Symantec™ ServiceDesk 7.1 SP2 Customization Guide

Symantec™ ServiceDesk 7.1 SP2 Customization Guide

Documentation version:

PN:

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About Symantec® ServiceDesk 7

With Symantec® ServiceDesk 7 software, you can provide the level of service that your organization expects and can afford. ServiceDesk can keep hundreds—even tens of thousands—of computers running efficiently and provide new services on a regular basis. The key is to create an organized environment that quickly responds to reported issues, advertises, and provides new services to the organization. The ultimate goal is to provide better service by automating as many steps as possible. Where automation is not possible, the goal is to increase the efficiency of the people who provide the services.

Target Audience

This guide (particularly sections 2 and 3), is for administrative users who plan to customize ServiceDesk 7 on their own. You can also leverage experienced consultants to help.

Note: You must have knowledge of and be experienced with Symantec Workflow to perform many of the configuration steps explained in this document.

Relationship Between ServiceDesk 7 & Symantec Workflow

ServiceDesk 7 relies upon Symantec Workflow software to drive the core ServiceDesk 7 ITIL processes, and the Service Catalog and Knowledge Base process. Symantec Workflow is a critical technology to understand, as it is fundamental to the functionality and customization of ServiceDesk 7. Most customization explained in this document is done using this tool.

ServiceDesk 7 processes are contained in Symantec Workflow projects that the ServiceDesk 7 installation provides.

ServiceDesk 7 follows a different paradigm than other help-desk applications in that it is process driven, not data driven. The process enforces the rules. Symantec took great care in creating the processes, taking into account customer feedback and ITIL best practice recommendations.

Note: Changes to a Symantec Workflow project require testing and deployment to production in order for the changes to become visible to ServiceDesk 7 users.

The instructions in this document cover the basics of deployment. More in-depth instructions on deployment and using the Debugger for testing are covered in the Symantec Workflow documentation.

Process Manager (ServiceDesk) Database

The term “Process Manager” refers to the database that stores process data, and ServiceDesk data such as groups, users, and permissions. The Process Manager database is a standard part of Symantec Workflow. When you install ServiceDesk, it is expanded to become the ServiceDesk database. However, it is commonly referred to as “Process Manager”. This database resides on the SQL Server computer.

Relationship Between ServiceDesk 7 & Altiris Notification Server Computer

Note: Symantec Management Platform 7.0 is the product installed on the Notification Server computer that manages the licensing.

Previous versions of Altiris Helpdesk Solution used the Notification Server computer to define business rules; now all of these are handled in Symantec Workflow. ServiceDesk 7 relies upon Altiris Notification Server for three functions:

- Licensing information.
- IT asset locations, configurations, and historical information.
- Exposure to the Configuration Management Database (CMDB)

It is required to have Notification Server computer running and configured before you implement ServiceDesk 7.

Best practice : Keep It Simple in the Beginning

Out-of-the-box, ServiceDesk is intended to require little customization; use this guide as a checklist to identify the most important aspects to customize. Keep the initial implementation of ServiceDesk 7 easy enough for most of your staff to understand and manage. Aim to provide base functionality and the services that are needed to achieve a reasonable amount of satisfaction, not the ultimate “end all” solution. Then, build up the ServiceDesk 7 system over time as the support staff and the end users become more familiar with it.

Phases in Implementing ServiceDesk

This document organizes the process of implementing ServiceDesk 7 into three phases.

Phase 1:	Process and Workflow Planning.
Phase 2:	Installation, Configuration, and Basic Customization.
Phase 3:	Advanced Customization.

Chapter 2

Phase 1: Process and Workflow Planning

This chapter includes the following topics:

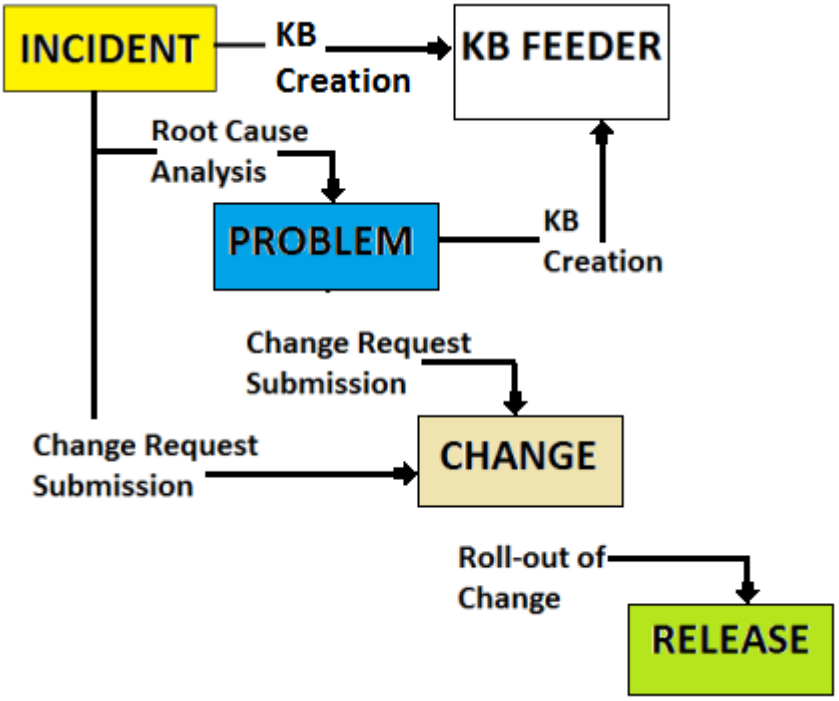
Phase 1: Process and Workflow Planning

In this initial phase, you consider the processes that you want to use in ServiceDesk 7. You can use the following processes:

- Four core ITIL processes (Incident Management, Change Management, Problem Management, and Release Management)
- Service Catalog process
- Knowledge Base process

You also want to map out your current process. Mapping your process can help you identify where customization need to be made in the “out of the box” ServiceDesk 7 processes.

