mail address like jdoe@acme.com.

- **JavaScript identity transformer**
  Transforms a username using server-side JavaScript transformation. This enables you to implement your own custom logic in the username transformation.

- **X509 JavaScript identity transformer**
  Transform user identities obtained from x509 certificates using sample JavaScript. You can also override the identity transformer and establish your own ID mappings if converted identities are identical or you want to define specific key-value pairs. The **Mapping keys file** called cert2user_mapping_keys.xml that is provided by default contains a sample identity mapping override that you can modify as needed.

- **LDAP identity transformer**
  This transformer enables you to transform a user identity by using an LDAP attribute as the source of the transformed identity. Once an authenticated user is found in LDAP, the attribute value from the user's LDAP record is used as its login identity.

### Configuring Custom Identity Transformers

Select **Custom identity transformer** to enter XML that describes for your custom identity transformer. Click **Reindent** to fix any indentation problems in the XML and improve readability. Click **Validate** to check that the XML is valid.

### Using Smart Card Authentication with SBM Composer

In addition to browser users, you can enable Smart Card authentication in SBM Composer. This enables designers to log in to the repository using a Smart Card instead of an SBM user name and password.
Configuring SBM Composer

You configure Smart Card authentication for SBM Composer users on a machine-by-machine basis.

To enable Smart Card authentication in SBM Composer:

1. On an SBM Composer machine, navigate to the directory that contains the SBM Composer executable, and launch SBM Composer using the following command:


   The Advanced Security Setup for SBM Composer dialog box appears. This dialog box is intended for administrators; it is not available in the standard SBM Composer interface, nor described in the SBM Composer Guide. The Client Certificate Administration tab lists all self-signed certificates that currently reside in the user's personal certificate store that contain both a private and public key.

2. Click the Smart Card Authentication tab.

3. Select the Enable smart card authentication check box.

4. Optionally, if you want to make the Smart Card certificate available for use in client certificate authentication from SBM Composer, select the Make available as client certificate check box. This enables you to use the Smart Card certificate on the Client Certificate Administration tab. Follow the steps in Client Certificate Authentication with SBM Composer [page 127] to use this certificate for client certificate authentication.

   **Note:** This does not require you to use the Smart Card certificate for client certificate authentication. You can still use separate certificates for client certificate authentication and Smart Card authentication from SBM Composer. However, if you would like to use the Smart Card certificate for client certificate authentication, this option enables you to do so.

5. Click Done to finish. The SBM Composer user can now select the Use smart card check box and select a Smart Card certificate on the Repository tab in the SBM Composer Options dialog box.

Logging in with Smart Card Authentication

After you have configured each client machine that requires Smart Card authentication, SBM Composer users will perform the following steps to log in and access the repository.

**Prerequisites:**

Smart Card authentication must be configured in SBM. Review the configuration steps in Custom Authentication Settings [page 80] before designers attempt to log in with Smart Card authentication.

**To log in with Smart Card authentication from SBM Composer:**

1. Insert your Smart Card into the reader that is connected to your machine.
2. Launch SBM Composer, and then open the Repository tab in the SBM Composer Options dialog box.

3. Select the Work online option.

4. Enter the Machine name and Port number of the SBM Application Repository server.

5. Select the Use smart card check box. The User name and password fields are replaced by the Smart card certificate field.

6. Click the Select button. The Windows Security dialog box appears and lists the available certificates.

7. Select the certificate that is associated with your Smart Card, and then click OK. The certificate appears in the Smart card certificate field.

8. Click Test connection to verify that you can connect to the repository. The ActivClient middleware is invoked and prompts you to enter your PIN.

9. Enter the PIN that is assigned to your Smart Card, and then click OK.

10. Click OK to close the SBM Composer Options dialog box. You are now connected to the repository.

The certificate that you used will remain selected in the Smart card certificate field, which means you should only need to provide the PIN to connect to the repository again.

Other Settings

In the Other Settings tab, you configure optional authentication settings.

The following options are available (depending on your current selections on the General tab):

- **Re-authenticate from outside URL**
  
  Select this check box if you want to require users to re-authenticate after leaving the system and visiting another Web site. For example, a user logs in to SBM, and then visits http://www.MyFavoritePage.com. If the user then tries to use the back button to return to SBM, the user is prompted to log in again.

  - This also applies to pages within SBM if users enter an SBM URL directly into the address box or if users click the Refresh button on the browser. However, if users click a link or button on an SBM page that takes them to another SBM URL, they will not have to log in again.

  - This setting cannot be used in combination with the Single Sign-On (SSO) because SSO gathers user credentials differently. You must use SBM Session Cookies and either internal SBM passwords or LDAP authentication with for re-authentication to occur. (SBM Session Cookies are required because this is how user credentials are gathered for the re-authentication process).

  - If you are using LDAP authentication, users are automatically logged back in to SBM when the Re-authenticate from outside URL option is selected; however, the User session time-out setting can be configured to force users to re-
authenticate if they have not actively used the system for a specified number of minutes.

- **Disable users after failed login attempts**
  Select this check box to disable accounts of users who fail to correctly authenticate after a specified number of login attempts. Set the number of login attempts between 1 and 10. After users exceed this number of attempts, their accounts are disabled and must be re-enabled by an administrator.
  
  - User accounts can be re-enabled in SBM Application Administrator.
  
  - This feature is only available if users are validated against the internal SBM database or LDAP.

- **External Access**
  If you want users to access SBM without logging in to your network domain, or if they are not stored in LDAP, enter the name of an application in IIS that uses anonymous authentication in the **External Virtual Directory Name** box. You will need to manually create this application in IIS, and ensure that it can execute ISAPI extensions (enabled via Handler Mappings in IIS 7).

  **Note:** If you add an external application in IIS, you must manually configure the application's native modules and select the **ModSecurity IIS** module to enable the same level of threat detection and prevention that is configured on the default SBM applications.
• You must add the following MIME types to the new application that you create in IIS:
  • File name extension: .properties | MIME type: text/plain
  • File name extension: .woff | MIME type: application/font-woff
  • File name extension: .appcache | MIME type: text/cache-manifest

• If users are validated against your Windows Domain, this option sets up two authentication methods for your system: Windows Authentication for internal users and validation against the Internal SBM Database for other users.

• If users are validated against LDAP, this option sets up two authentication methods for your system: LDAP authentication and Internal SBM Database for non-LDAP users.

• If you plan to use the e-mail response feature in SBM with Windows Authentication, you must specify an application in IIS with anonymous authentication. For more information, refer to Notification Server Options [page 91].

• Select the check box in this section to restrict access so that only external users can access SBM through this anonymous application. External users are authenticated with their SBM passwords, which must be at least six characters in length.
  

  Note: You configure external access for users, not administrators or designers. SBM Application Repository is not accessible externally, which means administrators cannot log in to SBM Application Repository or access the repository using SBM Composer from outside the domain; however, SBM Application Administrator can be accessed externally for administrators who need to manage users and projects.

Mail Services

In the Mail Services tab, you enter the mail server connection information for the Notification Server, Mail Client, Event Manager, and Application Repository.

  Important: For new installations, the Mail Services settings are not saved in the Application Engine database until after you run the Create Database Wizard in SBM System Administrator. After you run the wizard and successfully create the database, use SBM Configurator to configure the settings.

The SBM Mail Services settings are stored in the SBM Application Engine database. Therefore, ensure that the server or servers that run the SBM Mail Services have access to the correct SBM Application Engine database connection information on the Database Servers tab.
About the Notification Server

The Notification Server generates e-mail notifications based on events or conditions that occur in the system. The Notification Server is also used for the following features:

- **Sending e-mail messages from items**
  In addition to e-mail messages that are sent when a specific event occurs in the system, the Notification Server is used to send e-mail messages directly from SBM items. This is useful when users need to communicate with one another about a particular item in the system. Additionally, by configuring the E-mail Recorder feature, e-mail conversations can be logged in the Notes section of an SBM item.

- **Adding or Removing items from folders**
  Instead of sending an e-mail message when a particular event occurs, a notification can add or remove an item from a folder in SBM. You configure this type of action on particular notifications in the SBM Application Administrator.

- ** Executing Web services and scripts**
  Instead of sending an e-mail message when a particular event occurs, a notification can execute a Web service call or invoke an AppScript in SBM. You configure this type of action on particular notifications in the SBM Application Administrator.

Configuring the Notification Server

This section describes configuration settings for the Notification Server. For distributed installations, you configure these mail server settings directly on the servers where the Notification Server is installed. You can change these settings any time after installation by running SBM Configurator in utility mode.

To configure the Notification Server, select the **Enable Notification Server** check box and then select an option in the **E-mail server type** drop-down list. Select **E-mail Disabled** to disable notifications and e-mail messages that users can send from items. (You can select this option to prevent e-mail from being sent, though the Notification Server can still be used to create links to items from folders or automatically execute scripts.)

**Note:** The **Advanced** button is used by Serena for troubleshooting purposes only.

- **SMTP Options** [page 88]
- **Exchange Options** [page 90]
- **Notification Server Options** [page 91]

SMTP Options

Many servers commonly use SMTP (Simple Mail Transfer Protocol). Anytime you send e-mail through the Internet, mail routes via one or more SMTP Servers. Setting up an SMTP connection is quick and easy—you do not need to install any additional software and you only need the IP address of your SMTP Server.
To configure the **Notification Server** to use SMTP, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>Enter the IP address or host name of the SMTP Server. This is typically an IP address, such as 165.212.186.1; however, your company might use a network name supplied by a DNS Server, such as <code>mycompany.com</code>. Contact your network administrator to find out the name of this mail server.</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the SMTP server port number of the SMTP Server. The default SMTP port is 25.</td>
</tr>
</tbody>
</table>
| **Enable VRFY**   | Select this option if the Notification Server should issue the SMTP VRFY command when it sends e-mail messages. Some SMTP servers support the VRFY command, which can be used to validate that the e-mail address is valid before sending e-mail. If the **Enable VRFY** check box is cleared, the Notification Server will not issue the SMTP VRFY command when it sends e-mail messages. Note that this setting is disabled by default:  
  - Older servers do not support the SMTP VRFY command. If you are using a server that does not support this command, clear this setting.  
  - Your SMTP server may have the verification command already disabled. If this option is selected, the Notification Server tries to verify the address with the SMTP server. Because the verification command is disabled in the SMTP server, mail is not sent. |
| **Use SSL**       | Select this option to send and receive messages through a secure connection.                                                                                                                                  |
| **Port is SSL dedicated** | Select this option if you know that the server requires an SSL-dedicated port. Otherwise, to use SSL encryption in the standard way, clear this check box.                                                          |
| **Domain**        | Enter the domain name of the SMTP Server, such as `mycompany.com`. Some SMTP Servers require a domain name for user authentication purposes.                                                                     |
| **Use authentication** | Select this option to use SMTP authentication as defined by RFC 2554. You might need to use this option if your SMTP server does not allow relaying.  
  By default, many SMTP servers do not allow relaying. This prevents SBM from sending e-mail messages to users outside the local domain. For example, if your SMTP server belongs to the `mycompany.com` domain, then the SMTP server might not send messages to users who do not belong the same domain. |
If you use a self-signed SSL certificate, you must add the certificate to the Java VM truststore. Use the Manage Trusted Certificates option on the Tomcat Server tab to add the certificate.

**Exchange Options**

Use the Exchange (via Web services) option to communicate directly with an Exchange server using the MS Exchange Web services API. You might use this option if your company does not allow connection through SMTP. If no such restriction exists, consider using SMTP because it enables faster connection speeds than MS Exchange.

To configure the Notification Server to use Exchange, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange version</td>
<td>Select the current version of your Exchange server.</td>
</tr>
<tr>
<td>Service URL</td>
<td>Enter the service URL for your Exchange server. For example: <a href="https://servername/EWS/Exchange.asmx">https://servername/EWS/Exchange.asmx</a>.</td>
</tr>
<tr>
<td>Login</td>
<td>Enter the login name for a system user on the Exchange server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the user account.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Enter the password again to confirm it.</td>
</tr>
</tbody>
</table>

If the Exchange Service URL is secured by SSL, you must provide the certificate authority (CA) chain that signed the endpoint certificate. This means that you must add the public certificate of each CA in the certificate chain to the Tomcat truststore. If the endpoint is secured via SSL, use the Manage Trusted Certificates option on the Tomcat Server tab to import the certificates and trust the chain that signed the endpoint's SSL certificate.
Notification Server Options

To configure Notification Server settings that apply to both server types, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject max length</td>
<td>Enter the maximum number of characters that should appear in the subject line for each notification. The default is 200 characters. If the subject line contents are greater than the max length that you specify, the subject line is truncated.</td>
</tr>
<tr>
<td></td>
<td>When the subject line is truncated, the last three characters are replaced by ellipses (...). For example, if the maximum length is set to 100, the subject line will contain 97 characters followed by ellipses.</td>
</tr>
<tr>
<td></td>
<td>If the subject line contains a TTID string, it is preserved and inserted before the ellipses even if the TTID string is located in the excluded portion of text.</td>
</tr>
<tr>
<td>Retry period</td>
<td>Enter the number of seconds in which the Notification Server should attempt to send a failed message. The default value is 10800 seconds (or three hours).</td>
</tr>
<tr>
<td>Retry count</td>
<td>Enter the maximum number of times the Notification Server should attempt to send a failed message. The default value is five times.</td>
</tr>
<tr>
<td>Sender that appears in e-mail subject or body</td>
<td>Enter a text string that will appear in the subject and body of messages to indicate the sender of the notification. The default is &quot;SBM Notification Service.&quot;</td>
</tr>
<tr>
<td></td>
<td>This setting is only applicable after the $SENTBY() tag has been added to the notification e-mail template in use. For details on using this tag, refer to the SBM Application Administrator Guide.</td>
</tr>
<tr>
<td>Start date</td>
<td>Enter a start date for mail delivery to begin. The start date is recorded in the database as specified in SBM Configurator and does not adjust according to the server's time zone; Coordinated Universal Time (UTC) is used instead.</td>
</tr>
<tr>
<td></td>
<td>If you need to re-send notifications because of a mail server failure, you can set the Start Date to an earlier date to send messages that were not sent. However, use caution because the Notification Server will reprocess existing change history and resend all the messages that have been created since that date.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
--- | ---
Enable inline images | Select this option to include images from Rich Text fields in notification messages and e-mails that are sent from the browser. Use the check box to toggle this option on or off globally (for all notifications), or optionally toggle it on or off for specific notifications using SBM Application Administrator. Note that this option is enabled in SBM Configurator and on every notification by default.

**CAUTION:**

Serena recommends that you review your notifications and determine if this setting should be enabled globally, or if individual notifications should have the setting enabled instead. A notification that contains a large embedded image and several hundred subscribers could negatively affect notification server performance.

In the **Link Settings** section, configure the server URLs that appear at the bottom of Notification Server messages.

**Note:** The **Link Settings** options are only applicable to notification e-mail templates that contain the `$LINK()` tag. For information on notification template tags, refer to the *SBM Application Administrator Guide*.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server</td>
<td>Enter the Application Engine host name that should appear in the URL. <strong>Tip:</strong> This setting also controls the host name that appears in the URL that is returned with items in Application Engine Web service calls.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the SBM Application Engine Web Server port number. The default port value is 80.</td>
</tr>
<tr>
<td>Address for external links</td>
<td>Enter the name or address of your external Application Engine that should appear in the URL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the external Application Engine port number.</td>
</tr>
</tbody>
</table>
### Field Description

**E-mail response with external virtual directory**
Select this option to use the e-mail response feature with **Windows Domain (NTCR) authentication**. This allows users to execute transitions in notification messages while outside of the domain and without authentication credentials.

This option uses the external directory that you specify on the **Authentication | Other Settings** tab for both internal and external e-mail response links in notification messages.

Enter your Web server host name or IP address and port in the fields that appear.

**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.

In the **From and Reply-to Addresses** section, specify e-mail addresses for replies to messages that are sent from the Notification Server.

These settings can be overridden for projects in SBM Application Administrator.

### Field 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.

**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.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From last modifier</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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 |

In the **Expired Notification Messages** section, configure how the Notification Server handles messages that have not been successfully delivered.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiration time</td>
<td>Enter the number of days that should pass between the first failure of an e-mail notification and the expiration period. By default, failed e-mail messages are deleted after seven days.</td>
</tr>
<tr>
<td>Log expired messages</td>
<td>Select this option to enable logging for failed e-mail notifications. To delete expired notifications without logging them, clear the check box.</td>
</tr>
</tbody>
</table>

The `expiredmessages.log` file is located here:

`installationDirectory\Serena\SBM\Common\Tomcat 7.0\server\default\logs`

E-mail messages with an invalid e-mail address that are not sent by the Notification Server remain in the database until the **Expiration time** has passed. If the log indicates that messages failed to send due to an invalid e-mail address, update the user's e-mail address in Application Administrator. This will update the notification message in the database, and the Notification Server will send the message to the correct address on the next cycle.

In the **Expired Notification Tokens** section, configure the amount of time that e-mail response URL tokens are valid. E-mail responses enable users to transition items directly from a notification message without having to log in. For more information, refer to the *SBM Application Administrator Guide*. 
### Field Description

**Expiration time**
Enter the number of days and hours that should pass before the token expires. Once the token expires, the recipient must log in to transition the item. The default value is three days.