Step 1: Select Pieces of ServiceDesk 7 to Use



The following explanations can help you determine what processes you want to use in ServiceDesk 7. Most clients use at least one process, the Incident Management Process . These processes directly follow Symantec's opinion of ITIL best practices, which are determined through customer feedback and scrutiny of ITIL documentation.

- Incident Management Process
  This process focuses on restoring the user to an operational state as quickly as possible. The level of operation is identified in the Service Level Agreement.
- Problem Management Process
  This process aims to reduce the occurrence and negative effect of incidents that are reported to the ServiceDesk. The process looks proactively for trends in the environment to identify the root cause of incidents and initiates action to improve or correct the situation.
- Change Management Process

This process aims to plan for and control the risks and effects of changes to the IT infrastructure. Changes are handled according to standardized procedures to minimize effects on service.

- Release Management Process
  This process aims to distribute and maintain tested versions of software and licenses for the software. It provides oversight of all other changes and releases to identify any problems or conflicts.
- Knowledge Base Process
  This process provides a centralized location for the information that is used in diagnosing and resolving incidents.
- Service Catalog.
  The Service Catalog provides links to routine "self-service" functions. Examples include automated password reset, and automated software request.

Step 2: Identify Current Processes

Think about how your organization currently addresses incidents, both the formal and the informal processes. Think about how incidents are reported, who is the first to find out about them, what happens next, and so on.

Plot the current processes in flow charts, noting where you want to see changes. These flowcharts can help guide you when you go into Symantec Workflow to do customization.

Consider these questions when thinking about your current processes:

- Is the process different if the issue is a hardware problem or a software problem?
- Is the process different if you do not know what causes the issue, only that a user is unhappy?
- How do you determine if an issue is a high priority or what the level of effect to the organization is? Priority, Urgency, and Effected fields manage this part of the ServiceDesk 7 system.
- When the root cause is identified, what tools does your team use to troubleshoot and remedy the situation?
- Do you handle incidents differently than problems (based on the ITIL definitions of incidents and problems)? If so, what is the process from start to finish for the Level 2 workers to follow?
- How are service requests handled? For example, if an employee needs to move to a new office, who in your organization is involved and what are the process steps?

- What do you want end users to be able to do themselves?

Consult your IT staff to determine what part different employees take in workflows. Also, consider how your staff's areas of expertise may influence your ServiceDesk 7 implementation.

Chapter 3

Phase 2: Installation, Configuration, and Basic Customization

This chapter includes the following topics:

- Define E-mail Content
- Customize E-mail Monitoring
- Modify the Time span for end users to Confirm Incident Resolution
- Establish Change Management Groups
- Change Risk Assessment Participation for Change Management
- Verify Problem Categories

Phase 2: Installation, Configuration, and Basic Customization

Before you install ServiceDesk 7, you must install Notification Server. You need to determine where permissions come from. You need to set the location of the databases. You need to determine when you want to migrate incidents categories, and knowledge base content. You must also make sure that you meet all the prerequisites for migrating the knowledge base contents.

See "Installation & Configuration" on page 20.

Installation & Configuration

This section includes information about Notification Server and ServiceDesk 7 configuration steps.

See "Notification Server" on page 20.

See "ServiceDesk 7" on page 21.

It also includes information about migrating incidents, categories, and knowledge base content.

See "Migrate Incidents" on page 21.

See "Migrate Categories" on page 22.

See "Migrate Knowledge Base (KB) Content" on page 22.

Notification Server

Before you install ServiceDesk 7, you must install Notification Server and complete at least an initial discovery and inventory. For details, see Notification Server online Help .

ServiceDesk 7

The ServiceDesk 7 installation installs both ServiceDesk and Symantec Workflow Solution.

The ServiceDesk 7 Installation Guide covers all the necessary installation steps and configuration. Configuration includes the following important steps:

- Determining where users/groups/organizations and permissions come from (typically Active Directory)
- Setting the location of databases
- Migrating existing Helpdesk Solution 6.5 content

Migrate Incidents

Migration of incidents can happen during installation or afterwards, from the Service Catalog. Best practice is to migrate all incidents from Helpdesk Solution 6.5. Incidents from Helpdesk Solution 6.5 are not truly "migrated," rather metadata is brought in. Technicians see the incidents but work them in Helpdesk Solution 6.5 with **IFrame**. Therefore it is necessary to keep Helpdesk Solution 6.5 up and running until all of its tickets are closed. Best practice is to cut off users from submitting new incidents into Helpdesk Solution 6.5 once incident migration occurs. Migrated incidents receive their own category in ServiceDesk and are prefixed with **SDM-**. You can run a report or sort the list of all migrated incidents to see if the count is down to zero. Once the count is at zero, you can take down Helpdesk Solution 6.5.

Closed Helpdesk Solution 6.5 incidents are automatically imported into the ServiceDesk 7 database for reporting purposes. In fact, closed tickets are not available for migration, since they are already handled behind the scenes. Closed tickets are imported upon the migration. As tickets are closed they are imported post-migration. A ServiceDesk process automatically checks for them once a day and imports those that are found.

The KB Migration Wizard is for importing only the Helpdesk Solution 6 knowledge base content that was added to Helpdesk Solution through the installation of a KBI solution add-on for Helpdesk Solution. The Migration Wizard was not designed to import user-created knowledge base content from Helpdesk Solution 6.

If you want to import user-created KB content from Helpdesk Solution 6, then you must customize the SD.KBMigrationWizard project. To obtain project development or customization assistance, please contact Symantec's Consulting Services Group or one of Symantec's Partners that provide consulting services for Workflow/ServiceDesk. For more information about Symantec's Consulting Services Group, call 800-721-3934 or visit them online at following URL:

http://www.symantec.com/business/services/category.jsp?pcid=consulting_services.