In the **Work Center Notifications** section, configure the number of days to display Work Center notifications.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete notifications from Work Center after ( (n) ) days</td>
<td>Enter the number of days for which notifications should appear in Serena Work Center. The default value is thirty days. Notifications that are older than this value are purged from Work Center.</td>
</tr>
</tbody>
</table>

In the **Attachments** section, use the following options to define the attachment and note size limit for notification messages:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum attachment size (in MB) | This setting limits the size of the attachments that are included with notification messages. For example, you may decide that 3 MB is the maximum size for all attachments that are included with outgoing e-mails.  
- If the total size of all attachments exceeds this limit, then no attachments are included with the message and instead a link to view the attachment is sent.  
- The default (and maximum value) is 5 MB.  
- Attachments are only sent if e-mail template includes the $ATTACHMENTS() tag. For details, refer to the *SBM Application Administrator Guide*.  
- The Notification Server only includes attachments if they are stored in the database (not on the file system). For more information, see Chapter 7: "Customizing SBM Settings" in the *SBM System Administrator Guide*. |
### Inline note size limit

Enter the size limit (in characters) for notes that are sent as part of an item notification.

- This size limit applies to all notes that have been added to the item (either by the E-mail Recorder or in the item directly).
- The default is 10000 characters.
- Notes that exceed this size limit will appear as attachments in the e-mail, rather than being placed inline.
- Notes are only sent if the e-mail template includes the $NOTES() tag. For details, refer to the *SBM Application Administrator Guide*.

In the **Browser E-mail Template** section, select or edit the e-mail template for messages that users send from SBM items.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser E-mail Template</td>
<td>Select the default .txt or .htm file, or edit the template to create your own template. Users can format e-mail text using a Rich Text Editor; if you want this text to render correctly in the e-mail message that is sent, you must choose a .htm file. If Notification Server and the SBM Application Engine are installed on separate servers, you must restart IIS from the Manage Services tab after you change the browser e-mail template. For information on customizing e-mail templates, refer to Customizing E-mail Templates [page 161].</td>
</tr>
</tbody>
</table>

In the **Plugins** section, you register plugins to create additional notification channels in SBM. Notification channels enable you to send notifications to your users through different messaging mediums in addition to standard e-mail. The plugins are .jar files that contain libraries for the messaging service that you want to add. Once you add your desired plugins, you can add and configure new channels that consume the plugins in Application Administrator. For details, refer to "About Channels" in the *SBM Application Administrator Guide*.

**Important:** If you install and configure multiple instances of the notification server, you must register the same plugins on each server.

The following sample plugins are available with SBM:

- **Console**
Add this plugin and create an associated channel in Application Administrator to have notification messages written to the notification server log file ns.log. (Click **Open Log** to view logging information).

**Tip:** This plugin is useful if you want to create a channel that simply writes messages to the notification server log. This allows you to test notifications without actually sending e-mails.

- **RSS**
  Add this plugin and create a channel in Application Administrator to have notifications sent to an RSS feed.

- **Twitter**
  Add this plugin and create one or more associated channels in Application Administrator to have notifications broadcast to a specific Twitter wall that users can view.

- **XMPP**
  Add this plugin and create a channel in Application Administrator to have notifications sent to specific users in an IM client like Google Talk.

To register the sample plugins:

1. Click **Add**.
2. Browse to the following directory:

   installationDirectory\Serena\SBM\Common\Tomcat 7.0\server\default\webapps →\notificationsrv\default-plugins

3. Select a plugin .jar file, and then click **OK**. The plugin name and description appears in SBM Configurator.

4. Click **Apply** to register the plugins with SBM. After the services are restarted, the plugins are available from the **Channels** view in Application Administrator.

Certain plugins require authentication credentials to receive messages from SBM. If you configure a social network plugin for Twitter or Facebook, you must create a new account and an associated application by visiting the corresponding developer Web site (Twitter or Facebook). For more information about creating and registering plugins, visit http://www.serena.com/support and search for solution S139424.

In the **Common Options** section, configure the following options that apply to both the Notification Server and the Mail Client.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web services authentication user</td>
<td>Specify an SBM user account that the SBM Application Engine Web services should use for authentication when the E-mail Recorder receives an e-mail from a non-SBM user. This account is also used by the Notification Server to execute scripts and Web services for notifications without subscribers.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Logging Level</td>
<td>Select a logging level option that is appropriate for your needs. Click <strong>Open Log</strong> to view the current log.</td>
</tr>
<tr>
<td>Mail Server connection timeout</td>
<td>Use this option to set the number of seconds that should pass before connection attempts to your mail server time out. The default value is 120 seconds.</td>
</tr>
<tr>
<td>Web Services invocation timeout</td>
<td>Use this option as necessary to define the amount of time that is allotted for SBM to create your scheduled reports. The default value is 60 seconds. Note that if you increase the value to ensure that processing finishes, a greater timeout value will not affect processing time for smaller reports.</td>
</tr>
</tbody>
</table>

The Notification Server and Mail Client `ns.log` file is located here:

```
installationDirectory\Serena\SBM\Common\Tomcat 7.0\server\default\logs
```

The **Collect Log Files** button at the bottom of SBM Configurator captures the latest version of the log.

Consider increasing the logging level to help troubleshoot issues you encounter with sending notification messages or failures with e-mail submit and the E-mail Recorder feature. The following logging levels are available from the drop-down list:

- **Information**
  Displays the data source information and basic Notification Server actions such as reading change records, creating events, and sending messages. Use this option regularly to investigate problems with specific messages such as whether a condition has occurred for a notification to be sent and to whom the e-mail notification was sent. For Mail Client purposes, select this option if you want to log detailed information about e-mail submission, such as when a submission occurs.

- **Error**
  Displays more information related to the processing of the Notification Server and Mail Client. Problems with stopping and starting the service, thread counts and hangs, or other problems with running the services themselves are displayed here. Use this level to troubleshoot problems with sending messages and running the services.

- **Debug**
  Displays the most information and enables the SBM development team to troubleshoot problems. All of the details above are logged, in addition to more verbose logging for troubleshooting purposes.

For further help with diagnosing problems with the Notification Server and Mail Client, run the tests in the **Diagnostics** tab in SBM Configurator. These tests are helpful because they not only report problems, but also present solutions when possible. For more information, see *Static Diagnostics [page 135]*.
In the **Send Notification to Administrators on Errors** section, configure the following options to enable your administrators to be notified when problems occur.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin e-mail list</td>
<td>Enter a comma-separated list of administrator e-mail addresses.</td>
</tr>
<tr>
<td>Check errors every (in seconds)</td>
<td>Enter the number of seconds that should pass before the system scans for errors and e-mails the list above. The default is 60 seconds.</td>
</tr>
<tr>
<td>Send warning e-mail after a number of errors</td>
<td>Enter the number of errors that must occur before the system e-mails list above. A warning message is sent at the end of the check period if the number of errors that occur is greater or equal to the number of errors that you specify here. The default is 100 errors.</td>
</tr>
</tbody>
</table>

**About the Mail Client**

The primary functions of the Mail Client are e-mail submission and the E-mail Recorder feature:

- **E-mail Submission**
  
  The Mail Client accepts incoming e-mail messages and submits data from those messages as primary items. 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. You configure how the Mail Client handles HTML and attachments for e-mail submission in SBM Configurator; however, you establish e-mail submission for your SBM projects using the SBM Application Administrator. For details, refer to the *SBM Application Administrator Guide*.

  - **XML E-mail Submission**
    
    You can automate item submission from external tools by sending properly formatted XML via e-mail messages to a specified e-mail address. For details, refer to the *SBM Application Administrator Guide*.

    **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*. In general, orchestrations are the preferred method for automating submission of items. For guidance on using orchestrations, refer to the *SBM Orchestration Guide*.
• **E-mail Recorder**

  The E-mail Recorder feature automatically attaches e-mail messages sent from external e-mail clients as notes to primary and auxiliary items. E-mail Recorder also attaches replies to these messages, which enables users to record e-mail discussions that pertain to these items. In addition, E-mail Recorder can automatically attach a notification reply to the item that generated the notification.

  **Tip:** Administrators can enable or disable the E-mail Recorder feature on a project-by-project basis using SBM Application Administrator. E-mail Recorder is enabled for every project by default. You might consider disabling E-mail Recorder to prevent replies to messages from being logged in the originating item if it is not necessary for a given project.

  Notes that are created by the E-mail Recorder contain the To and CC contents of the incoming e-mail message in the **Message Address Details** section.

  E-mail Recorder enables users to:

  • **Reply to messages sent via E-mail Recorder and have their replies attached to items as notes**

    The reply must contain the [ttid: table ID,record ID] identifier and the To box must contain the name of the mailbox designated for the E-mail Recorder. This information is most easily provided when users select the **Reply to All** option in their external e-mail client.

  • **Reply to notifications and attach those replies to the related items**

    By default, the To box contains the name of the mailbox designated for the E-mail Recorder and the subject line contains the [ttid: table ID,record ID] identifier. The reply is only attached to the relevant internal SBM items if the mailbox name and the identifier are left intact. The identifier can be specified in either the subject or body of the reply.

  • **Use the Preferred E-mail Client link when sending an e-mail from an item**

    A new message dialog box from the external e-mail client opens, allowing users to send a message to other SBM users and non-users as well. Messages sent from an external mail client are only attached to SBM items if E-mail Recorder is enabled. If E-mail Recorder is not enabled, messages sent using the Preferred E-mail Client option are not attached to items.

    • The new message dialog box contains the name of the mailbox designated for the E-mail Recorder, a subject line specifying the user who sends the message, and the item the message is sent from, and, optionally, a link to the item.

    • By default, the subject line contains the database table and record ID for the item in the following format: [ttid: table ID, record ID]. If this database identifier is removed from the subject line, the e-mail message is sent, but not attached to the item unless the identifier is added to the message body. The message is sent and deleted from the mailbox used by the Mail Client if it cannot identify the ttid in the subject line or message body.

    • The message body that is sent from an external e-mail client is attached by the E-mail Recorder; however, attachments are only added to the item if you have selected the **Include Attachments When Using E-mail Recorder** option.
• Non-users can read the information in the e-mail message, but they cannot access the item from which the message was sent. You can, however, specify that replies from users are added as notes by enabling E-mail Recorder.

**Configuring the Mail Client**

This section describes configuration settings for the **Mail Client**. For distributed installations, you configure these mail server settings directly on the server or servers where the **Mail Client** is installed. You can change these settings any time after installation by running SBM Configurator in **utility mode**.

To configure the **Mail Client**, select the **Enable Mail Client** check box, and then select a **Protocol** from the drop-down list.

**Note:** The **Advanced** button is used by Serena for troubleshooting purposes only.

- **POP3 and IMAP Options [page 101]**
- **Exchange Options [page 102]**
- **Configuring E-mail Submission [page 103]**
- **Configuring E-mail Recorder [page 105]**

**POP3 and IMAP Options**

For each SBM project that will accept e-mail submissions, you or a network administrator must dedicate a mailbox under the POP3 or IMAP protocol. The SBM administrator must know the mailbox name and password for the mailbox; users who will submit via e-mail must know the e-mail address for the mailbox.

To configure **POP3** or **IMAP** mail server options for the **Mail Client**, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the IP address or host name of the mail server that hosts mailboxes that can be used for e-mail submission. These mailboxes will receive incoming e-mails, which will be used to create items in SBM.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number used by the mail server. By default, the port number is set to 110 for POP3 mail servers and 143 for IMAP.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Select this option to send and receive messages through a secure connection.</td>
</tr>
<tr>
<td>Port is SSL dedicated</td>
<td>Select this option if you know that the server requires an SSL-dedicated port. Otherwise, to use SSL encryption in the standard way, clear this check box.</td>
</tr>
</tbody>
</table>
### Include HTML formatted e-mail messages

Select this option to include HTML-based text from an incoming e-mail message for e-mail submissions and the E-mail Recorder.

- This prevents messages containing HTML-based text from being dropped.
- If this option is selected, the Mail Client processes messages that contain "text/plain" and "text/html".
- Clear the check box to force the Mail Client to only process plain text messages.

### Delete e-mail messages after processing

Select this option to have the Mail Client delete messages from your mail boxes after the message has been processed successfully.

- If this option is enabled for the POP3 protocol, messages are always deleted. If this option is disabled, the message is deleted if it is processed successfully, and left marked as unread if processing fails.
- If this option is enabled for the IMAP protocol, messages are only deleted if they are processed successfully. If this option is disabled, messages are only marked as read (regardless whether they are processed successfully or not).
- If this option is disabled, messages are processed and only marked as read (not deleted). This means unread messages may collect in the mailbox and the Mail Client will attempt to process them on every cycle until they are manually deleted.

If you use a self-signed SSL certificate, you must add the certificate to the Java VM truststore. Use the Manage Trusted Certificates option on the Tomcat Server tab to add the certificate.

### Exchange Options

Use the Exchange (via Web services) protocol to communicate directly with an Exchange server using the MS Exchange Web services API. You might use this option if your company does not allow connection through POP3 or IMAP. If no such restriction exists, consider choosing one of these options because they enable faster connection speeds than MS Exchange.

To configure the Mail Client to use Exchange, provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange version</td>
<td>Select the current version of your Exchange server.</td>
</tr>
<tr>
<td>Service URL</td>
<td>Enter the service URL for your Exchange server. For example:</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Include HTML formatted e-mail messages</td>
<td>Select this option to include HTML-based text from an incoming e-mail message for e-mail submissions and the E-mail Recorder.</td>
</tr>
<tr>
<td></td>
<td>• This prevents messages containing HTML-based text from being dropped.</td>
</tr>
<tr>
<td></td>
<td>• If this option is selected, the Mail Client processes messages that contain &quot;text/plain&quot; and &quot;text/html&quot;.</td>
</tr>
<tr>
<td></td>
<td>• Clear the check box to force the Mail Client to only process plain text messages.</td>
</tr>
<tr>
<td>Delete e-mail messages after processing</td>
<td>Select this option to have the Mail Client delete messages from your mail boxes after the message has been processed successfully. If this option is disabled, messages are processed and only marked as read (regardless whether they are processed successfully or not).</td>
</tr>
</tbody>
</table>

If the Exchange Service URL is secured by SSL, you must provide the certificate authority (CA) chain that signed the endpoint certificate. This means that you must add the public certificate of each CA in the certificate chain to the Tomcat truststore. If the endpoint is secured via SSL, use the Manage Trusted Certificates option on the Tomcat Server tab to import the certificates and trust the chain that signed the endpoint's SSL certificate.

**Configuring E-mail Submission**

You configure how the Mail Client handles HTML and attachments for e-mail submission in SBM Configurator. You designate mailboxes and map fields for e-mail submission in SBM Application Administrator. For details, refer to the *SBM Application Administrator Guide*.

💡 **Tip:** Serena recommends that e-mails submission file attachments be limited to less than 100 MB. If larger files must be attached to items, users should attach them by logging in and attaching the files.
In the **E-mail submission** section, configure the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Use HTML e-mail section | Select this option to tell the Mail Client which part of an e-mail message should be included in the submitted item if both plain text and HTML parts are present in the e-mail message.  
  - This option is only applicable if **Include HTML formatted e-mail messages** is selected.  
  - This option is useful when combined with the **Attach HTML e-mail as PDF** option below.  
  - If HTML rendering is disabled due to security concerns, then disabling **Use HTML e-mail section** is preferable so that only plain text is attached (instead of attaching text with HTML tags that is more difficult to read). |
| Attach HTML e-mail as PDF | Select this option to attach "text/html" formatted e-mails as PDF attachments to the SBM item (in addition to the field mappings you define in Application Administrator).  
  - This option is only applicable if **Include HTML formatted e-mail messages** is selected.  
  - This option is useful if you receive incoming e-mails with HTML and embedded images because it preserves the text and image sequence in the original e-mail.  
  - The Mail Client host machine must have at least one .ttf Unicode font installed in the Windows font directory to ensure that high-ASCII characters appear in the resultant PDF.  
  - You can customize the following .css file to set the preferred font:  
    \notificationsrv.war\WEB-INF\classes\pdf.css  
  - Contact Support or visit the Knowledgebase at [serena.com](http://serena.com) for help with modifying the size or layout of the resultant PDF. |
| Include embedded attachments | By default, attachments embedded in e-mail submissions are ignored. Select this check box to add all embedded attachments, including e-mail signatures, to submitted items. This setting applies to all e-mail submissions. |

The following tables describe how messages are processed depending on the message content type and the various combinations of the **Use HTML e-mail section** and **Attach HTML e-mail as PDF** options.

### Table 1. text/plain messages
<table>
<thead>
<tr>
<th>Use HTML e-mail section</th>
<th>Attach HTML e-mail as PDF</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>PDF is not generated and only plain text is submitted</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>PDF is not generated and only plain text is submitted</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>PDF is not generated and only plain text is submitted</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>PDF is not generated and only plain text is submitted</td>
</tr>
</tbody>
</table>

Table 2. text/html messages

<table>
<thead>
<tr>
<th>Use HTML e-mail section</th>
<th>Attach HTML e-mail as PDF</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>PDF is generated and HTML is submitted</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>PDF is not generated and HTML is submitted</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>PDF is generated and only plain text is submitted</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>PDF is not generated and only plain text is submitted</td>
</tr>
</tbody>
</table>

The behavior is the same for incoming e-mails that are “multipart/alternative” depending on whether the type of a particular part is “text/plain” or “text/html”.

**Configuring E-mail Recorder**

On your mail server, create a dedicated E-mail Recorder mailbox using either the POP3, IMAP, or Exchange server protocols. These mailboxes are typically configured by an IT department or network administrator. The mailbox can have any name, but the SBM administrator must know the name and password for this mailbox.

**Note:** The E-mail Recorder mailbox is not added to the To line when users reply to notifications sent by a MAPI mail server.

Review the following information before using E-mail Recorder:

- You configure how the Mail Client handles HTML and attachments for e-mail submission in SBM Configurator; however, you establish e-mail submission for your SBM projects using the SBM Application Administrator.
• The E-mail Recorder mailbox cannot be used for other Mail Client functions, such as e-mail submission or cross-database posting.

• E-mail messages are attached to items in the order they are received.

• HTML is rendered in notes that are created by the E-mail Recorder only if Include HTML formatted e-mail messages is selected in SBM Configurator and Render HTML in Notes is selected in SBM System Administrator.

• By default, e-mail messages that are sent using an external e-mail client are set as restricted, meaning that only users who have privileges to view notes for a particular item can view the attached e-mail. To set an e-mail message sent from an external e-mail client as "unrestricted", users must edit the e-mail message after it is attached to the item as a note and select the Unrestricted check box on the Add/Modify Note dialog box. This enables users who can view the item to view the attached e-mail messages.

• Messages are deleted if they do not contain a valid [ttid: table ID, record ID] string from the mailbox dedicated for E-mail Recorder. To avoid losing e-mail messages not sent by the E-mail Recorder, Serena recommends you do not use the specified mailbox for any other purpose.

• E-mail Recorder messages that are attached to SBM items only display the reply portion of an e-mail reply by default. If users want to view the previous e-mail text, they can toggle the view using the show and hide options while viewing the item. Hiding the prior message text improves the overall readability of E-mail Recorder messages on items.

To enable the E-mail Recorder feature, select Enable E-mail Recorder check box and provide the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login name</td>
<td>Enter the login or user name of the mailbox account that will be dedicated to E-mail Recorder.</td>
</tr>
<tr>
<td>Mailbox e-mail address</td>
<td>Enter the e-mail address of the mailbox. This address appears in the To box in e-mail messages sent using E-mail Recorder.</td>
</tr>
<tr>
<td>Mailbox password</td>
<td>Enter the mailbox password.</td>
</tr>
<tr>
<td>Password verification</td>
<td>Verify the mailbox password.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Only if "From" matches an SBM user | Select this option to limit the e-mail messages that are attached to items to those sent by users in your system with a matching e-mail address.  
- If this option is selected, you must grant users the **Add Note** privilege for the necessary projects and/or auxiliary tables. Users do not need to be granted **Add Note** privileges to attach external e-mail messages to items as notes.  
- Clear the check box to allow non-users to attach e-mail messages to items as notes.  
- This option may be useful for tracking correspondence from customers or partners, but use caution because it allows unauthorized users to add e-mail messages as notes to items in your system. |
| Restrict size of e-mailed notes | Enter the maximum number of characters that can be added as a note to limit the size of attached e-mail messages.  
- The character limit applies to individual e-mail messages.  
- For example, if you specify a 500-character limit, each e-mail message attached to an item can contain no more than 500 characters.  
- Messages larger than the specified character limit are truncated once the limit is reached.  
- The default value is 0 (in which no limit is imposed).  
- The **show** and **hide** viewing options do not apply to e-mail messages that have been truncated by this setting. |
| Use HTML e-mail section | Select this option to tell the Mail Client which part of an e-mail message should be included in the submitted item if both plain text and HTML parts are present in the e-mail message.  
- This option is only applicable if **Include HTML formatted e-mail messages** is selected.  
- This option is useful when combined with the **Attach HTML e-mail as PDF** option below.  
- If HTML rendering is disabled due to security concerns, then disabling **Use HTML e-mail section** is preferable so that only plain text is attached (instead of attaching text with HTML tags that is more difficult to read). |
### Field Description

**Attach HTML e-mail as PDF**
- Select this option to attach "text/html" formatted e-mails as PDF attachments to the SBM item.
  - This option is only applicable if **Include HTML formatted e-mail messages** is selected.
  - This option is useful if you receive incoming e-mails with HTML and embedded images because it preserves the text and image sequence in the original e-mail.
  - The Mail Client host machine must have at least one .ttf Unicode font installed in the Windows font directory to ensure that high-ASCII characters appear in the resultant PDF.
  - You can customize the following .css file to set the preferred font:
    \notificationsrv.war\WEB-INF\classes\pdf.css
  - Contact Support or visit the Knowledgebase at serena.com for help with modifying the size or layout of the resultant PDF.

**Include attachments when using e-mail recorder**
- Select this option to attach files included with e-mail messages to items.
  - If you require that incoming messages be sent by SBM users, the e-mail address must match that of a user who has privileges to add attachments to items in the project.
  - If this user does not have privileges to add notes but has privileges to add attachments, then only the attachments are added to items.
  - If this user only has privileges to add notes, but not attachments, then only the notes are added to items.

**Insert e-mail as note**
- Select this option to attach e-mail messages that are sent from items as notes to those items.
  - Once the e-mail is sent, the message appears in the **Notes** section of the SBM item.
  - The **Message Address Details** portion of the note contains the To and CC contents of the e-mail. Replies that are added through E-mail Recorder also display these details in the notes that are created.

The following tables describe how messages are processed depending on the message content type and the various combinations of the **Use HTML e-mail section** and **Attach HTML e-mail as PDF** options.

#### Table 3. text/plain messages
<table>
<thead>
<tr>
<th>Use HTML e-mail section</th>
<th>Attach HTML e-mail as PDF</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabled</td>
<td>Enabled</td>
<td>PDF is not generated and only plain text is attached</td>
</tr>
<tr>
<td>Enabled</td>
<td>Disabled</td>
<td>PDF is not generated and only plain text is attached</td>
</tr>
<tr>
<td>Disabled</td>
<td>Enabled</td>
<td>PDF is not generated and only plain text is attached</td>
</tr>
<tr>
<td>Disabled</td>
<td>Disabled</td>
<td>PDF is not generated and only plain text is attached</td>
</tr>
</tbody>
</table>

The behavior is the same for incoming e-mails that are “multipart/alternative” depending on whether the type of a particular part is “text/plain” or “text/html”.

### Application Repository and Event Manager Mail Services

The Application Repository and Event Manager can be configured to connect to POP3 and SMTP servers for the following features:

- **Event creation via e-mail**
  
The Web service–based event mechanism exposed by SBM can accept events either through HTTP or via e-mail. Events through HTTP are enabled by default and require no additional configuration beyond the basic installation of SBM. Events through e-mail require that SBM be configured to access a POP3 e-mail mailbox provided by an external e-mail server.

- **Application Repository and Event Manager notifications**
  
By configuring an SMTP server, an e-mail notification can be sent when the Event Manager fails to process an event or when an activity fails in Application Repository.
Configuring Application Repository and Event Manager Mail Services

This section describes configuration settings for the Application Repository and Event Manager mail services. For distributed installations, you configure these settings directly on the Event Manager and Application Repository servers. The SMTP settings apply to both the Event Manager and Application Repository. If these components are installed separately, update each server with the SMTP server information. You can change these settings any time after installation by running SBM Configurator in utility mode.

- POP3 Options [page 110]
- SMTP Options [page 111]

**POP3 Options**

The SBM Event Manager can only receive events from a POP3-compliant mail server. To use this feature, you must set up a dedicated account on the POP3 server and establish an e-mail address that you want to use to accept the e-mailed event requests.

SBM can retrieve the ALF event from either a plain text body (single part e-mail message) or the last plain text part of a multi-part message. SBM does not process single part messages that contain only HTML. Some POP3 mail servers are able to convert single part HTML messages into multi-part messages that also contain plain text equivalent HTML. If you are using this type of POP3 mail server, you can send HTML-only messages as well.

To enable the Event Manager to process incoming e-mails, select the **Use POP3 Mail Server for the Event Manager** check box and enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>The network name of your POP3 e-mail server. The local host name appears by default; however, it is likely that your mail server resides on a different machine.</td>
</tr>
<tr>
<td>Port</td>
<td>The port used by the POP3 e-mail server. POP3 typically uses port 110.</td>
</tr>
<tr>
<td>Use SSL</td>
<td>Enable SSL to receive messages through a secure connection. The default SSL port is 995.</td>
</tr>
<tr>
<td>User name</td>
<td>The e-mail account name for the inbox that your POP3 server provides.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the e-mail account.</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Enter the password again to confirm it.</td>
</tr>
</tbody>
</table>
SMTP Options

To enable the Event Manager and Application Repository to send e-mail notifications, select the **Use SMTP Mail Server for the Event Manager and Application Repository** check box, and then enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the SMTP server host name.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the SMTP server port number.</td>
</tr>
<tr>
<td>Notification &quot;From&quot; e-mail address</td>
<td>Enter the &quot;From&quot; address that appears for failure notification messages from the Event Manager.</td>
</tr>
</tbody>
</table>

Common Services

In the **Common Services** tab, you configure features that are powered by SBM Common Services.

The **Common Services** tab is available on the server that hosts SBM Application Engine if Serena Release Control or Serena Service Manager is installed. If you create a Tomcat cluster for SBM Common Services, you select the node that runs the Relationship Service on this tab. (The Relationship Service is only available with Serena Release Control.) This instructs SBM Application Engine as to which node in the cluster will run the Relationship Service.

Tip: You can manually type a host name that is not one of the nodes in the cluster if your Relationship Service instance is not part of a cluster.

Configuring the Work Center Search Engine

In the **Work Center Search Engine** tab, you configure settings for Smart Search—the search engine that provides sophisticated search capabilities by automatically indexing the content of items and files and notes that have been added to items. For distributed installations, you configure Smart Search settings directly on the SBM server that hosts SBM Common Services.

- Smart Search Settings [page 111]
- Attachment Directory Access [page 113]

Smart Search Settings

Smart Search operates on pre-built indices. For SBM upgrades, the index building begins once Tomcat is started for the first time after you upgrade your installation. The complete indexing operation can take significant time to finish for very large databases; however, some search results in Work Center begin to appear immediately and the number of results continues to grow while the initial indexing operation works toward completion.

Indexing is also performed on information in most file attachments that contain text (PDF and Microsoft Word, for example). For large documents, only the first 1 million characters are indexed and searchable.
You can view the overall progress of the indexing operation in the ssf.log file located on the server that hosts SBM Common Services. The log file is located here:

installationDirectory\Serena\SBM\Common\Tomcat 7.0\server\default\logs

Use the following options to configure Smart Search Settings:

- **Indexer directory path**
  
  Specify a directory to host the Smart Search index files. The index files are used to enhance the searches that users perform in the browser. To increase the overall search response time, consider hosting the indexer on a separate dedicated host machine.

  **Important:** If you host the indexer on a separate server, you must enter the UNC path and ensure that the Tomcat user identity has full permissions to the specified directory. Click **Test** to verify that the directory is accessible.

  You can increase scalability and improve search query throughput by clustering the SBM Common Services component on multiple servers. For more information about creating a cluster, see Clustering Server Components [page 49].

  If you configure Smart Search settings in a Tomcat cluster with multiple instances of SBM Common Services, note the following important information:

  - The indexer directory must be hosted on a server that is outside of the cluster.
  
  - This server must be accessible to all of the SBM server components in the cluster. This means that the same network path must be specified identically on each node in the cluster.
  
  - Each node in the cluster must contain identical Smart Search configuration settings; therefore, it is recommended that you configure the Smart Search settings on one node, export the settings to a snapshot configuration file, and then import the file into the other nodes in the cluster. This ensures that all nodes in the cluster contain identical Smart Search settings.
  
  - The indexer directory must be shared using simple file sharing in Windows (not advanced sharing).

- **Expected search usage**
  
  Smart Search adjusts internal parameters accordingly depending on how often your users perform searches. Select a usage indicator to control how many threads are spawned to perform indexing.

  **Tip:** The **Medium** setting should be sufficient, unless a very high volume of data is being added to the system (greater than 60 items per second).

- **Database polling interval**
Select a polling interval to control how often the service should poll the database to learn about new search strings and new related articles.

**Note:** The default Smart Search polling interval is 30 seconds; this means that by default, Work Center searches will return related items 30 seconds after the items have been created. If you change the polling interval to **Never**, search results in Work Center do not return results for items that are created after this change. Consider lowering the interval to 5 or 10 seconds to find newly-submitted items in search results sooner.

- **Re-Index**

  Use this option to reset the indexer. This operation cleans the current index by removing learned search strings and related articles that have been saved in the index.

  **Note:** URL attachments (such as links to an external Web site or to a page within SBM) and attachments marked as "restricted" are not indexed and returned in Work Center search results by default. To add them to search results, follow the steps in solution S141365.

**Attachment Directory Access**

SBM Common Services returns attachments for searches that are performed by users in Work Center. If your SBM item attachments are stored in the database, Work Center will access the database to return file attachments in search results, and no additional configuration is necessary in SBM Configurator. However, if your SBM item attachments are stored on the file system, you must provide the attachments directory and access information to SBM Common Services.

To configure attachment access information for SBM Common Services:

1. Enter the location of the attachments directory. The path might be different than what is specified in SBM System Administrator, but the ultimate location must be the same attachments directory.
   For example, you can specify a shared network drive:

   `\servername\file_attachments`

2. Enter the authentication credentials in the **User** and **Password** fields.
   If you did not enter credentials in SBM System Administrator because the attachment directory is on the same server, select the check box to use the current Tomcat identity to access the attachments directory. If the attachments directory is located on a remote server, you must ensure that the current Tomcat identity has permissions to the directory.

   **Tip:** To change the attachments directory location for SBM, change the file path in SBM System Administrator first, and then update the path in SBM Configurator if necessary.

**Advanced Settings**

From the **Advanced** menu, you can configure advanced system settings for performance, security, and proxy servers. The **Advanced** menu is only available during **utility mode**.
Performance

Use the options in the Performance tab to manage performance settings for the Notification Server, Web Services, and orchestrations. The performance options for each component only appear if the related component is installed on your local machine. Review these settings to ensure that your SBM system performance is optimized.

For some additional recommendations on tuning Tomcat memory consumption and SBM performance, refer to solution S141569.

- Notification Server Performance [page 114]
- Throttling Web Services [page 115]
- Throttling Orchestrations [page 117]
- Removing Successful Event Manager Log Entries on Completion [page 118]

Notification Server Performance

This section describes how to configure performance settings for the SBM Mail Services. For distributed installations, you configure these settings directly on the server or servers where the SBM Mail Services are installed.

- Process Rate Control Settings
  These settings control how often the Notification Server cycles through new change records that are generated by users, creates events based off those changes, and sends messages according your notification rules. This setting impacts the load bearing capabilities of the Notification Server.

  To configure process rate settings for the Notification Server, use the slider to change the process rate level to one of the following options:

  - **Minimum load level** – At this level, the average cycle rate is two minutes. Use this setting if your users generate very few changes.
  - **Low load level** – At this level, the average cycle rate is one to two minutes. Use this setting if your users generate occasional changes.
  - **Average load level** – At this level, the average cycle rate is one minute. Use this setting if your users generate consistent changes.
  - **High load level** – At this level, the average cycle rate is thirty second. Use this setting if your users make several changes often.
  - **Max load level** – At this level, the average cycle rate is five to ten seconds. Use this setting if several of your users make numerous changes daily.

- Cache Expiration Time Control Settings
  The Notification Server uses the ehCache framework to store data in the local cache from several tables in the SBM Application Engine database. The reliance of this cache has a direct impact on the system's performance, so consider monitoring and adjusting the cache limit as necessary.

  - If you find that SBM performance on this machine is suffering, consider increasing the Notification Server's cache level, which decreases the number of database reads made by the Notification Server.
• If you find that the performance of the Notification Server itself is lagging, you could decrease the cache level, thereby decreasing the Notification Server’s dependency on system memory and forcing more direct database reads, which will improve Notification Server processing times but may affect other server components.

• To configure cache expiration time limit options for the Notification Server, use the slider to change the cache level.
  • Low cache capability – This setting forces the Notification Server to consume much less memory, but increases usage of the database for table reads.
  • Average cache capability – At this level, the Notification Server attempts to evenly balance both system memory consumption and database usage for table reads.
  • Max cache capability – This setting forces the Notification Server to consume a greater amount of memory, but decreases usage of the database for table reads.

• Skip changes for
  Use this slider to set the time period for which changes should be skipped by the Notification Server for a particular item after the first notification is sent.
  • The default value is sixty seconds.
  • This means that after processing an initial change and sending a notification, the rest of the changes that occur against the item for the next sixty seconds are skipped before a new change is processed and another notification is sent.
  • This setting is useful if you do not want to receive all of the notification messages that are generated when an item is moved from state to state in rapid succession. These messages might become redundant if the item is transitioned several times, and you might not want to receive all the notification messages that were generated while the item was still in flux.

• Attempt to send all Notifications for an item
  Select this option to have the Notification Server attempt to send every applicable notification for an item, regardless if the notifications might no longer be applicable.
  • Normally the Notification Server does not send e-mail messages each time an item changes state if the changes happen in rapid succession. Instead, the service assumes that an e-mail should be sent for only the last state change that occurs.
  • If you enable this setting, the Notification Server attempts to send messages for each individual change that occurred, even if the change is no longer relevant to the current status of the item.
  • Once this option is selected, the following slider control is not applicable.

**Throttling Web Services**

SBM Application Engine and SBM Orchestration Engine can potentially invoke several Web service calls depending on your usage and configuration model. To manage these calls,
you can adjust performance settings in SBM Configurator to "throttle" the Web service activities for each component. You can also throttle Web services to safeguard against denial of service attacks or inadvertent high-volume repeat Web service invocations. When a threshold has been reached, subsequent calls are rejected. The Common Log is updated with these failures.

The SBM Application Engine calls referred to in this topic refer to calls made directly into the SBM Application Engine Web services provided by SBM. Calls made to third-party Web services are not affected by the settings in this file.