Migrate Categories

Migration of categories can happen during installation or afterwards, from the Service Catalog. If you intend to use categories from Helpdesk Solution 6.5, best practice is to import them before new incidents are created in ServiceDesk.

Migrate Knowledge Base (KB) Content

Migration of KB content is performed by running a KB Migrator executable that is found in the Service Catalog. Out of the box, the migrator is configured to migrate Helpdesk Solution 6.5 HTML files. However, the process can be modified to import content from another document repository. The project that performs the migration is SD.KBMigrationProcess.

Prerequisites:

- Before you run the KB Migrator, you must copy the directory that houses the KB files to the ServiceDesk server. This requirement is due to .NET restrictions at the command-line level.
- The directory structure for the KB content to copy must follow this format: `C:\Libraries\another directory\Articles`. This structure is the directory structure of Helpdesk Solution 6.5 knowledge base content by default. The "`another directory`" folder represents the individual libraries.
- You must also grant the Network Service account access to the directory.

After migration, you can delete the copied directory (unless there were failures and you want to run the migrator again for the .failed content).You can run the migration tool multiple times. However, do not run the migrator against any content that is already migrated due to high risk of duplication of articles.

Be advised that the migration process takes a long time to complete. Testing against the average-sized KB of a few thousand entries, it took approximately eight hours. You can check the Configuration Logging Utility for Symantec Workflow to make sure that it is still running. In the tool, right-click the KB migration process, turn on logging, and go to the **Log View** tab.

The migration wizard sends notifications throughout the migration process to the email address that is specified in one of the wizard screens. You are notified each time a KB category successfully migrates, and if there's a failure (down to the specific article that failed).

If a directory fails migration multiple times, you should take the following actions:

- Remove the articles from the source directory.

- Delete the source directory.
- Then, try to migrate smaller subsets of those articles to help identify a problematic article.

Also, you should turn on a“visual” setting in the migration wizard. It provides more detail. The process tries three times before it deems a true failure.

Note that the numbering of the migrated articles is new, and is based on the order of import. You can retain your old numbering, however that would also require modifying SD.KBMigrationProcess to get the current number of the article.

After migration is complete, the original source directory can be deleted. Migrated knowledge base articles are stored to the Process Manager database. However, the images that are used in articles are saved to the server drive.

Versioning Processes

Before you make changes to the Symantec Workflow processes that ship with ServiceDesk, it is important to determine a versioning process. Versioning enables you to return to a previous working state if necessary, and to track the origin of a change.

By default, each time you click Save in Symantec Workflow, a copy of the project is automatically stored in the `C:\Program Files\Altiris\Workflow Designer\WorkflowProjects\Backup` directory. Up to 10 copies are saved.

To version a process

1. Create a copy of a project, renaming the copy accordingly.
2. Make and test changes.
3. Publish to production. Use the name of the project (renamed in step 1).

A more sophisticated change management process is detailed in a series of four videos that are posted to http://www.WorkflowSwat.com, under **Learn**. This method, for maintaining versions of processes, is recommended for any company that has larger scale usage of Workflow processes. Symantec recommends reviewing both methods then making a decision that makes sense for your organization.

Development Considerations When Publishing a New Version

An updated URL application property should not break a process that is “in progress” that uses the old URL. Changes in the process are more likely to cause breaks to the process in this state. For example, missing data is a change that causes incompatibility.

The way to mitigate incompatibility is to properly build the new version. For instance, say that you have a process with two **Dialog Workflow** components. In the first one, you collect “Name” and “City of Birth” from the user. Then in the second **Dialog Workflow** component you display this information to a manager.

Now you want to update the process because of a new regulation. Therefore, in the first **Dialog Workflow** component, you also start collecting “Age.” In the second **Dialog Workflow** component, you add a rule that shows the manager a warning form if the user is 13 or younger. If you add this rule, then all submissions that were made before “Age” was collected are broken. The manager opens a task and gets an error. The error says **“object reference not set to the instance of an object”**. The error is displayed because “Age” does not exist.

To write the new version correctly, you need to add a Variable Exists rule. The Variable Exists rule is to make sure that “Age” exists before the workflow reaches the rule that evaluates ages and compares them to 13. If you wrote the second version properly, there should be no risk. Since, all the instances that were already submitted without age would not break, and all the new instances that were submitted with age would work.

Basic Steps for Versioning

To publish & version a ServiceDesk process in Symantec Workflow

1. Create the new version of the project by either copying an existing project, or unpacking the original and renaming it as desired. For example, append a version number to the name, such as “SD.RoutingRules_2_0.” Leave the Generate New Service ID checkbox cleared, otherwise the link between the process and ServiceDesk is broken.
2. Modify the project as needed. Make note of the type of the project. Also, decide whether the process is to be published to the same virtual directory as the current process. The type of project determines if you need to build in rules to handle new data. The same applies to publishing to the same virtual directory.
3. If it is the first time a project is deployed, it is necessary to select the Process Manager publishing method. Choose either “Publish to Process Manager Forms” or “Publish to Process Manager Services.”
   - The rest of the default settings are acceptable.
   - Select the server where you want to publish your changes and click OK.

4 From the **Application Properties Editor** screen, note the new Base URL to Project. Copy this link.

5 Click Save and complete the publishing process. If you are prompted, answer the following:

- **Open deployed project** --> No
- **Deploy workflow to NS as DialogWorkflowItem** --> No

About application properties

ServiceDesk knows which Symantec Workflow processes to invoke based on the URL fields that are populated from the **Admin tab > Data > Application Properties** screen. The data in these URL fields, along with other information that is configured here, are called application properties.

Processes “in progress” look to Process Manager for their application properties, (individual processes do not store application properties).

Updates made to the application properties are not immediately applied to Process Manager, because Process Manager relies on cached application properties. You can force the new application properties by restarting IIS, thus clearing the cached data. Unfortunately, clearing the cached data is not usually feasible in a production environment. Once Process Manager updates its cache, then the current processes starts to use the new application properties.

By default, Process Manager updates its cache every 45 minutes, and is set under **Admin > Portal > Master Settings > Optimization > Clean Cache Time**. Which means, if you update a URL field application property with a new process URL, it does not immediately affect the live processes.

Restoring ServiceDesk Processes

ServiceDesk comes with Workflow packages. These packages are unpacked when launched. The original package content is retained, unless a user intentionally overwrites that package. Therefore, if you need to revert to the original project, unpack the project again.

The Workflow Designer also saves backups of a process upon each save, up to 10. Best practice is to save your changes periodically (i.e., not after every change) to have meaningful backup copies. These copies are stored in a Backup directory: `Program Files\Altiris\Workflow Designer\WorkflowProjects\Backup`.

If you need to obtain the original packages that shipped with ServiceDesk, rerun its installation.

Project Differential Tool

Note: This tool is not yet available in the released version of Symantec Workflow, but should be available in the future.

The Workflow Differential tool takes a baseline project and a secondary project and compares the two, identifying the differences. Use this tool as a first step to identify changes when troubleshooting a project.

The first project that is selected in the tool is the project to which a second project is compared. Any changes to the following in the second project are identified. These changes are:

- The libraries the projects use.
- Project properties
- Project resources.
- Project models.
- The components' settings or names.

To open the Project Differential tool in Workflow Solution 7 from the Projects list, select **Advanced > Compare Projects**. Follow the prompts to select the baseline and the secondary projects. If you want, you can use the import feature to select which changes you want to import into the destination model.

Basic ServiceDesk 7 Customization

Editing the Core ITIL Processes

When you open the core ITIL projects from packages, (for example, **SD.IncidentManagement**), the process name by default is the file name of the package.

Note that it is necessary to add a space in between `IncidentManagement`, `ChangeManagement`, etc., within the name of the project that you unpack. If you do not add a space, and accept the default process name, then you see two entries for incident management in ServiceDesk, `SD.Incident Management`" and `SD.IncidentManagement`. For example, the **My Task List** tab displays the names of both process.

Verify Users, Groups, and Organizations

ServiceDesk 7 automatically reads users, groups, and organizations from the Active Directory domain if one was specified during the installation. Log on to ServiceDesk 7 as the administrative user to **Admin > Users > Accounts > Manage Users** page. Look at the information to see if it appears correctly and to see if it is complete. Administer users, groups, and organizations as needed. Symantec recommends using groups as the primary way of maintaining permissions.

ServiceDesk 7 comes with default groups to which you can add users. During installation it is possible to map existing AD groups to these default groups. The groups and associated permissions are defined in the ServiceDesk 7 User Guide.

If native authentication is to be used solely without Active Directory, you must add users manually to each respective group.

If you create a new group in ServiceDesk, you must manually add that group to the application properties in ServiceDesk. Now the group shows up as available data in Symantec Workflow. This step is what makes the new group show up in the profile properties list in Symantec Workflow. (Note: the term “application” is synonymous with “profile” properties in Symantec Workflow.)

To add a new group to the application properties:

1. Create the new group from **Admin > Users > List Groups**.
2. From the Admin tab, go to **Data > Application Properties**.
3. Click on the **Actions** button (orange lightning-bolt) for **ServiceDeskSettings** and select **Edit Profile Definition**.
4. Click on **Next**.
5. Scroll down and click on **Add Definition Value**.
6. In the **Name** field, enter the name of the new group. For example, “GroupSupportIII.”
7. Enter **User Groups** as the category.
8. Leave the data type as text. In the **Default Value** field, enter “SD.IncidentManagement.”
9. Click on **Save**.
10. Click on **Finish**.

If the new category does not appear in Symantec Workflow, try restarting IIS and reloading the Symantec Workflow project. For example, you browse the profile properties in SD.IncidentManagement.

Set up Incident Categories (Classifications)

A good category system is key to building a smoothly running ServiceDesk 7 system. ServiceDesk 7 sorts the more useful reports by category. Sorting reports by category lets you see what types of issues are most common and what trends occur in your environment.

ServiceDesk 7 ships with a list of suggested categories that you can find under **Admin > Data > Hierarchy Data Service**. These are the same default categories used in Altiris Helpdesk Solution 6.5. Change the list as much as you want. Up to 10 category levels can be used. You can also import the categories that you used in Helpdesk Solution 6.5 during installation or afterwards, from the Service Catalog.

Remember that the more complex you make the category system, the harder it might be for ServiceDesk 7 workers to correctly categorize incidents. If workers do not categorize incidents correctly, steps in your processes may be skipped. incorrect categorization may also lead to the wrong steps being processed, or an incident being routed incorrectly. The ramifications depend on the customizations that you set up for your categorization. Out of the box, categories are pieces of the information that are assigned to an incident, which do not effect on workflow.

Best practice is not to delete a category once you start using it because an incident may be assigned to that category. The incident is not removed, rather it retains the old category. Therefore, it is left out of reporting and search results if only the new category is used.

Note: Imported incidents maintain the categorization originally assigned. Imported categories are available for incidents going forward. Imported categories do not map to the default categories in ServiceDesk 7. Therefore, some cleanup may be required. For example you may want to remove the categories that seem redundant or not needed for your organization.

Verify Default Priority, Impact, and Urgency Values

The Priority, Urgency, and Impact fields of incidents can help you manage Service Level Agreements and comply with the concepts of ITIL service management.

The Priority and Urgency fields indicate how quickly an issue should be resolved. The Impact field indicates how broad an issue is. The effects of an issue may be considered low if only one person is affected. The effects are considered to be high if the whole organization is affected.

ServiceDesk 7 ships with the following values for these fields:

- Default priority values: Emergency, urgent, high, normal, minor, or low.