**Important:** If you change the throttling settings any time after the initial installation and configuration, you must apply the changes to each Tomcat server in your installation. For example, if you modify throttling settings for SBM Orchestration Engine, you must run SBM Configurator on each Tomcat server and use the Update From Database option or use configuration snapshot files to update each server.

The following table describes the throttling settings you apply on the SBM Application Engine server:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Web services invocation timeout            | Designate the amount of time SBM should wait for a Web service to return calls. This setting applies to Web service functions assigned to transitions, states, and notifications. The default setting is 30 seconds.  
**Note:** This setting is also used as the time to wait for a synchronous orchestration reply from ODE. The timeout value that you specify controls the amount of time that the system will wait for an synchronous orchestration to complete. If your orchestration is consistently taking longer than sixty seconds to finish, consider changing the orchestration from synchronous to asynchronous instead of increasing the specified timeout. |
| Maximum number of invocations ... In duration | Enter the maximum number of allowed SBM Application Engine Web service invocations per second.                                                                                                          |
| Maximum payload size                       | Enter the maximum threshold size for the payload (amount of data) that is sent with a Web service call (for calls into SBM Application Engine Web services).                                                  |
| Send throttle notifications to             | Select this check box and enter an e-mail account to receive notifications when a limit has been reached. The e-mail account does not need to be associated with an SBM user.                              |

In the **Whitelisted users** table, set specific throttling parameters for a particular user or users that can override the default settings defined above. You may find this useful if you often designate a single user to perform all your Web service calls (perhaps from within...
an orchestration). For example, you can "whitelist" a certain user account that is used only for authentication purposes in Web service calls, which thereby requires a higher threshold.

**To "whitelist" specific user accounts:**

1. Click **Add**.
2. Enter the user login ID.
3. Enter the maximum number of allowed Web service invocations.
4. Enter the number of seconds.
5. Enter the maximum payload size.

**Note:** The **Whitelisted users** table only applies to SBM Application Engine Web service calls.

### Throttling Orchestrations

On the SBM Orchestration Engine server, you can throttle the activity and load handling behavior for the Orchestration Engine. By default, SBM allows 40 simultaneous orchestration executions (either synchronous or asynchronous) whether you enable or disable throttling for orchestrations. You can adjust this value to control the trade off between delays in orchestration processing and server resource usage in order to avoid out-of-memory conditions from occurring while the server is under load. The values that you set depend on the computing resources available to the SBM Orchestration Engine server and how your orchestration workflows use those resources.

To properly adjust the throttling controls for your environment, consider the following:

- Reducing the number lowers the risk of an out-of-memory condition, but it might delay orchestration workflows from finishing because they have to wait to execute. For synchronous orchestrations, this delay might cause timeouts that are undesirable for users.

- Increasing the number raises the risk of an out-of-memory condition, but it enables more requests to be processed immediately.

- The optimal setting balances the two extremes for a particular process app. If your orchestration workflows perform a lot of calculation, then allowing less concurrency might prove optimal. If the orchestration workflows mostly call Web services, then allowing more concurrency might help.

Determining the optimal settings is likely a matter of trial and error; however, changing the default value is not generally necessary unless you are experiencing out-of-memory conditions or delays in orchestration execution. If both conditions exist, then consider increasing the amount of memory or CPU, or create a cluster for the SBM Orchestration Engine.

The following table describes the throttling settings that you apply on the SBM Orchestration Engine server. Change the values as necessary to increase or decrease the maximum number of allowed simultaneous executions.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of simultaneous executions</td>
<td>Enter the maximum number of orchestrations that can be executed at the same time. Orchestrations are processed according to when they are received and the priority that is assigned to the event definition in SBM Composer.</td>
</tr>
</tbody>
</table>
| Maximum payload size                          | Enter the maximum payload size for Web service responses that can be received by the SBM Orchestration Engine.  

**Tip:** Once you enable throttling, this setting acts as protection against unexpected large responses. Any response that is received that is larger than the amount specified is rejected and an entry is added to the Orchestration Engine log file. |

Additionally, for details on configuring SBM process timeout execution, refer to solution S141751.

**Removing Successful Event Manager Log Entries on Completion**

Select the *Remove all successful Event Logs upon completion* check box to have the system automatically remove Event Log records for events that are processed successfully on the first attempt. Note that this option is disabled if the database has not been initialized, or no event data has been processed. You can select this option once the system has processed an asynchronous orchestration.

**Security**

Use the **Security** tab to configure advanced security settings and features for SBM.

**Important:** You must generate new certificates in the **Secure SBM** tab in order to properly secure your installation. For more information, see [Securing SBM](#) [page 118].

- Securing SBM [page 118]
- Securing SSO [page 122]
- Configuring Client Certificate Authentication [page 124]
- Securing Anonymous Events [page 130]
- Securing Integrations [page 131]

**Securing SBM**

In the **Secure SBM** tab, you generate, export, or import key pairs (certificates with their private signing keys) to secure connections in your SBM installation. Configuring trust keys ensures greater security for your entire SBM installation.

- Securing Your Installation [page 119]
- Working With Trust Keys [page 120]
Securing Your Installation

SBM Configurator warns you if your installation currently uses default certificates (which should be replaced) or if your current certificates will expire soon.

Important: To properly secure your installation, you must generate new key pairs even if you do not plan to use SSO. If you do not generate new key pairs, then the default certificates that the Security Server inherently trusts are used. To increase security, click Generate All to create new unique certificate for all components.

The steps that you perform to secure your installation depend on your installation type. Determine your installation type from the list below, then follow the corresponding steps:

• Single server installation – All SBM components are installed on a single server.

• Distributed server installation – SBM components are installed on multiple servers that comprise a single production environment.

• Multiple environment installation (or "path to production") – SBM components are installed on single or multiple servers that are separated into multiple SBM environments (such as development, test, and production).

To secure SBM in a single server installation:

1. Launch SBM Configurator.
2. Click the Security tab.
3. Click the Secure SBM sub-tab.
4. Click the Generate All button. This operation creates new unique key pairs.
5. Click the Apply button.

To secure SBM in a distributed server installation:

1. Launch SBM Configurator on the server that hosts the Single Sign-On (SSO) component. (View the Components tab in SBM Configurator to determine which server has SSO installed if you are not sure).
2. Click the Security tab.
3. Click the Secure SBM sub-tab.
4. Click the Generate All button. This operation creates new unique key pairs.
5. Click the Apply button.

If you are using the Configuration Settings database to store the configuration from all servers in a centralized location, click Update From Database, and then Apply on your other servers. You have now successfully secured your entire installation.
If you are not using the **Configuration Settings** database, proceed with the next step.

6. Click the **Export All** button. This operation creates a .zip file that contains the new unique key pairs. Enter a password for the keystores in the .zip file and save the file locally.

7. Copy the .zip file to each other server in your distributed installation.

8. Navigate to the **Secure SBM** sub-tab on each server and click the **Import All** button. Browse to the .zip file that you saved in the previous step.

**To secure SBM in a multi-environment (path to production) installation:**

1. Launch SBM Configurator on the production server that hosts the Single Sign-On (SSO) component. (View the **Components** tab in SBM Configurator to determine which server has SSO installed if you are not sure).

2. Click the **Security** tab.

3. Click the **Secure SBM** sub-tab.

4. Click the **Generate All** button. This operation creates new unique key pairs.

5. Click the **Apply** button.

   If you are using the **Configuration Settings** database to store the configuration from all servers in a centralized location, click **Update From Database**, and then **Apply** on your other servers. You have now successfully secured your entire multi-environment installation.

   If you are not using the **Configuration Settings** database, proceed with the next step.

6. Click the **Export All** button. This operation creates a .zip file that contains the new unique key pairs. Enter a password for the keystores in the .zip file and save the file locally.

7. Copy the .zip file to each of the other servers in each of the environments throughout your installation.

8. Navigate to the **Secure SBM** sub-tab on each server and click the **Import All** button. Browse to the .zip file that you saved in the previous step.

**Note:** Additionally, if you choose to enable SSO, you can secure connections from the end-user browser into the SSO Security Server by selecting **Use HTTPS for SSO login** on the **General** tab.

**Working With Trust Keys**

You can also generate, import, and export key pairs for individual components in **utility mode**. You can use the options in the **Actions** menu to establish trust relationships with other Serena products.
In the Trust Keys section, click the Actions link, and then select one of the following options:

- **Generate key pair** – Click Generate Key pair to create a new unique signing key. For example, you can generate a new key pair for each component that is listed in the Components group box to create a unique trust between the selected component and the other SBM entities on the server.

- **Import key pair** – Click Import Key pair if you want to import key pairs. This does not import the certificates that are exported from SBM Configurator; instead, it imports a key pair that has been generated outside of SBM Configurator.

- **Export Key pair** – Click Export Key pair if you want to export a key pair for a selected component.

- **Export Certificate** – If you have integrated SBM with other Serena products that use SSO, their truststores need to be updated as well. SBM Configurator cannot perform the update on these other products; therefore, click Export Certificate to export the certificate and save it as a local file and then import it into each product's truststore manually. Please refer to the documentation for these other products for assistance with importing the certificate.

**Web Application Firewall**

This option controls the ModSecurity web application firewall in SBM, which enables you to implement tighter security screening for your SBM installation. You can choose to enable threat detection logging (via the Log option), or threat detection logging and request filtering (via the Block option) depending on your needs. For details on ModSecurity, refer to https://www.modsecurity.org/.

This feature enables Serena to address security concerns quickly, in a focused manner without the need to install a patch or upgrade to address potential vulnerabilities. For example, if a vulnerability is discovered, Serena can provide a ModSecurity configuration rule that addresses the issue.

Note that the default configuration that is provided by Serena contains a basic set of rules that tighten system security; however, you will ultimately need to customize the ModSecurity rules in order to block specific requests or threats as necessary.

The web application firewall is enabled via a module (ModSecurity IIS) in IIS that SBM Configurator adds to each SBM application in IIS. The module uses a set of pre-defined rules in configuration files that are located in the following directory:

```
installationDirectory\Serena\SBM\Application Engine\modsecurity\conf
```

If you add or modify any rules in the configuration files, you must reset IIS for the changes to take effect. For more information about ModSecurity rules, refer to solution S141332.

Select one of the following options to configure the firewall:

- **Log**

  Enables threat detection logging only. Captures potential vulnerabilities and writes them to the Application Event Log on the SBM Application Engine server.

- **Block**
Enables threat detection logging and filters requests (according to your configuration rules) that are considered dangerous.

- **Off**

  No threat detection or filtering is enabled. This is the default option.

  **Note:** If you add an external application in IIS, you must manually configure the application’s native modules and select the **ModSecurity IIS** module to enable the same level of threat detection and prevention that is configured on the default SBM applications.

### Enabling Legacy SSL Protocols

If your system requires older versions of the SSL and TLS protocols (such as v3.0, 2.0, 1.0, and TLS 1.0), select the **Enable legacy SSL protocols** check box to allow SBM to use these protocols. Use caution, however, as these older versions contain known security vulnerabilities that could expose your system to malicious attacks. Serena recommends that you do not enable legacy protocols unless absolutely necessary.

### Securing SSO

In the **Secure SSO** tab, you configure settings to secure SSO for your SBM installation. You can configure the following settings at any time in utility mode.

- **Setting the SSO Session Lifetime** [page 122]
- **Establishing SSL for the SSO Log in** [page 123]
- **Updating SSO Keystores** [page 123]
- **Encrypting SSO Configuration Files** [page 123]
- **Overriding SSO URLs** [page 124]

#### Setting the SSO Session Lifetime

Enter a **Session lifetime** value for SSO security tokens. This setting controls the length of time for which an issued SSO token is valid. It is not related to browser session inactivity. Enter a numeric value and select hours or minutes in the drop down box to set the timeout.

**To change the session timeout value:**

1. In the **Session lifetime** field, enter a numeric value (which represents the number of hours or minutes for the timeout period).
2. In the drop down box, select hour or minutes to set the timeout.
3. Select **Enable automatic session renewal** if you want to ignore the token lifetime setting completely, thereby preventing a trip to the SSO Security Server login page when the session expires. After this setting is enabled, the next time a session expires, the SSO Gatekeeper renews the expired token instead of the SSO server. In that case, the session only ends by closing the browser.

  **Note:** If you enable this setting in a distributed server environment, you must run SBM Configurator on each server and enable this setting.
Establishing SSL for the SSO Log in

Select the **Use HTTPS for SSO login** check box below to establish secure communication between the user Web browser and the SSO Security Server. This creates a secure log in channel between the browser and the SSO server using the sample SSL certificates that are included with SBM.

**Important:** This setting only secures the SSO login page. This setting does not establish SSL for end-user connections into SBM. For details see Configuring SSL [page 56] and Configuring SSL [page 59].

If you enable this setting in a distributed server environment, you must enable this setting on both the SBM Application Engine server and the Application Repository server.

Updating SSO Keystores

Click the **Change Keystore Passwords** button to change the default password for the following SSO components:

- SSO Security Server (IDP) and gatekeeper keystores
- SSO Security Server (IDP) and gatekeeper truststores

Changing the default password updates the keystores and their corresponding certificate entries with a password of your choice, which improves security.

To update the default password:

1. Click **Change Keystore Passwords**.
2. A window appears and displays the current password. (The default is `changeit`).
3. Enter a new password and click **OK**.
4. Click **Apply**.

Encrypting SSO Configuration Files

Use the SSO encryption options to protect vulnerable passwords in the SSO configuration files that are installed on your server. These passwords are not encrypted by default; therefore, to properly secure your installation, select an encryption algorithm and encrypt your SSO configuration files.

You can apply SSO encryption on all of your SBM servers to encrypt the SSO configuration files that are installed on each server.

SBM Configurator provides the following encryption options:

- **Encrypt All**
  Select this option to encrypt your SSO configuration files using a selected algorithm from the drop-down box. This operation encrypts passwords that normally appear in clear text in various SSO configuration areas (such as the ALFSSOgatekeeper and IDP).

- **Decrypt All**
  Select this option to decrypt files that you have previously encrypted using SBM Configurator. If you need access to the decrypted version of a password, select this option to remove the current encryption.
• **Re-Encrypt**

Select this option to apply a new encryption to the files that you have previously encrypted using SBM Configurator. If you manually decrypt a previously encrypted password, this option will not re-encrypt the password.

After you change any of the encryption settings, you are prompted to restart the SBM Tomcat service for the changes to take effect.

**Overriding SSO URLs**

Click Override to change the default SSO URLs. This enables you to configure access through your company firewall as necessary. For example, if you need to override the internal hostname and port in the gsoap URL for servers that are beyond the firewall, you can change those values here.

You might also override the SSO URLs in the event that you want to use the IIS filter plugin instead of Tomcat to filter requests. You can modify the URLs to override the SSO login page to use IIS (via port 80) instead of Tomcat so that IIS initially handles the authentication request and then passes the information to SSO.

**To override the default SSO URLs:**

1. Click **Override**.

   The override dialog box appears.

2. In the dialog box, change the URL value as desired. Refer to the sample Template URL to view the required syntax for the URL.

3. Click **Test Connection** to validate the URL. If the URL is valid, a **Connection successful** message appears.

4. Click the **Override** button to save your changes.

   The new URL value is displayed in the list of URLs.

5. Click **Override** to change the URL again, or click [Reset to default] to undo your changes and use the default SSO URL.

6. Click **Apply**.

**Configuring Client Certificate Authentication**

In the **Client Certificate Authentication** tab, you can enable bi-directional (or two-way SSL authentication) between the components in SBM. Client certificate authentication provides tighter security for your entire SBM installation because once trust is established, each machine can reliably identify itself and provide assurance of its identity to the server. This prevents sniffing and relaying types of attacks against your SBM system.

Trust is established by assuring the client's identity to the server. To provide this assurance to a server, a client signs messages that it sends with the private key of an asymmetrical encryption key pair. If the server has the corresponding public key installed in its trust store, it is able to decrypt the message to prove that it was sent by a client with the private key. If a server receives a message from a client, but it does not have a key corresponding to the one used by the client, the message is rejected.

Note the following:
The client certificate authentication set up process is two-fold: you must establish trust between your IIS and Tomcat servers, and you must establish trust between all of your SBM Composer client machines and the Application Repository and SSO servers. Begin by performing the steps according to the type of server installation you have, and finish by completing the steps for SBM Composer.

If you are using a software load balancer with SBM that is already configured to use client certificate authentication for all internal communication between the SBM components, select the **Client Certificate Authentication is handled by load balancer** check box in the IIS and Tomcat sections (whichever is applicable) before you perform the following steps.

For IIS, this ensures that the certificate is added to the Windows trust store and the certificate details are stored in the database, and removes the SSL requirement for the gsoap application in IIS. If you do not use a load balancer for IIS or Tomcat, do not select this checkbox in either section.

The sbmproxy ISAPI filter on the Default Web Site in IIS provides the capability to handle SOAP traffic. However, it does not proxy SOAP requests if client certificate security is enabled in SBM—the SOAP proxy cannot be secured by two-way SSL transport security like the SBM components. This means the sbmproxy ISAPI filter will not proxy SOAP traffic if you configure two-way SSL authentication between SBM components.

Single Server Installation

To enable client certificate authentication, you must configure SSL for IIS and Tomcat first according to the steps in Configuring SSL [page 56] and Configuring SSL [page 59]. The SSL port that you specify on the **IIS Server** tab is used on the **Client Certificate Authentication** tab. The server SSL port that you specify for Tomcat must be different than the port that is used for client certificate authentication.