- Default urgency values, on the incident submit, form that is shown to end users: No Immediate Urgency, Preventing Some Non-Urgent Work, and Blocking Critical Business.
- Default impact values, on the incident submit, form that is shown to end users: Single User, Entire Team or Group, Entire Department, or Unsure.
- Default urgency values (to technicians): Core business service, Support service, and Non-urgent services.
- Default impact values (to technicians): Department/LOB/Branch, Small group or VIP, and single user.

Note: You can change the values, however doing so requires caution and a good understanding of the Symantec Workflow software.

These instructions focus on impact and urgency additions to Incident Management. Note that if you decide to make priority, impact, and/or urgency changes global, you must make many more updates. You must make the same updates to Change Management and/or Problem Management.

Changing the priority values is likely the most difficult edit. The "emergency," "urgent," "high," "normal," and "low" are hard-coded throughout the Symantec Workflow projects for ServiceDesk. More so than impact and urgency values. Change priority values only when necessary.

This example adds "Financial Group" as a new impact, and "No Internet Access" as a new urgency value. Note that “Financial Group” is not a group of users in ServiceDesk, rather it is a group of employees in a company for this example. First, add these values to the form that the end user uses to submit an incident. Use this example as a model when you edit urgency, impact, and priority.

To add new impact and urgency values

1. The technician urgency, impact, and priority values are set as application properties, under **Admin > Data > Application Properties**. Log in to ServiceDesk as the administrator, and go to **Admin > Data > Application Properties**.
2. Click on **ServiceDeskSettings**, in the list of application properties.
3. Click on the **Actions** button (orange lightning-bolt) and select **Edit Values**.
4. Scroll down to the Urgency, Impact, and Priority category.
5. To add “Financial Group,” click on the **Add** button for **Impact**.

   Type “Financial Group” and click on **Add**. Click on **Save**.

6 To add “No Internet Access,” click on the **Add** button for **Urgency**.

Type “No Internet Access” and click on **Add**. Click on **Save**.

7 Scroll down to the bottom of the **Edit Instance** window and click on **Save**.

8 You must update the forms that contain impact and urgency. Then update the decision table, which the process uses to calculate the corresponding priority.

- If no changes to processes are made, any new urgency values are treated as a “No Match” in the decision table. Also, the impact value is equal “Non-Urgent Services.”
- If you add a new priority value to the application properties, but do not add that priority value to the decision table that calculates priority, Incident Management automatically sets the priority to “normal” even if the form selection was the new priority.

To add new impact and urgency values to the end-user Submit Incident form and the decision table that calculates priority

1 Open the `SD.Feeder.GeneralIncidentSubmitForm` project.

2 In the Primary model, open the **Create New Incident** Form Builder component.

3 The lower left section of the form contains the **Radio Button List** components for impact and urgency. Double-click on the radio button component under "Urgency of this need or issue."

In the **Items** list, add "No Internet Access."

4 Double-click on the radio button component under **"Who is Affected?"**

In the **Items** list, add **Financial Group**. You must expand the size of the radio button component box to see the new entry in the form.

5 Click **OK** to close the form.

6 Double-click the **Show Incident Information, such as Urgency, Impact, User, Needed by Date** Embedded Model component.

7 Open the **Set Impact Decision Tree** component.

- Click on **Next**.
- Click on **Add**, and type "Financial Group" to create the respective entry under the **Matches Rule**.
- Click on **Financial Group** under the **Matches Rule** and in the **Urgency** field on the right and type "Financial Group."

Note: We opt to use the same impact value (on the right) that the end user sees, rather than an internal or technician-side value. However, the rest of the values under the Matches Rule use the impact values that are technician-facing. You can see the difference if you click on “Entire Department” under the Matches Rule on the left. Notice the corresponding “Department/LOB/Branch” value, which appears on the right. Refer back to the bulleted list in the previous section to compare and see the subtle difference.)

- Click on **Finish**.

8 Open the **Set Urgency Decision Tree** component.

- Click on **Next**.
- Click on **Add**, and type "No Internet Access" to create the respective entry under the **Matches Rule**.
- Click on "No Internet Access" under the **Matches Rule** and in the **Urgency** field on the right, type "No Internet Access."
- Click on **Finish**.

9 Set the priority value for the new urgency and impact values; priority is based off the combination of urgency and impact. Double-click the **Calculate Priority Decision Table** component

- Click on **Next**.
- Double-click the **Matches Rule** for **Impact** (vertical, on the left).
- Click on **Add**.
  Type "Financial Group" and click **OK**.
- Click **OK**.
- Double-click the **Matches Rule** for **Urgency** (horizontal, across the top).
- Click on **Add**.
  Type "No Internet Access" and click **OK**
- Click **OK**.
- In each "cell" that displays invalid, type the desired priority value. It must be exact (no extra spaces). For example, set all of the Financial Group priorities to "High" in all cells except for the cells corresponding to "no match."

10 Click on **Finish** when complete.

Note: The priority of "Normal" is hard-coded in the `SD.IncidentManagement project` > `CreateIncidentAdvanced model`, in the **Set Priority** embedded model. Open that model and replace "normal" with the desired value.

Additional Updates for Priority, Urgency, and Impact

You must also edit the priority levels hard-coded in the **Matches Rule** found for SLA calculation, found in `SD.DataServices` > `Setup SLA Requirements`.

The goal throughout processes in ServiceDesk is to use the application properties for populating the urgency, impact, and priority values when possible. Occasionally you come across hard-coded values. For example, in the Matches Rules like you see in the Setup SLA Requirements model.

To make priority, urgency, and impact values global, you must also update the components that have the hard-coded values found in the following projects:

- `SD.Feeder.ProbemCreation`

  The decision table for priority is in the `Create New Problem model` > **Set Priority** embedded model.