To enable client certificate authentication in a single server installation:

1. Import or select an existing server certificate to establish SSL on the **IIS Server** and **Tomcat Server** tabs.
2. Click the **Security** tab, and then open the **Client Certificate Authentication** sub-tab.
3. Select the **Enable SSL Client Certificate Authentication** check box.
4. In the IIS section, click **Generate Client Certificate** to create a new certificate and key pair for IIS.
5. In the Tomcat section, click **Generate Client Certificate** to create a new certificate and key pair for Tomcat.
6. On the **Component Servers** tab, select **Use HTTPS on port** in the IIS section.
7. Click **Apply** in SBM Configurator.

8. In SBM Application Repository, update the Application Engine server URL for your environment, the target servers URLs, and any internal endpoints to use HTTPS with the client certificate authentication port. After you have updated the environment and any endpoints, redeploy your process apps.


### Distributed Installation

**Important:** To enable client certificate authentication, you must configure SSL for IIS and Tomcat first according to the steps in Configuring SSL [page 56] and Configuring SSL [page 59]. The SSL port that you specify on the **IIS Server** tab is used on the **Client Certificate Authentication** tab. The server SSL port that you specify for Tomcat must be different than the port that is used for client certificate authentication.

**To enable client certificate authentication between components in a distributed installation:**

1. Configure SSL on your IIS and Tomcat servers by importing or selecting an existing server certificate on the **IIS Server** and **Tomcat Server** tabs.

2. On each IIS and Tomcat server:
   a. Click the **Security** tab, and then open the **Client Certificate Authentication** sub-tab.
   b. Select the **Enable SSL Client Certificate Authentication** check box.
   c. Click **Generate Client Certificate**.

3. On the IIS server, open the **Component Servers** tab, and then select **Use HTTPS on port** in the IIS section.

   If you are using the **Configuration Settings** database to store the configuration from all servers in a centralized location, click **Update From Database**, and then **Apply** on your other servers. You have now successfully secured your entire installation.

   If you are not using the **Configuration Settings** database, proceed with the next step.

4. On each Tomcat server, click the **Export** button at the bottom of SBM Configurator. Save the configuration snapshot file on each Tomcat server.

5. Copy the snapshot files from each Tomcat server to the IIS server.

6. On the IIS server, click the **Import** button at the bottom of SBM Configurator and import the snapshot files from each Tomcat server.

7. Once all the snapshots have been imported on the IIS server, click the **Export** button at the bottom of SBM Configurator. Save the configuration snapshot file on the IIS server.

8. Copy the snapshot file from the IIS server to each Tomcat server.
9. On each Tomcat server, click the **Import** button at the bottom of SBM Configurator, and then import the snapshot file from the IIS server.

10. Click **Apply** in each instance of SBM Configurator.

11. In SBM Application Repository, update the Application Engine server URL for your environment, the target servers URLs, and any internal endpoints to use HTTPS with the client certificate authentication port. For example:


   https://servername:8443/jbpm-bpel/services/DeployService

   https://servername:8443/eventmanager/services/ALFAdmin

   After you have updated the environment and any endpoints, redeploy your process apps.

12. Follow the steps in **Client Certificate Authentication with SBM Composer** [page 127] to secure connections from SBM Composer.

If you do not want to export and import configuration snapshots to establish client certificate authentication, you can use the **Export Client Certificate** and **Import Client Certificate** buttons to establish trust between your IIS and Tomcat servers. In the **Export** dialog box, you can export just the public certificate, you can export the public and private certificates (for example, if you want to clone the certificate on multiple Tomcat servers).

**Client Certificate Authentication with SBM Composer**

To finish the client certificate authentication setup between your SBM components, you must configure each instance of SBM Composer by generating or importing a public and private key certificate into the client user's personal key store, and then importing the public key certificate from that key pair in the Application Repository and SSO servers. This creates a client trust between each SBM Composer client and the Tomcat servers in your installation.

The process for establishing client trust is flexible. For example:

- You can generate a certificate that contains a private and public key pair on each SBM Composer machine, export the public key certificate from each SBM Composer machine, and then import all the public key certificates on the Application Repository and SSO servers.

  This ensures each client machine has a unique key pair; if one key pair is lost it does not impact all the other client machines. However, you must ensure that all of the public keys from each key pair are imported on the Application Repository and SSO servers.

- You can generate a certificate that contains a private and public key pair on one SBM Composer machine, export the key pair certificate, import the key pair certificate on your remaining SBM Composer machines, and then import the public key certificate on the Application Repository and SSO servers.
This means that the key pair that is used by all clients is imported only once on your Application Repository and SSO servers; however, if the private key is compromised, all client machines are impacted.

- You can use the same private and public key pair for a set of SBM Composer machines if necessary, and have other clients use unique private and public key pairs.

- You can use a Smart Card certificate for client certificate authentication with SBM Composer. Follow the steps in Using Smart Card Authentication with SBM Composer [page 83] to make the Smart Card certificate available for use on the Client Certificate Administration tab.

  **Important:** If you decide to use the Smart Card certificate for client certificate authentication from SBM Composer, you must export the public certificate from your personal store, and then import it in SBM Configurator on the SSO and Application Repository servers.

Before you begin configuring client certificate authentication for your SBM Composer, consult your IT department and decide which strategy will satisfy your security needs.

The following steps describe the process for creating private and public key pairs on each SBM Composer machine. You must launch SBM Composer using a special command-line prompt in order to launch the Advanced Security Setup for SBM Composer dialog box. This dialog box is intended for administrators; it is not available in the standard SBM Composer interface, nor described in the SBM Composer Guide.

**To enable client certificate authentication in SBM Composer:**

1. Ensure each SBM Composer instance can connect to Application Repository using SSL. This means you have configured SSL for the Application Repository server by generating or importing a server certificate on the Tomcat Servers tab, and connections are made to Application Repository over HTTPS using the Secure connection check box in SBM Composer.

   **Tip:** If your Tomcat server SSL certificate is self-signed or signed by an authority that is not well-known, you must import the server's public certificate into the Trusted Root Certificate store on each SBM Composer machine using the Microsoft Management Console (MMC) or import the certificate by connecting to Application Repository via HTTPS from a Web browser and trusting the public certificate.

2. On an SBM Composer machine, navigate to the directory that contains the SBM Composer executable, and launch SBM Composer using the following command:

   ```
   Serena.Studio.Shell.Application  /ClientSideSSLSetup
   ```

   The Advanced Security Setup for SBM Composer dialog box appears. The dialog box lists all self-signed certificates that currently reside in the user's personal certificate store that contain both a private and public key.

3. Click **New** to create a new self-signed certificate that contains a new unique private and public key pair. Provide the following:

   - Select the Available in Composer check box to allow the SBM Composer user to select the certificate in the Repository Connection Settings dialog box when he or she attempts to connect to the repository.
• Enter a **Composer name** for the certificate that will easily identify the certificate to the SBM Composer user. The **Composer name** is what appears to the user in SBM Composer (not the certificate's issued to, subject name, or friendly name).

**Tip:** If SBM Composer will connect to only one repository, then giving the certificate a meaningful name is not necessary, and any name will suffice. However, if more than one certificate is flagged in the list as **Available in Composer**, consider naming the certificates in a way that distinguishes them (perhaps to identify which server they connect to).

• Enter a **Subject (CN)** for the certificate. This is used to complete the certificate's friendly name.

The new certificate is created and added to the user's personal certificate store.

4. Click **Export**, and then select **Public Key Certificate**. This option saves the public key to a DER-encoded binary X.509 (*.cer) public key file. You will import this file on the Application Repository and SSO servers to establish trust.

You can export the public and private key pair from this machine and use it to secure other SBM Composer clients (instead of generating several unique key pairs on each machine). To export the key pair:

a. Click **Export**, and then select **Public and Private Key Certificate**.

b. Enter a password to secure the private key.

c. Save the file locally, and then copy the .pfx file to your other SBM Composer machines.

d. On each SBM Composer machine, launch SBM Composer using the /ClientSideSSLSetup command, and then click the **Import** button.

e. Select the .pfx file, and then enter password.

5. On the server or servers that host Application Repository and SSO, navigate to the **Client Certificate Authentication** sub-tab, and click the **Manage Trusted Certificates** button in the **Tomcat** section. Click **Import Certificates**, and then select the X.509 (*.cer) file that contains the public certificate from SBM Composer.

**Important:** If you generated a unique key pair for multiple SBM Composer machines, you must repeat this step for each SBM Composer machine with a unique key pair. You must import the public certificate from each SBM Composer machine in order for Tomcat to trust that machine.

6. Click **Apply** in SBM Configurator.

7. In SBM Composer, open the **Composer Options** dialog box, and then click the **Repository** tab. Select the **Use secure connection** check box. The **Client certificate** drop-down becomes available.

8. Select the client certificate that is trusted by Application Repository in the **Client certificate** drop-down list.
9. Enter the client certificate authentication port for Tomcat (the default is 8443). This is the **HTTPS port for client certificate authentication** that is specified for Tomcat in the **Client Certificate Authentication** tab in SBM Configurator.

10. Click **Test connection** to verify that SBM Composer can connect to Application Repository.

Note the following additional options in the **Advanced Security Setup for SBM Composer** dialog box:

- Click the **Show Filter** button to only display certificates that match a certain string. In the **Look for** combo box, search for certificates by entering a string, and then click **Find**. Certificates with one or more properties that match the specified string are displayed. Click the **Options** button to specify whether to search details, match case, or match whole word.

- Click **Edit** if you need to rename the certificate or select the **Available in Composer** check box after the certificate has been created.

- If you import a self-signed certificate that contains multiple key pairs, you can select which key pair certificates should be imported. If one or more of the certificates (identified by thumbprint) already exist in the personal certificate store, a dialog box indicates the number of duplicate certificates that were skipped.

- Click the **Properties** button to view details of the self-signed certificates in the user's personal certificate store. You can also select a certificate in the list, right-click, and then select **Properties**.

- Press the F5 key to refresh the list of certificates if any changes have been made using the MMC console instead.

**Troubleshooting Issues**

If users experience connectivity issues or problems deploying process apps after client certificate authentication is configured, click the **Advanced Settings** button in the IIS section and configure the following:

- **Send trusted authorities list**
  Select this check box to ensure that the list of trusted root certificate authorities is sent to the client during the TLS/SSL handshake. This can fix connectivity issues for users who are trying to log in to the system.

- **Buffer size**
  Increase the client request size (in bytes) that IIS will buffer and pass to the SBM ISAPI extension. If users encounter a **413 Error: Request entity too large** message when trying to deploy process apps, consider increasing the buffer size. For example, setting the buffer size to 100000000 bytes should allow deployment to finish.

**Securing Anonymous Events**

In the **Secure Anonymous Events** tab, you enter an SBM user name and password to use with anonymous events that are sent to the Event Manager.
About Using Anonymous Events

By default, SBM Orchestration Engine rejects anonymous events unless you select Allow Anonymous Events and provide an SBM user and password that the Event Manager will use for anonymous events that it receives.

For integrations that support it, Serena recommends that you configure Single Sign-On (SSO), which typically means that any events from the integrated system will be accompanied by a credential representing the originating user. If SSO is not used then the event source must add an SBM credential to the event or it will be rejected. This ensures that the remote entity that sends the event can identify itself and that SBM will only process events from approved entities.

However, if you must use anonymous events, you can designate an anonymous event user in SBM Configurator, which allows SBM to process anonymous events if credentials are not provided. While this configuration is not recommended because the caller's identity is unknown, it does provide control over anonymous use by enabling you to change or de-authorize the anonymous user account if necessary.

Securing Integrations

In the Secure Integrations tab, you manage security for integrations with other Serena products that use SSO such as Dimensions CM, Dimensions RM, and PVCS VM. SBM has a trusted relationship that is established with these different servers for them to work with SSO. This relationship is established using certificates that are generated by or for these other products. SBM is installed with sample certificates; however, Serena recommends that you replace the default SSO certificate for these integrations to improve security.

SSO Trusted Certificates

To secure your integrations:

1. In the SSO Trusted Certificates section, select the Serena product from the integrations drop-down list. Details for the current trusted certificate (if enabled) appear.

2. Select the Enable trusted certificate for SSO check box.

3. In the Trusted Certificate section, you can view, import, or export the trusted certificate.

Proxy Server

On the Proxy Server tab, you configure advanced proxy server settings for systems that run in tight security networks that need to control outbound traffic or in other situations that call for controlling traffic (inbound or outbound).
You might use a proxy server in your environment if you need to control Tomcat access to outside URLs. For example, when SBM Orchestration Engine makes Web service calls to outside URLs as part of an orchestration workflow, the SBM Orchestration Engine connects to the outside URL via the proxy server that you specify.

In the **Proxy Server** dialog box, provide the following information for HTTP or HTTPS connections:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the proxy server's host name.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number for the proxy server.</td>
</tr>
<tr>
<td>User name</td>
<td>Enter a user account name that has access to connect to your proxy server.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the user's password.</td>
</tr>
<tr>
<td>Skip proxy for</td>
<td>Enter a comma-separated list of server host names that can be accessed directly without going through the proxy server.</td>
</tr>
</tbody>
</table>

**Note:** If you use an HTTPS connection to a proxy server with SBM, you must enable HTTPS tunneling in your proxy server's configuration settings. Refer to your proxy server's documentation for assistance with enabling HTTPS tunneling.

**Utilities**

From the **Utilities** menu, you can stop and start SBM services, view system information, troubleshoot your installation, and view configuration history. The **Utilities** menu is only available during **utility mode**.

**Manage Services**

In the **Manage Services** tab, you control the services that power each SBM server component.

The following table describes where each SBM service is managed in a distributed installation:

<table>
<thead>
<tr>
<th>Service</th>
<th>Component Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>SBM Tomcat</td>
<td>All SBM servers except an Application Engine-only server</td>
</tr>
<tr>
<td>World Wide Web Publishing Service</td>
<td>The server that hosts SBM Application Engine</td>
</tr>
<tr>
<td>Notification Server</td>
<td>Each SBM Mail Services server that hosts the Notification Server</td>
</tr>
<tr>
<td>Mail Client</td>
<td>Each SBM Mail Services server that hosts the Mail Client</td>
</tr>
</tbody>
</table>
### System Settings

The **System Settings** tab provides a summary of your SBM system information, which is useful when you upgrade your system or when you send information to Serena Customer Support. You can also manage how your configuration settings are stored in the **Configuration Settings** tab.

- **General Settings** [page 133]
- **Configuration Settings** [page 133]

### General Settings

The following information is available in the **General** tab:

- **Hardware**
  
  This section displays the amount of RAM that is available to the operating system and the amount of storage room that is available on the server.

- **Software**
  
  This section displays information about the software that is installed on the server, including the current versions of IIS and the .NET Framework.

- **SBM**
  
  This section displays the current version number for each SBM component that is installed. The value format indicates the major version, patch level, and build number.

- **Plugins**
  
  This section displays a list of plugins that are currently installed.

### Configuration Settings

The following options are available on the **Configuration Settings** sub-tab.

**Using the Configuration Settings database**

Select **Use Configuration Settings database** to store the configuration settings from each SBM server in a centralized location.

- If you have a distributed installation, it is highly recommended that you use this option to easily synchronize configuration settings between each SBM server.
Otherwise, you must export and import configuration snapshot files between SBM Configurator instances on each machine.

- If you select the **Use Configuration Settings database** option, and you have a multi-environment installation (in which users complete acceptance testing prior to pushing changes into production), specify which environment this server belongs to (for example, **Production**). Otherwise, leave the environment name as **DEFAULT**.

- Each environment in an "environment set" requires a different name. When you are prompted to use the Configuration Settings database on each server, enter the name of the environment that the server belongs to.

When you use the Configuration Settings database, the **Revision History** button appears. This enables you to view and manage prior configurations that have been applied. Each entry provides a complete summary of your installation because it pulls data from the Configuration Settings database (not just the settings from your local machine).

- Use the **Search** field to find a particular snapshot of the Configuration Settings database. You can search by revision, SBM version, environment name, host name, or comment.

- Filter the list of snapshots using the **Environment** or **SBM version** drop-down lists.

- Click **View** to display an entire snapshot in XML format.

- Select one or more rows (via CTL+click or SHIFT+click) and click **Export** to save a snapshot file. You can send this file to Support for troubleshooting issues.

- Select a snapshot from the list and click the **Revert To** button to rollback to an earlier configuration, if necessary. You are prompted to confirm that you want to rollback to a previous configuration. If you decide to continue, you must click **Apply** after the rollback is finished in order to use the prior configuration.

- Select two rows (via CTL+click or SHIFT+click) and click **Compare** to launch the comparison window, which enables you to compare snapshots side-by-side. Differences between the snapshots are highlighted.

- Click a column header to sort the list of snapshots by values in that column.

- Hover over a column header and click the filter icon to filter the list by one or more values in the column. A summary of applied filters appears at the bottom of the dialog box.

**Using Configuration Snapshots**

Select **Use Configuration Snapshots** to save your configuration in a snapshot file instead of the **Configuration Settings** database.

This means you will use the **Export Configuration** and **Import Configuration** buttons to export your configuration to a local file, which you can import into SBM Configurator on another server to update it with settings from the server where the export was performed. In a distributed installation, if you select **Use Configuration Snapshots**, you must use the import and export operations to update the connection information and security settings on each server.
**Diagnostics**

In the **Diagnostics** tab, you can view a detailed summary of your system configuration, run diagnostic tests to help you troubleshoot installation and configuration issues, and configure settings related to Active Diagnostics. The **Diagnostics** tab can be used by Serena Customer Support to quickly and accurately solve problems in your SBM installation.