- `SD.ProblemManagement`

  The **Setup SLA** model that is inactive by default. If you choose to customize and use the model, be aware that hard-coded priority, urgency, and impact values are present.

- `SD.ChangeManagement`

Verify Close Codes

Close codes in incident management are: Completed Success, Training Required, Review Documentation, No Fault Found, Monitoring Required, Advice Given, Change Required, and Other. If you want, open the SDIncidentManagementProcess project and modify the list. These default values can be changed with no ramifications.

To modify the close code values for Incident Technicians

1. Open the `SD.IncidentManagement` project in Symantec Workflow.
2. In the Initial Diagnosis model, open the Initial **Diagnosis Dialog Workflow** component.
3. From the Interaction Setup tab, open the Dialog Model.

4 Open the **Work/Resolve Incident** Form Builder component. This Form Builder component contains the UI technicians access for working an incident.

5 Edit the items list within the **Drop Down List** component for **Close Code** to reflect the desired changes.

Portal Master Settings

Portal master settings are established during installation. However, in ServiceDesk, under **Admin > Portal > Master Settings**, it is recommended to review settings and make changes as necessary. At a minimum, make yourself familiar with what settings exist. Do not change settings for data like URL, or disable check boxes without fully understanding the implications. You should not need to change that type of information.

- **Account Management > Password Expire Months**.
  Default is six months.
- **Account Management > Register Fail e-mail address**.
- **Account Management > Security Question 1**.
- **Email Settings > Admin Email**.
  Change to actual domain admin email address.
- **Process Manager Events**.
  These settings determine whether a particular event automatically generates a message, which ServiceDesk delivers. If users complain about getting prompts within the portal at certain points within a process, you can disable them here. Prompts are different from email notifications, which are handled in the Workflow project.
- **Report Settings > Process Reporting Interval**.
  Makes the information available to web parts quicker. Can be dropped to a lower number. Good to use for a smaller-scale SD instance with only a handful of technicians. This setting would work with the refresh time of the Web part itself.
- **Workflow Settings > Task Refresh Time**.
  Reduces the default time, in milliseconds, to make a task available to the next user in line.
- **Workflow Settings > Auto Refresh Task Page**.
  Selected so the user doesn't have to manually refresh the task list.
- **Workflow Settings > Task Lease Time**.
  Default is 15 minutes, this time frame can be changed depending on how often you want to check if a lease is broken. This setting comes into play when

someone closes a task. When you close a task, it can take up to 15 minutes to find out whether a task is leased or not. Do not lower the time too much. Doing so increases overhead on the system.

- **Customization > Logo URL**.
  Adds a company logo in place of the Symantec one in the upper left.
- **Process Manager Settings > Update Business Hours**.
  Sets the business hours in the portal.
- **Process Manager Settings > Help Link URL**.
  Point it to where you have your ServiceDesk documentation housed.

Warning: Do not change settings under Application Management, or Process Manager Events.

Determine AD Sync method:

- Internal sync method, which is selected by default. Built in to the Process Manager. Syncs everything. **Process Manager Active Directory Settings > AD Sync Process Interval** (default is once an hour).
- Workflow method, enabled by checking the **Process AD Changes Using Workflow** checkbox.

Introducing Active Directory: Post-installation

If AD settings were not provided during installation, it is possible to set up AD integration from the **Admin > Portal Master Settings** screen, under **Process Manager Active Directory Settings**. Configure these settings accordingly, then add the AD server under **Admin > AD Servers** page.

The **Process AD Changes Using Workflow** setting has an upside and a downside to consider: upside is that you can customize the AD Sync process in Workflow so only certain users/groups/organizations sync, therefore getting a better level of control. Downside is that it is more complicated process; it is an interaction of three projects to occur, so you're introducing another element of complexity.

Use the Ignore AD users field to choose not to sync the users that are listed here.

Customize the General Appearance of the Portal

In ServiceDesk 7, under **Admin > Portal > Master Settings**, there is a **Customization** section. The **Customization** section lets you set a company logo, pick a theme, menu style, and a few other appearance-related features. Users with customization permission can further modify their pages.

Customize Form Appearance & Content

In ServiceDesk, the **feeder** screens that are used to submit data and the pages that are used to work incidents are built using various form components in Symantec Workflow. Note that when the document refers to“forms,” that in ServiceDesk, forms refers to the dialog boxes that appear for entering or working with data that “feed” into the database.

Forms in Symantec Workflow are created using the Form Builder components, often housed within a **Dialog Workflow** component.

Forms in ServiceDesk are intelligent and enforce the validation rules that often had to be manually configured in Helpdesk Solution 6.5. These forms enforce required data and enforce the field data type. These forms can also have custom validation set-up to further improve the integrity of the data before it is submitted.

Customizing a form entails the following:

- Setting its appearance using a theme and template.
- Determining the wording on the form.
- Setting the desired closing messages.
- Setting the desired error messages.
- Adding data (additional fields) to forms.

The following sections offer examples to give you ideas of how you can make your own form changes throughout ServiceDesk 7.

Change the Theme and Template for a Form

Themes in Symantec Workflow dictate component control styles (like font attributes), dialog box (form) size, border width and style, and background images. Templates in Symantec Workflow dictate more general features, such as components for pieces of data you want standard across the process. For example, you can standardize the ticket header information in Incident Management. Templates also dictate features such as the Incident Management Logo.

You can modify form appearance by selecting from a range of theme and template styles provided, or create your own.

Note that if you modify a theme or template that came with ServiceDesk, the changes affect all forms that use that theme or template. If a new theme or template is created, it is necessary to manually apply the theme or template to its respective form.

These instructions explain working with themes and templates using the customer service satisfaction survey as an example.

To change the theme and template of the customer service satisfaction survey

1. In Symantec Workflow, open the `SD.CustomerServiceSurvey` project.
2. Double-click the **Customer Service Survey Main Form** Form Builder component.

   The **Web Form Editor** window opens.
3. Click the folder icon (the **Select Theme** icon) on the top left.

   The Select Theme and Templates window opens.

   - You can modify the theme that is listed in the window by clicking the **Edit Selected Theme** button and making the desired changes.
   - You can add a new theme by clicking the **Edit Project Themes** button, then selecting **Add** to access a blank theme to configure.
   - You can change the theme selection by selecting a different theme and clicking **OK**. You must click okay when you create a new theme to apply it.
   - You can also change the templates by going into the **Templates** tab on the **Select Theme and Templates** window. **Service Desk** is the template that the process uses. You can edit this template by selecting the template and clicking on the **Edit** button on the right.
     If you want to add a new template, click on **New** to add a new template, then configure the template.

Note: A form can use more than one template. It depends on how you want to present the data on the form.

To create a new theme using the Composer Theme Editor

1. New themes are created using a utility that is included with Symantec Workflow. From the Start menu, select **All Programs > Symantec > Workflow Designer > Tools > Composer Theme Editor**.
2. Click the **New** icon to start a new theme. Once the theme is saved, it automatically defaults to the directory where themes can be selected to when you edit a form.
3. New themes need to be applied manually to the respective forms.

To create a new template

- New templates are created within the form editor itself by right-clicking the form and selecting **Templates > New Template**.

Change Task Assignee

In **Dialog Workflow** components, the Task Assignments tab contains the user/group/organization to whom the task is initially assigned. You can change this assignment as desired by opening up the respective **Dialog Workflow** component, scrolling down the **Task Assignments** tab, and updating the Assignments section.

Make Changes to Form Text

This section explains how to make changes to existing text using the Customer Satisfaction Survey as an example.

To change text in the customer service satisfaction survey

1. In Symantec Workflow, open the `SD.CustomerServiceSurvey` project.
2. Double-click the **Customer Service Survey Main Form** Form Builder component.

   The **Web Form Editor** window opens.
3. Change the "Thank you" message at the top by double-clicking that component and changing the content of the **Text** field.
4. Change text style using the options under **Look and Feel**.
5. To adjust the size of a text field, click on the text field in the **Web Form Editor** and use the mouse to resize. You can also drag and drop existing form fields to reorganize the content.

Note: Keep in mind that the output variables for data collected are named to correspond with the default wording of its label. For example, the first Customer Satisfaction Survey question "Ability of ServiceDesk to diagnose your problem?" has a corresponding **Radio Button List** component to collect the user's input, and this component has an output variable called NewSurvey.QualityOfDiagnosis. If you change the label wording completely, it may be best to rename the variable that collects the output data by modifying the `SD.Data` project.

Modify error messages

Forms often have required fields. The process requires certain data to continue. Forms in ServiceDesk 7 have error messages built in, however you may want to modify them. By default, error messages in ServiceDesk 7 appear only if a required field is not populated. You can get more sophisticated with your error messaging. For example, a specific error message can appear if a field value violates a rule

other than the field being empty. For example, in a numeric field, an error message can say “the value must be between 1 and 10.”

The following instructions use the Customer Satisfaction Survey as an example.

To modify the message that appears when a required field is empty

1. In Symantec Workflow, open the `SD.CustomerServiceSurvey` project.
2. Double-click the **Customer Service Survey Main Form** Form Builder component.

   The **Web Form Editor** window opens.
3. Within the Form Builder component, find the required field for which you want to edit its error message. The label shows a red asterisk to indicate it is required. Double-click the field. For example, double-click the radio button field corresponding to the **Overall quality of the solution?** field.
4. Scroll to the bottom of the **Functionality** tab. Modify the **Required Error Message** field as desired.

   For example, change “Please answer the Overall Quality question” to “Please let us know how you rate the overall quality, your opinion is important to us.”

Modify Confirmation Pages Presented to end users

The following confirmation pages are presented to end users:

- “Thank you” page upon submitting the Customer Satisfaction Survey with positive results (`SD.CustomerServiceSurvey`).
- “Thank you” page upon submitting the Customer Satisfaction Survey with negative results (`SD.CustomerServiceSurvey`).
- Page that is presented when a ticket is reopened (`SD.ReopenIncident`).
- “Thank you” page upon submitting a knowledge base article suggestion (`SD.Feeder.KnowledgeBase`).
- Login failure form (`SD.LoginFailureForm`).

Many of these pages are found in the “feeder” Symantec Workflow projects, where information is initially submitted. Most exist as **Terminating Form** Builder components.

The example, which is used to demonstrate how to modify confirmation pages, modifies the **Thank you** page. This page is presented to end users upon submitting an incident.

To modify the confirmation page upon submitting an incident

1. In Symantec Workflow, open the `SD.Feeder.GeneralIncidentSubmitForm` project.
2. Double-click the **Thank You Terminating** Form Builder component, found at the bottom of the model.

   The **Web Form Editor** window opens.
3. By default, two variables are included in the form content, the incident ID variable and the variable containing the URL to track the incident. You can add more variables as desired by dragging and dropping them onto the Editor screen from the Variables list in the lower left.
4. To edit the text in the form, double-click the text component and modify the content of the **Text** field.

Adding Data to Forms

Adding data to forms requires two steps.

To add data to forms

1. Adding the new data to the respective data type, therefore enabling the variable that houses the data to exist. For example, adding CostCenter attribute to the Incident data type.
2. Adding the field to the form so the data can be captured. For example, creating a “cost center” input field for technicians to enter a cost center upon submitting an incident.

Step #1 is a very important. It is also more technical.

Warning: Use caution when removing components from a form. If you remove components, the output variables that these components designate are no longer valid after the removal. For example, a text box component collects data that is designated as “ReasonforRequest.” If you remove the textbox component, anywhere in the remainder of the process where “ReasonforRequest” is pulled and displayed an error initiates. The process is broken. A best practice true of any process is to disable components rather than remove.