- Configuration Report [page 135]
- Static Diagnostics [page 135]
- Active Diagnostics [page 136]

**Configuration Report**

Use the **Configuration Report** option from the **Utilities** menu to create a report that describes the configuration of your SBM system. This report is useful when you need to obtain information about the server hardware, OS, and version of SBM that is installed. A complete topology of your SBM system appears, including datasource information for each component and SSO configuration details.

**To generate the report:**

1. On the **Diagnostics** tab, open the **Configuration Report** sub-tab.
2. Review the information in the report. Use the **Word wrap** option if necessary.
3. Click **Save Report As** to save the report to the specified location.

This saves your SBM configuration in a report file. You can use this report to review the overall layout, settings, and configuration of your SBM system.

**Tip:** The **Collect Log Files** operation includes a copy of your system's current Configuration Report.

You can also automate collection of log files from the command line. For example:

```
C:\Program Files\Serena\SBM\ConfigUtil\ConfigurationUtility.exe
/util /collect-log-files c:\output.zip
```

**Static Diagnostics**

In the **Static Diagnostics** tab, you can run a variety of diagnostic tests to help you troubleshoot problems with your SBM installation and configuration. You can run static diagnostic tests from a list of predefined categories and view the exact area that is not configured properly, not accessible, or not functioning as intended. Serena recommends that you run the static diagnostics tests if you are not able to access certain components or features in SBM.

For example, if your users are not receiving notification messages, you can perform a series of diagnostic tests against the Mail Servers to see if the SMTP server is accessible or determine if the Notification Server can access the database. If a problem is encountered, the tests that do not pass show a **Failed** status. You can click the drop-down arrow for details on any test (whether the result is **Success**, **Warning**, or **Failed**).
To execute a static diagnostic test:

1. From the Utilities menu, click the Diagnostics tab, and then click the Static Diagnostics sub-tab.

2. Click the Category drop-down list, select one or more categories to test, and then click OK. You can optionally type the name of a component or category that you want to test in the Search field.

3. Click the Status drop-down list, and then select one or more status messages to return. For example, to skip success messages, clear the Success option and click OK.

4. After you select one or more categories and choose status options, the available tests appear in the main window. Click Select All to choose all tests or Select None to clear selections. Use one of the following options to execute a test:
   - Run All Tests
     Selects and execute all tests that appear in the main window. Click Run All Tests again after you have addressed a problem to see if the same messages appear again.
   - Run Selected Tests
     Executes only certain tests that you have selected in the main window.
   - Clear Results
     Clears the Run Summary and results of the tests that you performed.
   - Export Results
     Displays the test results in a report format (similar to the Configuration Report) that you can save to your local file system. Use the Word wrap option to make longer report details easier to read. You can send attach this report to a Support case to provide specific details about a problem in SBM. Click Back to return to the test.

Use the arrows to page through large result sets or jump directly to page by entering the page number. You can also configure the number of Items per page (from 20 to 40).

Active Diagnostics

In the Active Diagnostics tab, you configure logging for runtime activities and events that are processed by the SBM Application Engine Web Server, including the end-to-end processing of workflow activities that fire orchestrations. For example, when a user fires a transition that invokes an orchestration, and the orchestration makes a Web service call back to Application Engine, the entire cross-component transaction is logged by Active Diagnostics.

You can configure Active Diagnostics logging at runtime, which means you do not need to stop and start any of the services in the Manage Services tab to change the settings. Once you start the SBM Logging Services service on the server that hosts SBM Logging Services, all activities and events that are processed by the SBM Application Engine Web Server are logged.

Note the following:
• Use the **Manage Services** tab to stop and start SBM Logging Services. This service stops and starts Active Diagnostics logging activities.

• The SBM Logging Services service and the Active Diagnostics database are only installed on the server that hosts SBM Logging Services.

• For multi-environment installations, each environment should have its own dedicated SBM Logging Services instance (and each environment can only run one instance of SBM Logging Services).

• Use the **Collect Log Files** button to gather the logs and send them to Support to troubleshoot problems in areas including, but not limited to:
  ▪ The SBM API
  ▪ The SBM Application Engine Web Services API
  ▪ SBM AppScript
  ▪ Transition actions and mass updates
  ▪ Authentication
  ▪ Database Connections
  ▪ Deploying and promoting snapshots
  ▪ Report execution
  ▪ Read and write locks
  ▪ File attachments
  ▪ Notification Server and Mail Client activities

• **Server Configuration** [page 137]

• **Runtime Configuration** [page 138]

**Server Configuration**

In this section, you configure the connection information for the Active Diagnostics database on your local machine. The Active Diagnostics database is powered by MongoDB. For more information on MongoDB, visit [http://mongodb.org](http://mongodb.org). To change the default connection information for the database, edit the following:

<table>
<thead>
<tr>
<th><strong>Field</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Only appears if SBM Logging Services is installed on a node in a Tomcat cluster. Select the node on which SBM Logging Services is running.</td>
</tr>
<tr>
<td>Port</td>
<td>Only appears if SBM Logging Services is installed on a node in a Tomcat cluster. Enter the port number. The default is 27017.</td>
</tr>
</tbody>
</table>
### User name
Enter the username of the account that connects to the Active Diagnostics database. The default user name is **logger**.

**Note:** This user is not an SBM user; it is a user that connects to MongoDB and interacts with the Active Diagnostics database. The default value can be changed if necessary for security purposes.

### Password
Enter the user's password. The default password is **sbm**.

### Confirm password
Enter the user's password again to confirm.

**Note:** If you change the default user name or password, you must click **Apply** to update the configuration files and Active Diagnostics database.

### Runtime Configuration
Use this section to adjust what type of runtime data is logged and how much data is captured. The following options are available:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Activity</td>
<td>Select this option to capture high-level, global server activity that is not limited to a specific SBM functional area. This option is useful when you want to capture the server's general usage model.</td>
</tr>
<tr>
<td>Collect CPU and Memory Counters</td>
<td>Select this option to collect CPU and memory counters for the processes used by the SBM Application Engine Web Server and SBM Application Engine Web Services API application pools.</td>
</tr>
<tr>
<td>Filter by User ID</td>
<td>Enter an SBM user's login ID to filter log messages for a specific SBM user. Requests that are not associated with a specific user are still logged.</td>
</tr>
</tbody>
</table>

The sliders represent distinct logging contexts that you can adjust as necessary. Logging contexts are loose functional groupings that capture various SBM activities. For each context that is listed, you apply a logging level to control how much detail is recorded. Note that the contexts and their corresponding logging levels are global—they apply to the entire SBM instance.

Use the slider to apply a logging level to each of the following functional logging contexts:
<table>
<thead>
<tr>
<th><strong>Logging Context</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>Captures all administrative requests performed in SBM Application Administrator and remote administration operations performed by the SBM Application Engine Web Server.</td>
</tr>
<tr>
<td>System</td>
<td>Captures system-level information such as system hangs, read and write locks, IIS stop and start activities, thread usage, and caching information. Also captures activities related to the SBM API.</td>
</tr>
<tr>
<td>Authentication / Licensing</td>
<td>Captures authentication LDAP, NT Challenge Response, Internal Passwords, and SSO authentication calls. Also captures license requests and when licenses are released.</td>
</tr>
<tr>
<td>Reports and Searches</td>
<td>Captures information related to report execution and searches.</td>
</tr>
<tr>
<td>Deploy and Promotion</td>
<td>Captures deploy, promote, create snapshot, and get process app activities that are performed by SBM Application Engine.</td>
</tr>
<tr>
<td>Workflow</td>
<td>Captures end-to-end workflow activities such as transition actions that call SBM Application Engine Web services or orchestrations and their execution. Also includes submitting, updating, and viewing items; adding notes or attachments to items, and SBM AppScript operations.</td>
</tr>
<tr>
<td>Notification Server</td>
<td>Captures the end-to-end process for calls to the Application Engine and the Orchestration Engine that are made by the Notification Server.</td>
</tr>
<tr>
<td>Mail Client</td>
<td>Captures complete transactions involving the Application Engine and the Mail Client.</td>
</tr>
<tr>
<td>User Interface</td>
<td>Captures messages from SBM User Workspace and Serena Work Center browser sessions and logs activities related to page render requests. <strong>Tip:</strong> Use the <strong>Filter by User ID</strong> option to prevent the log from capturing data from all users.</td>
</tr>
<tr>
<td>Common Services</td>
<td>Captures messages related to SBM Common Services. Useful for diagnosing issues with backlogs and Serena Work Center related requests.</td>
</tr>
<tr>
<td>Solution Framework</td>
<td>Captures framework messages related to Serena Service Manager and Serena Release Control. This context only appears if you install one of these solutions.</td>
</tr>
</tbody>
</table>
The following logging levels (in descending order of logging detail) are available for each context:

- **Fatal** – Captures only system crashes and fatal events that occur.
- **Error** – Captures errors and single thread execution failures.
- **Warn** – Captures warning messages for problematic events that might occur.
- **Info** – Provides high-level information about thread execution and server requests.
- **Debug** – Captures a deeper level of information and covers more functionality.
- **Trace** – Captures the most detail through verbose logging. Includes SQL statements and fine detail.

**Important:** System performance may be negatively impacted when you enable either the **Debug** or **Trace** logging levels.

After you have set the desired logging level for each context, you must click the **Apply Runtime Configuration** button for the changes to take effect.

Once the maximum log file size is reached, the log file rolls and older entries are removed in favor of newer entries. You can save existing log files by clicking the **Collect Log Files** button, and then saving the archive locally. If you want to view the Active Diagnostics logs prior to sending them to Serena, you can use a third-party tool such as MongoVUE or MongoExplorer. For information about exporting the MongoDB into a text file, visit http://www.mongodb.org/.

To purge all of the data that has been collected to date, click the **Empty Logs** button. This operation clears the content from the log files, but does not reduce the file size that has been allocated. This action cannot be reversed, so make sure you have saved your logs or sent them to Serena before you empty them.

To reduce the allocated file size, use the **Restrict Log Size** field. The default size is 3 GB. To successfully reduce the allocated file size, enter a lower value, click **Apply** to save the change, and then click **Apply** again to shrink the database. This sequence of operations allows SBM Configurator to perform a repair database operation that ultimately reduces the file size.

**Utility Log**

The **Utility Log** enables you to view a single log file that contains a history of all the configuration changes that you have made to your SBM system.

**To view the log file:**

1. Launch SBM Configurator.
2. From the **Utilities** menu, select the **Utility Log** tab.
3. Click **Save As** to save the `ConfigurationUtility.log` file to your local machine. Click **Clear** to delete the contents of the log file.

The log file is also located in the `ConfigUtility` directory inside the SBM installation directory.
Creating Users and Establishing Privileges

You must create user accounts and establish privileges before users can work with process apps. Perform the following steps to get started:

1. Log in to the SBM Application Administrator using the primary system administrator account, and create new regular users and users with Managed Administrator product access. For details about types of administrators you can create, see the "Types of Administrators" topic in the SBM Application Administrator Guide.

2. Grant end user accounts privileges to work with process apps.

3. Grant managed administrators privileges to export and deploy process apps and access the Application Repository and manage process apps. You must grant managed administrators deployment privileges on the Deployment tab in order to enable access to the Application Repository.

4. Log in to Application Repository and grant managed administrators privileges to the repository.

You must also set the privileges for a user to deploy a particular process app from SBM Composer. These permissions are set in Application Repository. They are set after you have connected to an environment and exported the process apps to the repository. Once the process app is in the repository, select the process app and make it available from SBM Composer by enabling the appropriate privileges.

To learn more about privilege examples for publishing and deploying, and privilege examples for environment tasks, refer to the SBM Application Repository Guide.

Privilege Examples for Publishing and Deploying

**Audience:** On-premise.

This topic provides examples of the privileges required for designers who create and publish process apps, and for a managed administrator who deploys those process apps.

**Note:** The examples below indicate the minimum set of privileges users need to perform the described tasks. Users will generally need additional privileges to use the system effectively.
Creating and Checking in a Process App

Pauline, a process app designer, has the requirements that she needs to create a new Issue Tracking process app in SBM Composer. She completes a prototype and checks a public version in to the repository. She will not deploy the process app to a runtime environment, but will ask Robin, a managed administrator, to do so at a later time.

Table 1. Pauline’s Privilege Requirements

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
</table>
| Repository    | None, however, when Pauline publishes the process app for the first time, she is automatically granted the following privileges:  
  • Create Process App  
  • Create Application/Orchestration  
  • View, Edit, Publish, and Deploy for the process app just created  
  • View and Edit for the applications and orchestrations included in the process app | SBM Application Repository |
| Deployment    | None, since Pauline will only check in the process app from SBM Composer, but will not deploy it to a runtime environment. | N/A |
| Administrative| None, since Pauline will not log in to SBM Application Repository or configure the deployed application. | N/A |

Updating a Previously Published Process App

Alex, a co-designer with Pauline, needs to modify the Issue Tracking process app prototype. Once he does so, he needs to publish the process app so that Pauline can check out the updated process app.

From SBM Composer, he tries to open the process app from the repository so he can make his modifications. Alex gets an error message saying that he does not have the privileges required to view process apps in the repository.

Robin, a managed administrator, logs in to SBM Application Repository and grants Alex the privileges he needs to view and open the process app. Alex opens the process app in SBM Composer, makes his changes, and then publishes the process app. He then informs Pauline that an updated version is in the repository.

Table 2. Alex’s Privilege Requirements
<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
</table>
| Repository     | • View, Edit, and Publish for the Issue Tracking process app  
• View and Edit for the applications and orchestrations included in the process app | SBM Application Repository |
| Deployment     | None, since Alex will only check in the process app from SBM Composer. | N/A |
| Administrative  | None, since Alex will not log in to SBM Application Repository or configure the deployed application. | N/A |

**Deploying a Process App From SBM Application Repository**

Robin, a managed administrator, receives a request from Alex and Pauline to deploy the Issue Tracking process app to the test environment. Robin logs into SBM Application Repository, and then deploys the process app to the SBM Application Engine server used as the test environment.

**Table 3. Robin's Privilege Requirements**

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>View and Deploy for the Issue Tracking process app</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td>Deployment</td>
<td>• Deploy Process Apps to This Host (Administration — Deployment page)</td>
<td>SBM Application Administrator</td>
</tr>
</tbody>
</table>
| Administrative (with Managed Administration product access)  | • Remote Administration privilege (User — System page)  
• Add Tables (Administration — System page)  
• Edit Tables (Administration — System page)  
• Application Table privileges (Administration — Tables page) | SBM Application Administrator |
Deploying a Process App From SBM Composer

Robin decides that for testing, Pauline and Alex can deploy process apps directly from SBM Composer to the test environment. Pauline and Alex are glad that they can now deploy the latest revision of the Issue Tracking process app without waiting for someone else. Pauline updates the process app, and then from SBM Composer, she deploys it.

**Note:** Pauline and Alex must be assigned Managed Administration product access before they can deploy to a runtime environment.

**Table 4. Deployment Privileges Required for Pauline and Alex**

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>View, Edit, and Deploy for the process app</td>
<td>SBM Application Repository</td>
</tr>
</tbody>
</table>
| Deployment    | • Deploy Process Apps to This Host  
                 • Deploy to This Host from SBM Composer | SBM Application Administrator |
| Administrative (with Managed Administration product access) | • Remote Administration privilege (User — System page)  
                                                             • Add Tables (Administration — System page)  
                                                             • Edit Tables (Administration — System page)  
                                                             • Application Table privileges (Administration — Tables page) | SBM Application Administrator |

**Privilege Examples for Environment Tasks**

**Audience:** On-premise.

This topic provides examples of environment tasks and the privileges required to complete them for a managed administrator like Robin (who is a user with Managed Administration product access and the Remote Administration user privilege) and a primary administrator like Ken (a user with the same product access and privileges as Robin, but who also has full administrative access to the production environment). These product access types and privileges are granted in SBM Application Administrator.

A global administrator, who is someone who has Regular User product access and the Remote Administration privilege granted in SBM Application Administrator, can perform
most of the tasks below without additional privileges in either SBM Application Repository and SBM Application Administrator. For details on types of SBM administrators, refer to the *SBM Application Administrator Guide*.

**Note:** The examples below indicate the minimum set of privileges users need to perform the described tasks. Users will generally need additional privileges to use the system effectively.

### Creating an Environment

Robin decides the team needs a staging environment so that users can test and accept changes to process apps. She follows the steps outlined in to install the SBM Application Engine component on a separate server machine and configure a database for the staging environment.

This requires Robin to log in to SBM Application Repository and create a new environment called "Staging" that uses the newly installed SBM Application Engine component.

**Table 1. Robin's Required Privileges**

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>Create, Edit, and Delete Environments for This Host</td>
<td>SBM Application Administrator for the destination environment</td>
</tr>
</tbody>
</table>

### Promoting a Process App Snapshot

Development testing is complete on the Issue Tracking process app, and Robin promotes the process app snapshot from the test environment to the staging environment. Robin first creates a process app snapshot in the testing environment. She then promotes it to the staging environment.

**Note:** Promotion is the process by which administrators replicate a process app from one environment to another. After testing, for example, the process app might be ready to be used for real work.

**Table 2. Robin's Required Privileges**

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Deploy (for the process app being promoted)</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td>Deployment (source environment)</td>
<td>Export Process Apps From This Host</td>
<td>SBM Application Administrator</td>
</tr>
</tbody>
</table>
| Deployment (destination environment) | • Deploy Process Apps to This Host  
|                               | • Export Process Apps from This Host                            | SBM Application Administrator                   |
Promoting a Process App Snapshot into Production

User acceptance testing is complete in the staging environment and the Issue Tracking process app is ready for use in production. Ken, a primary administrator with full access to the production environment, first creates a process app snapshot in the staging environment. He then promotes it to the production environment.

Table 3. Ken’s Privilege Requirements

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Deploy (for the process app being promoted)</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td>Deployment (staging environment)</td>
<td>Export Process Apps From This Host</td>
<td>SBM Application Administrator</td>
</tr>
<tr>
<td>Deployment (production environment)</td>
<td>• Deploy Process Apps to This Host</td>
<td>SBM Application Administrator</td>
</tr>
<tr>
<td></td>
<td>• Export Process Apps from This Host</td>
<td>SBM Application Administrator</td>
</tr>
</tbody>
</table>

Deleting a Process App From the Repository

Robin notices that many test process apps are stored in the repository. She would like to delete those that are no longer used. Robin understands that by deleting the process apps, they will no longer be available in the repository and can no longer be deployed to a runtime environment. She also knows that deleting the process apps from the repository will not remove them from any runtime environments until she undeploys them.

Robin logs into the SBM Application Repository and deletes the process app from the Process Apps tab.

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>• Delete Process Apps</td>
<td>SBM Application Repository</td>
</tr>
<tr>
<td></td>
<td>• Delete Application/Orchestration</td>
<td></td>
</tr>
</tbody>
</table>

Undeploying a Process App

After Robin deletes the test process apps from the repository, she decides to clean up the runtime test environment and remove some of the deployed process apps that were used for testing. To remove these process apps from the runtime environment, she needs to undeploy them. She realizes that she will be permanently removing data, such as primary items and projects, but decides that it’s appropriate to remove this unused data from the test environment.

Robin logs in to the SBM Application Repository and undeploys the process app from the Deployed Process Apps tab for the test environment.
Table 4. Robin's Required Privileges

<table>
<thead>
<tr>
<th>Privilege Type</th>
<th>Privileges</th>
<th>Granted in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deployment</td>
<td>Delete Process Apps for This Host</td>
<td>SBM Application Administrator</td>
</tr>
</tbody>
</table>

Allowing Users to Connect to SBM

After you have created users and established privileges, direct users to access SBM using one of the following interfaces:

- **Serena Work Center**
  A simplified end-user interface. Users can access the Work Center by opening the following URL:
  
  http://servername/workcenter

- **SBM User Workspace**
  The legacy end-user interface. Users can access the User Workspace by opening the following URL:
  
  http://servername/tmtrack/tmtrack.dll?

  To access the User Workspace from SBM Composer, click the User Workspace button on the Deployment tab of the ribbon. SBM Composer must first be connected to a runtime environment.

- **Serena Request Center**
  A Serena Service Manager portal that enables users to submit requests and access knowledge management items. Users can access the Request Center by opening the following URL:
  
  http://servername/tmtrack/tmtrack.dll?shell=srp

Working with Application Repository

As part of the post-installation process, you will "get" the Global Process App from the newly created SBM Application Engine database. This enables designers to include core database elements, such as system auxiliary tables, in their process apps.

If you are setting up multiple environments, you will also need to create new environments in Application Repository for test and staging as well.

The following topics describe these steps in more detail:

- Getting the Global Process App [page 148]
- Creating an Environment [page 148]
Getting the Global Process App

The Global Application contains the system auxiliary tables that may be referenced in multiple process apps. Before a designer can reference this table when creating a process app, the Global Process App must be retrieved from SBM Application Engine database using the Get command in SBM Application Repository.

To make the Global Application available for new process apps:

1. Launch SBM Application Repository using the following URL:
   
   http://servername:port/mashupmgr

2. Log in using the primary system administrator account that you defined in the Create New Database wizard.

3. Open the Environments tab. The Default Environment appears.


5. In the Actions column, click the Get icon. In the dialog box that appears, click the Get button. The process starts. Click OK to close the dialog box.

6. In SBM Composer, connect to the repository, and then Open the Global Process App from the repository. Perform a check-in of the Global Process App.

7. Create your new process app in SBM Composer.

8. Create a new reference to the Global Application in your new process app.

9. Check in your modified process app. The Global Application is now available to the process app, and other applications can reference the data in the tables.

Creating an Environment

In SBM Application Repository, use the Create New button to define a new environment. After the environment is created, edit the environment's Details, Target Servers (such as the BPEL engine or Event Manager server), and any Web service Endpoints that are required to support your process apps.

Prerequisites:

To create a new environment, you must have the Create, Edit, and Delete Environments privilege, which is set in SBM Application Administrator. The primary system administrator account should have all of these privileges.

To create a new environment:

1. On the Environments tab, click the Create New button.

2. Select the environment and edit the environment's Details, Target Servers, and Endpoints using the sub-tabs below the list of the environments.

The new environment is created and ready for use.
Chapter 7: Client Installation

The client installation is performed separately from the suite install. A separate client installer exists that installs only SBM Composer.

The following topics describe using the standalone client installer:

- The Client Installer [page 149]
- Installing SBM Composer [page 149]
- Silent Installation [page 149]

The Client Installer

You run the client installer on each client machine for designers who will use SBM Composer. SBM Composer is a Windows client application that designers use to create, edit, and deploy process apps.

You can install SBM Composer on one or more servers using the suite installer for testing or evaluation purposes; however, you must use the client installer to install SBM Composer on client machines for use in a production environment.

Installing SBM Composer

To install SBM Composer on a client machine, perform the following steps:

1. Launch the client executable. The installer is available on the installation DVD and as a download. To launch it from the HTML front-end on the DVD, click the Install SBM Composer link.

2. Click Next on the Welcome dialog box.

3. Accept the license agreement and click Next.

4. Choose the location path to install the client and click Next.

5. Choose whether to create a desktop shortcut and click Install on the summary dialog box to install SBM Composer.

When the installer finishes, SBM Composer is installed and links are added to your Windows Start menu.

Silent Installation

You can also install SBM Composer silently by entering required parameters using the command-line. The installer will run without prompting you during the actual installation. For more information on the available Windows installer command-line options and parameters, visit the MSDN site at http://msdn.microsoft.com/en-us/library/aa367988.aspx.
To silently install SBM Composer for the first time on a client machine, or to perform an upgrade on a client machine silently, navigate to the directory that contains the client executable and launch the silent installer. In a Command window, type the client installer executable name, and then append the following:

`s /v"/qn INSTALLDIR="installationDirectory\Serena\SBM""`

**Note:** The `INSTALLDIR` path denotes the desired client installation location.
Chapter 8: Troubleshooting

This chapter focuses on troubleshooting server installations. Refer to the topic below for help when you run into problems with your installation.

- Configuring Internet Information Services (IIS) [page 151]
- Changing the Primary SBM Application Engine Web Server [page 156]
- Additional Troubleshooting Tips [page 156]

Configuring Internet Information Services (IIS)

SBM Configurator automatically configures the SBM applications in Internet Information Services (IIS). You may need to modify IIS settings for your system depending on your authentication settings and usage model.

The instructions in this guide are recommendations for specific settings needed for IIS to work with SBM. For details on configuring IIS, refer to Microsoft documentation.

Settings for IIS 7 and IIS 8

Minimum steps for configuring IIS 7 and 8 include:

- Enabling the Web Server (IIS) Role and Role Services [page 151]
- Modifying Application Pool Options [page 152]
- Granting Permissions to the Database and File Structure [page 154]
- Enabling the ISAPI Filter [page 155]

Enabling the Web Server (IIS) Role and Role Services

SBM requires that you enable the Web Server (IIS) role and a specific set of role services for IIS 7 and IIS 8. If you have not added the Web Server (IIS) role, add it using the Windows Server Manager.

Tip: On Windows 2008, the Add Roles Wizard prompts you to install the Windows Process Activation Service. Click Add Required Features to install the service. Click Next to continue.

Once the Web Server (IIS) role is enabled, enable the following role services:

- Common HTTP Features – Select all, except WebDAV. WebDAV blocks important operations that are used by Serena Release Control.
- Application Development – ASP.NET, .NET Extensibility, CGI, ISAPI Extensions, ISAPI Filters.
- Health and Diagnostics – HTTP Logging.
• Performance – None.

• Management Tools – None.

Modifying Application Pool Options

**Important:** The following configuration steps are performed by SBM Configurator automatically. They are included here in case there is an issue during installation or if the settings are improperly changed at a later time.

Depending on your network configuration and security policies, you can modify the following application pool settings at the default level, or create a new application pool specifically for SBM Application Engine. For instructions on adding application pools, refer to your IIS documentation.

The following steps describe how to configure the recommended application pool settings:

1. Open Internet Information Services (IIS) Manager.

2. In the Connections pane, select the Application Pools node that appears. In the list of application pools, select DefaultAppPool. Click Add Application Pool in the Actions pane if you want to create a new application pool.

   **Note:** SBM Configurator automatically modifies the DefaultAppPool for the tmtrack and sbmconnector applications in IIS. If you want to create a new application pool, note that SBM Configurator will not automatically adjust the settings that are described in this section. You must manually configure the new application pool with the settings described below.

3. In the Actions pane, select the Recycling option. Clear every check box that appears in the Recycling Conditions dialog box. Click Next and then click Finish.

4. In the Actions pane, select the Advanced Settings option. In the Process Model section, perform the following steps:
   
a. Set the Identity to NetworkService.
   
b. Set the Idle Time-out (minutes) value to 0.
   
c. Set the Maximum Worker Processes to 1.
   
d. In the Recycling section, set the Regular Time Interval (minutes) value to 0.
   
e. On 64-bit servers, ensure that the Enable 32-bit Applications setting is set to False.

5. Click OK to save your changes.

6. If you receive the following error message when trying to connect to the database, change the application pool Identity to LocalSystem.

   **We are sorry but last operation caused an error**

   To change the application pool Identity, perform the following steps:
   
a. Edit the SBM Application Engine application pool and select Advanced Settings.
b. In the **Process Model** section, change the **Identity** from the default `NetworkService` to `LocalSystem`.

**Note:** If connection succeeds when using `LocalSystem`, but not with `NetworkService`, you may need to review the file system privileges granted to the `NETWORK SERVICE` account. See [Granting Permissions to the Database and File Structure](#) for more information.
Granting Permissions to the Database and File Structure

**Important:** The following configuration steps are performed by SBM Configurator automatically. They are included here for troubleshooting purposes in the event that settings are improperly changed at a later time.

Before you begin, note the following:

- SBM Configurator automatically grants the DefaultAppPool Identity account *(NetworkService)* permissions to the SBM file structure and database directory. If you change the application pool identity, or create a new application pool for the tmtrack application, you must grant the identity account permissions to the database and file system as described in this section.

- You must ensure that the identity account that you use has **Read** and **Execute** privileges for the WINDOWS directory or WINNT directory (depending on your version of Microsoft Windows). If you use NT Challenge Response, permissions must be applied to those folders for the **Domain Users Group** instead. This group must include all domain users who will be SBM users.

- The following directory is used to store temporary resource data on the SBM Application Engine server:

  \installDir\Serena\SBM\Application Engine\bin\resourcetmp

You must assign the **Modify** permission to the `resourcetmp` directory as follows, depending on the authentication type you have selected:

- **Anonymous Authentication**

  If you are using internal SBM passwords and IIS Directory Security is set to anonymous, the IUSR account normally writes these files to `resourcetmp`. Ensure that the IUSR account owns the `resourcetmp` folder listed above and has the **Modify** permission assigned.

- **Windows Authentication (NTCR)**

  If you are using Windows Authentication, the first user that logs in to SBM after a restart must have **Modify** privilege to the `resourcetmp` directory. This ensures that the appropriate files are pulled from the database and created on the file system. If you are not certain that the first user who will access SBM will have the **Modify** privilege, consider granting the entire **Domain Users Group** permission to just this folder.

The following steps describe the required permissions for **Anonymous Authentication**:

1. On the SBM Application Engine machine, navigate to the `installationDirectory\Serena\SBM\Application Engine` directory.

2. Right-click on the SBM Application Engine directory, and then select **Properties**.

3. Select the **Security** tab. The top pane contains list of users and groups who currently have access to these folders.

4. If you do not see the **NETWORK SERVICE** in the list of users, click **Edit**, and then click **Add**.
5. Enter **NETWORK SERVICE** and click **Check Names**.

6. Click **OK** after the NETWORK SERVICE account appears.

7. Select the NETWORK SERVICE account, and then select the **Full Control** check box in the **Allow** column of the **Permissions** box.

8. Perform the same steps to add the IIS_IUSRS users group to the SBM Application Engine directory. Grant this group **Full Control** (just like the NETWORK SERVICE account).

   **Note:** Do not apply to all child folders; instead, let these folders inherit the security settings. Verify the permission is inherited by selecting SBM Application Engine directory and checking the Security settings.

9. Click **OK**.

10. Repeat these same steps for the NETWORK SERVICE account on the WINDOWS and WINDOWS\system32 directories, but grant only **Read** and **Execute** permissions.

11. On the IIS server, navigate to your database client directory and files, and grant read permissions to NETWORK SERVICE (or the identity that you are using if you have changed it).

### Enabling the ISAPI Filter

**Important:** The following steps are automatically performed by SBM Configurator. They are included here in case there is an issue during installation or if the extensions are mistakenly changed. If these already exist in IIS, you do not need to create them.

**To enable the ISAPI filter:**

1. Open Internet Information Services (IIS) Manager.

2. Click the server node in the **Connections** pane. In the server **Home** page that appears, open **ISAPI and CGI Restrictions**.

3. In the **Actions** pane, click **Add**.

4. In the **Add ISAPI or CGI Restriction** dialog box, browse to the tmtrack.dll file located here: `installationDirectory\Serena\SBM\Application Engine\bin`. In the **Description** field, type `tmtrack`.

5. Select the **Allow extension path to execute** check box.

6. Click **OK**.

7. Perform the same steps for the gsoap_ssl.dll and isapi_redirect.dll files (provide unique descriptions for each). The gsoap_ssl.dll is located here: `installationDirectory\Serena\SBM\Application Engine\webservices\bin`. The isapi_redirect.dll file is located here: `installationDirectory\Serena\SBM\Application Engine\bin`. 
Changing the Primary SBM Application Engine Web Server

Every Application Repository installation requires a primary SBM Application Engine Web Server that authenticates and authorizes users. This primary SBM Application Engine Web Server is specified in SBM Configurator.

To change the primary SBM Application Engine Web Server after installation, launch SBM Configurator, and then edit the SBM Application Engine server connection information in the Component Servers dialog box.

⚠️ **Important:** If you apply changes while the SBM Configurator runs in utility mode, browser users may not be able to access the system immediately while the services are restarting. Therefore, consider applying configuration changes at a time when users are not actively using the system.

Additional Troubleshooting Tips

This sections provides additional troubleshooting tips not covered elsewhere.

Installation Issues

To troubleshoot issues related to an SBM install, view the sbminstall.log located here:

```
installationDirectory\Serena\SBM
```

Note that the Collect Log Files operation in SBM Configurator gathers the sbminstall.log as well.

Application Repository and Tomcat Issues

If you have problems connecting to Application Repository or starting the SBM Tomcat service, check the server.log for error messages. You can also use the server.log to troubleshoot problems related to the jMaki Proxy server (which allows external data from disparate domains to be loaded and manipulated in the SBM User Workspace). The server.log is located here:

```
installationDirectory\Serena\SBM\Common\Tomcat 7.0\server\default\logs
```

Access Denied Errors

If you encounter an Access Denied error in SBM Configurator, the user account that is running SBM Configurator might not have sufficient privileges to private keys in the Windows machine MY store, located here:

**Windows 2008 or later**

```
C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```

💡 **Tip:** By default these folders are hidden even if your account has permissions. To view the directories, change the Folder and Search Options to Show Hidden files, folders and drives.
If the current user that is logged in to the server does not have access to this directory, log in with an account that does have access, and then grant the permissions. In addition, the account that is logged in must have access to the following registry key where the public certificates are stored:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\MY

**Database Column Limitations**

SQL Server databases support up to 1024 columns per table. Oracle databases support up to 1000 columns per table. For each field that you create in SBM, a new column is added to the associated table in the database. When you delete a field from SBM, it is not permanently deleted from your database; it is only marked as deleted and will still exist as a column in the table. Although it is unlikely, your database tables may exceed the column upper limit over time. Therefore, check your deleted fields before adding new fields—you may find that you can use a field that is already in your database, thereby eliminating the need to create additional fields.
Appendix 9: Additional Information

The appendix contains the following topics.

- Core Database Elements [page 159]
- Customizing E-mail Templates [page 161]
- Adding Custom Spell Check Dictionaries [page 173]
- Using Web Queries with SBM Session Cookies [page 174]
- Performing a Silent Installation [page 174]

Core Database Elements

When you run the Create New Database wizard in SBM System Administrator, core elements that are needed for your SBM system are added to the databases. These elements include the Base Project, Base Workflow, root folders, and system tables.

Base Project

The Base Project serves as a root for your system's project hierarchy. The Base Project cannot be deleted, but it can be renamed to suit your company's needs. You can also set numbering properties for the Base Project. These numbering properties can be inherited by new projects created in the hierarchy.

Base Workflow

The Base Workflow serves as a root for your system's workflow hierarchy. The Base Workflow cannot be edited, deleted, or used by any project.

Root Folders

Two types of root folders are provided for you to add to as needed:

- Public Folders – Public folders contain links to items that can be accessed by all SBM users. Users with appropriate privileges can view items in, add items to, and remove items from public folders.

- Knowledge Base – Knowledge Base folders contain links to items in the SBM Knowledge Base. Problems and resolutions can be published to Knowledge Base folders for internal and external viewing.

Global Application

The Global Application is a container for system auxiliary tables and other assets that are generally 'global' across multiple process apps. The Event, Scripts, Triggers, Web Services, and Workflow nodes are not available in the Global Application because these design element types are generally not used 'globally' across process apps.
When designers add or edit items in the Global Application, these changes will be reflected in all process apps that reference the Global Application.

The following system auxiliary tables are contained in the Global Application and are provided for storing auxiliary information related to your workflows:

- **Companies table** – This table can be used to store information about the companies with which you interact. The **Database Wizard** provides two system required fields for this table (*Company Name* and *Company Number*), but you can also add custom fields, such as *Address*, *City*, *State*, *Phone Number*, and more. The fields can be modified at a later time, and all but the system required fields can be deleted.

- **Contacts table** – This table can be used to store information about individuals with which your company interacts. The **Database Wizard** provides five system required fields for this table (*First Name*, *Middle Name*, *Last Name*, *User Name*, *E-mail*, and *Company*), but you can also add custom fields that describe your contacts (such as *Department* or *Job Title*). The fields can be modified at a later time, and all but the system required fields can be deleted.

- **Problems table** – This table stores problem records that can be associated with a primary item, published to the Knowledge Base for either public or internal viewing, or both. The **Database Wizard** provides several fields for this table that can be modified at a later time. Additionally, all but two system required fields (*Title* and *Visibility*) can be deleted at a later time.

- **Resolutions table** – This table stores resolution records that can be associated with a problem contained in the *Problems* table and published to the Knowledge Base for either public or internal viewing, associated with a primary item, or both. The **Database Wizard** provides several fields for this table that can be modified at a later time. Additionally, all but three system required fields (*Title*, *Problem*, and *Visibility*) can be deleted at a later time.

The following system auxiliary tables are provided for translating SBM into one or more languages or for modifying provided labels in the end-user interface:

- **Languages table** – This table stores language records that enable you to associate strings with a specific language, which is associated with a locale. This table is used in conjunction with the *Strings* and *String IDs* tables to enable users to view labels and error messages in the language associated with the locale specified in their user profile, if such strings exist.

- **Strings table** – This table stores string records that can be used to modify or translate elements, such as labels, button names, and error messages, into one or more languages.

- **String IDs table** – String identifiers contain the root string information and should not be modified.
CAUTION:

For best results, limit privileges to the Languages, Strings, and String IDs tables to users who will translate your SBM system into another language or are responsible for modifying existing strings. For example, you might grant privileges to these tables to a translator from a globalization vendor or to an SBM managed administrator who is authorized to modify string names. Before granting privileges to the Languages, Strings, and String IDs tables, refer to the SBM System Administrator Guide.

The following system auxiliary tables are provided for the SBM Connect for SharePoint® integration. These tables track the SharePoint servers and their relationship to SBM projects.

- **SharePoint Servers** – This table is used to store information on available SharePoint servers.

- **SharePoint Project Servers** – This table stores information on the relationships between specific SBM projects and their related SharePoint sites.

Refer to the Integration Guide for SharePoint for more information.

**Customizing E-mail Templates**

You can customize the e-mail template that is used for e-mail messages that users send from primary and auxiliary items. This template is not used for customizing e-mail messages that send links to reports.

The provided e-mail template is stored in the appropriate language folder of the emailtemplate\useremailtemplates folder in your SBM Application Engine installation directory. You can customize the provided template to meet your needs or create a new text or HTML template; however, templates must be stored in this directory.

You can also manage these templates from the global Templates view in SBM Application Administrator.

**To customize or create an e-mail template:**

1. On the SBM Application Engine server, open SBM Configurator.

2. Select the Mail Services tab, and then click the Notification Server sub-tab.

3. The Browser E-mail Template drop-down list contains the text and HTML files stored in the appropriate language folder of the emailtemplate\useremailtemplates folder in the SBM Application Engine installation directory. Select the file you want to use to send e-mail messages, and then click Edit.

4. Modify the provided template using text, template tags listed in E-mail Template Tags [page 162], Base template tags listed in Base Global Template Tags [page 165], or Base Item Template Tags [page 168]. If you are using an HTML template, you can also use HTML tags and hyperlinks.

   **Note:** All template tags must begin with $ and end with (). All text in the template is placed in the e-mail message, except for tags themselves. Additionally, all line breaks and spaces are left in the message during template processing.
5. After modifying the template, click **Save** to save your changes.

6. Select the template from the drop-down list and click **Apply** to begin using the modified template. This saves the template change to the file system and database.

7. To create a new template, type a new template name in the **Browser E-mail Template** drop-down list or navigate to the appropriate language folder of the `emailtemplate/useremailtemplate` folder of your SBM Application Engine installation directory and create a new template file. If you manually create or edit the file directly in the file system, send the file to the database by selecting **Put Files in Database** from the **File** menu in SBM System Administrator.

   **CAUTION:**
   Use caution with the **Put Files in Database** command. When you use this command, ALL files from your local machine replace files in the database. You must stop and start your Web server before changes will take effect.

8. Select the new template from the drop-down list and click **Apply** to begin using the new template. This saves the template change to the file system and database.

   **Tip:** If you create the template in the file system, but you want to later edit the new template from within SBM Configurator, close and reopen the utility to have the new file appear in the **Browser E-mail Template** drop-down list.

### E-mail Template Tags

The e-mail template tags below can only be used in browser e-mail templates; in addition, Base template tags can be used in all e-mail templates. Base template tags are discussed in [Base Global Template Tags][page 165] and [Base Item Template Tags][page 168].

#### $FILEATTACHMENTLINKS(external)

- **Description**
  This tag adds links to files attached to items associated with the e-mail message.

- **Usage**
  For HTML e-mail templates, users can click the links to open the attachments. For e-mail templates formatted as text, the URL to the attachment on the Web server is provided. Users can copy and paste this tag into a browser address bar to open the attachment. Links to file attachments only appear in the e-mail message if users have permissions to view those attachments in the associated item.

- **Parameters**
  Use the optional parameter external to link to attachments in an external instance of your system.

- **Sample**
  The attached images display the reported issue. $FILEATTACHMENTLINKS(external).

   Result:
The attached images display the reported issue. **File Attachment(s):**

image1:  
http://servername/tmtrack/tmtrack.dll?AttachmentPage&AttachmentId=45

$ITEMNUMBER()

- **Description**
  
  For primary items, this tag provides the prefix and ID number of the item associated with the e-mail. For auxiliary items, this tag inserts the singular item name and a description of the item.

- **Usage**
  
  Use this tag to include the singular item name. The singular item name is defined in SBM Composer and can be viewed on the **General** tab of the **Edit Table** dialog box for the applicable auxiliary table.

- **Parameters**
  
  None.

- **Sample**
  
  $BEGINSUBJECT()$USERSUBJECT()$TTID()$ENDSUBJECT()$STRING(IDS_EMAIL_NOTEFROM)$SENTBY()$STRING(IDS_EMAIL_ABOUT)$ITEMNUMBER()

  **Result:**

  Note from Administrator about **BUG000173** [ttid: 1000,109]

$ITEMTYPENAME()

- **Description**
  
  This tag inserts the singular item name of the primary or auxiliary item.

- **Usage**
  
  This name is provided in SBM Composer and can be viewed on the **General** tab of the **Edit Table** dialog box for the applicable primary or auxiliary table.

- **Parameters**
  
  None.

- **Sample**
  
  $STRING(IDS_EMAIL_TOVIEW) $ITEMTYPENAME(): $LINK()

  **Result:**

  To View Issue:  
  http://servername/tmtrack/tmtrack.dll?View&I=109&T=1000
$TTID() 

- **Description**
  This tag inserts the [ttid: table ID, record ID] identifier required by the E-mail Recorder feature, which attaches e-mail messages sent from an external e-mail client to the item from which they were sent.

- **Usage**
  By default, the $TTID() tag is enclosed by the $BEGINSUBJECT() and $ENDSUBJECT() base template tags in the default.txt user e-mail 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 Configuring E-mail Recorder [page 105].

- **Parameters**
  None.

- **Sample**

  $$BEGINSUBJECT()$USERSUBJECT()$TTID()$ENDSUBJECT()$STRING(IDS_EMAIL_NOTEFROM)$SENTBY()$STRING(IDS_EMAIL_ABOUT)$ITEMNUMBER()$$

  Result:

  Note from Administrator about BUG000173 [ttid: 1000,109]

$USERSUBJECT() 

- **Description**
  This tag provides the text in the Subject box of the Send E-mail dialog box.

- **Usage**
  To insert the text into the Subject line of the message, it must be enclosed by the $BEGINSUBJECT() and $ENDSUBJECT() base template tags discussed in Base Global Template Tags [page 165].

- **Parameters**
  None.

- **Sample**

  $$BEGINSUBJECT()$USERSUBJECT()$TTID()$ENDSUBJECT()$STRING(IDS_EMAIL_NOTEFROM)$SENTBY()$STRING(IDS_EMAIL_ABOUT)$ITEMNUMBER()$$

  Result:

  Note from Administrator about BUG000173 [ttid: 1000,109]

$USERBODY() 

- **Description**
This tag inserts the text provided by the user in the **Message** box of the **Send E-mail** dialog box into the body of the message.

- **Usage**
  Include this tag to see the body of the e-mail message.

- **Parameters**
  None.

- **Sample**

```tag
$BEGINSUBJECT()$USERSUBJECT()$TTID()$ENDSUBJECT()$STRING(IDS_EMAIL_NOTEFROM)$SENTBY()
$STRING(IDS_EMAIL_ABOUT)$ITEMNUMBER()
$USERBODY()
$STRING(IDS_EMAIL_TOVIEW) $ITEMTYPENAME(): $LINK()
```

Result:

note from Administrator about BUG000173

Hi, Bill. Can you please assign this issue to me? Thanks, Carmen.

To View Issue:
http://or-pu-en2k8x32/tmtrack/tmtrack.dll?View&I=109&T=1000

**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?.
### $BEGIN_SUBJECT(), $END_SUBJECT()

- **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)**

  ```html
  $BEGIN_SUBJECT()$NOTIFICATION() - $ITEMNUMBER() $TTID()$END_SUBJECT()
  <html>
  <head>
  
  Result:
  
  subject  CAR - Any Change Request changes state - UPLA000142 [ttid: 1003,19]
  ```

### $GET_SETTINGS_STR()

- **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 Guide.

- **Sample**

  For assistance, contact $GET_SETTINGS_STR(AdminEmailToolbar)

  Result:

  For assistance, contact SBMA Administrator@serena.com

### $KNOWLEDGE_BASE()

- **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:

**$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.

**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 without the field display name.

• **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 field display name or database field name between the parentheses. If you use the database field name, be sure to omit the TS_ prefix. If you want to return the value for a *Sub-Relational* field, use the field display name.

  • **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.

• **(JOURNAL_FIELD_NAME, 1)** - For *Journal* fields, this displays the last comment in the specified *Journal* field. Use the second parameter to specify how many entries to include from the end of the *Journal* field.

  **Important:** If the second parameter is not specified, the contents of the entire *Journal* field are included.

• **Sample**

```
$FIELDVALUE(DOC_LEAD)
<br>
$FIELDVALUE(PROJECTID)
<br>
$FIELDVALUE(PROJECTID, FULL)
<br>
$FIELDVALUE(SUBMIT_DATE)
<br>
$FIELDVALUE(WRITER, NO_EMAIL)
<br>
$FIELDVALUE(STATUS_LOG, 2)
```

**Result:**

**Pam Doc Manager**

Serena Service Manager

Base Project:Documentation Project:Serena Service Manager

08/20/2015 01:09:42 PM

Allison Tech Writer

08/20/2015 02:42:39 PM - Administrator
Please update the readme.

08/20/2015 02:43:25 PM - Administrator
Also, please update the Installation Guide.
$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) $ITEMTYPEPENAME():</b> $LINK(TRUE, Click here.)

  Result:  
  
  **To View Change Request:** [Click here](#).

$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. This enables you to change the sender of an e-mail that is sent from an item.  
  
  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

```html
<html>
<head>
<meta http-equiv="Content-Type" content="text/html">
</head>
<body>
  Specifies an item link that opens the item in either the SBM or SRC mobile app.
  <br>
  <br>
  The tag inserts the appropriate URL (sbmmobile:// or srcmobile://) depending on the
  link type you select in a notification.

• Parameters
  - TRUE - Applies only to HTML templates and returns a mobile 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 mobile hyperlink to the primary or auxiliary item to which the e-
    mail message pertains.

• Sample
```
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.

Adding Custom Spell Check Dictionaries

SBM ships with three English dictionaries, a technical dictionary, and an accented words dictionary.

The English dictionaries include American English, Canadian English, and British English. The English dictionary checked depends on the user's locale setting. The American English dictionary is used for other locales outside of Britain and Canada. Other lexicons can be purchased from third-party vendors and added as described below.

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.

You can add additional dictionaries for use by the Spell Checker by placing the custom dictionaries in the bin directory on the SBM Application Engine Web Server.

CAUTION:

⚠️ Do not modify the provided standard dictionary files. These files are overwritten when you upgrade SBM.

To add a custom Spell Check dictionary:

1. Using a text editor, create a file named with a .tlx extension, such as custom.tlx.
2. Add words to this file that make up your custom dictionary. The file should only contain one word per line, followed by a carriage return.

3. Add the file to the installationDirectory\Serena\SBM\Application Engine\bin directory.

Using Web Queries with SBM Session Cookies

For Web queries to work with SBM Session Cookies, users must add their login parameters to the SBM URL. For example, if the Web query is:

http://servername/tmtrack/tmtrack.dll?ReportPage&Template=reports→%2Flistframe&TableId=1000&Target=Query&QueryName=-6&ShowSubLinks=1

The user must add &ttAuthUID=USERNAME&ttAuthPWD=PASSWORD to the URL. For example, Bill would add his login ID and password (app) as follows:

http://servername/tmtrack/tmtrack.dll?ReportPage&Template=reports→%2Flistframe&TableId=1000&Target=Query&QueryName=-6&ShowSubLinks=1&ttAuthUID=bill&ttAuthPWD=app

SBM Session Cookies also enable users to append a user name and password to a URL to set a session cookie on the browser. For example:

http://servername/tmtrack/tmtrack.dll?StdPage&Template=wrapper→&ttAuthInfo=am91OmpvZXNwd2Q=3D

This attempts to log in Joe with password joespwd in coded form. Joe could also attempt to log in with password joespwd in un-encoded form:

http://servername/tmtrack/tmtrack.dll?StdPage&Template=wrapper→&ttAuthUID=joe&ttAuthPWD=joespwd

To access Serena Work Center, users must include the corresponding shell extension. For example:

http://servername/tmtrack/tmtrack.dll?shell=swc→&StdPage&Template=wrapper&ttAuthUID=joe&ttAuthPWD=joespwd

To access Serena Request Center, users must include the corresponding shell extension. For example:

http://servername/tmtrack/tmtrack.dll?shell=srp→&StdPage&Template=wrapper&ttAuthUID=joe&ttAuthPWD=joespwd

Performing a Silent Installation

You can optionally run the suite installer and SBM Configurator in silent mode if you want to install the components without using a graphical interface. You enter parameters in the command line ahead of time, and then the installer runs without prompting you for any information.
**Silent Install Options**

The silent installation performs either a complete SBM install on your server. If SBM is already installed, the silent install performs an applicable **upgrade**.

*Note:* SQL Server Express is not installed by the silent installer.

**Performing a Silent Install**

The silent install includes all of the SBM components.

**To perform a silent install:**

1. Navigate to the directory that contains the suite installer executable.

2. Open a command window and run the suite installer silently. In the command window, type the suite installer executable name, and then append the following to install to the default location:

   `/S /v"/qb /L*v c:\install.log"

   To install to a location of your choice, enter the installation location after `INSTALLDIR=` as shows in the following example:

   `/S /v"/qb INSTALLDIR="D:\Program Files\Serena" /L*v c:\install.log"

   Note that you specify the installation location after `INSTALLDIR=`. For more information on parameters available in the MSI installer, refer to http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx.

3. After the installation is finished, configure your installation by launching SBM Configurator from the Windows **Start** menu.

4. Finish the configuration and click the **Export** button to export your changes to a configuration snapshot file. Save the file (snapshot.cnfsnp) to your local machine. Use this configuration snapshot file if you want to perform a silent installation and silent configuration with no user input. Note that you must run the installer (which distributes the SBM Configurator files) before you can run SBM Configurator silently.

   **Tip:** After you export the snapshot, you can manually edit certain attributes as necessary. For distributed installations, the host name values you enter during the initial configuration might not apply to the next server you configure (unless you entered `localhost` as the host name). In that case, you must edit the exported configuration snapshot file and change the host name value that appears in the **PanelOrder** and **Host** parameters before you use import the snapshot on another server.

   **Note:** The database passwords that you enter in the SBM Configurator are encrypted in the configuration snapshot file.

5. To run the SBM Configurator silently, navigate to the directory that contains the `ConfigurationUtility.exe` and pass the configuration snapshot file as an argument. For example:
Tip: You can also upgrade the SBM Application Engine and Orchestration Engine databases by including either of the following parameters with the SBM Configurator command: /d or /database_upgrade.

6. Launch SBM Configurator and verify your configuration settings.

Performing a Silent Upgrade

You can also upgrade an existing installation using the silent install option. The silent upgrade is identical to a clean install, except that an upgrade un-installs the currently installed components before installing the new components.

Prior to the upgrade, it is recommended that you export a snapshot of the current configuration and then import the snapshot once the upgrade is finished. This eases the configuration portion of the upgrade process because the previous configuration will be carried forward and only new components that might have been added will need to be configured.