Additional Form Customization

Additional form customization examples include adding more sophisticated form data validation, marking or unmarking required fields, and setting up custom events surrounding form fields. An example of custom validation is found in the

`SD.Feeder.GeneralIncidentSubmtiForm` project, in the **Create New Incident** Form Builder component, in the entry field for **Who does this issue affect?** Double-click that textbox component and scroll down to the Validation section to see the custom validation in place. The validation model in this example makes sure that the submitter isn't the primary contact if submitting for someone else.

By default, ServiceDesk forms enforce required fields for the pieces of information that the respective process requires. To require a field, right-clicking the input field and selecting the required path.

ServiceDesk forms can also enforce data format through use of the **Masked Edit** component. For example, if you add a cost center field or a phone number format to a form, the **Masked Edit** component enforces that specific format.

Establish Service Level Agreement (SLA) Times

Incident Management SLA

By default, the SLA timeframes in Incident Management are:

- **Basic SLA level**
  Overall late time span is 60 days, with a warning at 30 days. You can configure individual levels within this **Basic SLA level**. For example, give the Support level 1 eight hours to respond, with a warning at four hours. Same with SLA level Support II and "Escalated." Emergency late time span is two hours with a warning at one hour.
- **Emergency SLA level**
  Overall late time span is 60 days with a warning at 30 days. You can configure it to be more aggressive. For example, you can configure it to have an overall late time span of eight hours with a warning at four hours. Then give the Support level 1 4 hours to respond, with a warning at 2.

The "overall" SLA timeframe is the real SLA requirement the ServiceDesk has to the customer. The levels within the overall SLA are "internal" SLA levels. These internal levels are a higher standard that the ServiceDesk holds itself to, to make sure the real SLA ("overall") is never missed.

When the internal SLA level reaches its "warn" time, an email is sent to the current assignee. Note that an email is only sent to an assignee if it is assigned to a specific user and not a group. The status remains unchanged. When the internal SLA level reaches its "late" time, the status is changed to **OUT OF TIME**. The ticket becomes assigned to Support I and Support II no matter who it was assigned to at the time it hit the "late" time. An email is not sent to an assignee because the ticket is now assigned to multiple groups of users rather than one particular user.

When a ticket reaches the overall SLA "warn" time, an email is sent to the current assignee. Note that an email is only sent to an assignee if it is assigned to a specific user and not a group. If the "late" date at the overall level is reached, chances are the ticket already auto-escalated and had notifications sent based on the internal SLAs. Therefore, no action is configured in ServiceDesk.

Customers can essentially disable SLAs by increasing the late and the warning time spans to a very large number of days if needed. This method of disabling the SLAs is recommended if your company does not use SLAs. Currently, ServiceDesk is set up for Basic SLA behavior.

Incident Management looks to a global value that is populated with the SLA status. The workflow components (such as the Dialog Workflow component), in Incident Management use the late date of the current SLA as their timeout value. If a late date is surpassed, the ticket "times out" and takes the times out path out of that component. The incident history is updated to reflect the timeout.

Incidents only auto-escalate once by default. Although you can change the number of times an incident can auto-escalate, as described later in this section.

To change SLA time spans

1. In the `SD.DataServices` project, open the Setup SLA Requirements model. Two SLA levels are identified, an Emergency SLA level and a Basic SLA level. Within each level, there is a "Add New Data Element" component. This component sets the SLA requirements time spans.
2. Open the respective **Add New Data Element** component to edit.
3. Click on the **Value** ellipses button.
4. At this level, there are two time spans. A late time span that, when exceeded, denotes the task and the subsequent SLA as late. A warn time span that, when reached, initiates a warning that the SLA deadline approaches. These values are the overall SLA values. which means that the levels of approval/action, which are within the lifespan of the entire process, are within the overall SLA time. Adjust these times as needed.
5. To change the time spans within individual SLA levels, select the respective level and click **Edit**.
6. Make adjustments to the time spans that make sense for the SLA level. Make sure that the adjustments are based on the Set the Late Time Span and Warn Time Spans set at the overall level.

To configure SLAs by customer name, location, contact, or equipment name, etc.

- In the `SD.DataServices` project, open the Setup SLA Requirements model. You want to replicate:

- The component that checks for the piece of information against which the SLA is applied.
- The Matches Rule.
- The **Add New Data Element** components (or only one, if only one track is desired).

Add the Matches Rule either before the priority level evaluation or after, depending on what is more important to evaluate first. Select the variable to compare against, then connect appropriately. The "no match" path of the component should connect to the original **Add New Data Element** component. Then set the appropriate SLA timeframes for the new SLA.

If you need several SLAs, it may make sense to create new models for each. Then use `SD.DataServices` project, Setup SLA Requirements model so it makes a call to the appropriate model. Or, use a decisioning component to handle which SLA to use.

To enable incidents to time out more than once

1. Open the `SD.IncidentManagement` project, and navigate to the Set Timeout Date model.
2. Copy and paste the **Set Date Far into the Future End** component and place it after the **Has Timed Out Before?** True False Rule component.
3. Connect the true path out of the **Has Timed Out Before?** True False Rule component to the **Add Process Message** component.
4. Connect the **Add Process Message** component to the new **End** component.

Set Business Hours & Holidays

Business hours and organization holidays can be set at three levels within Symantec Workflow:

- Globally, using the Business TimeSpan Editor tool (**Start > All Programs > Symantec > Workflow Designer > Tools > Business Timespan Editor**)
- Project-level.
- Component-level, in workflow projects.

Determine which level(s) need configuration based on your business locations and SLA policy. These levels are for one geographical location. For multiple geographic locations, Symantec recommends getting a consultant's help.

On a global level, business hours and holidays can be set by using the Business TimeSpan Editor. The Business TimeSpan Editor is one of the tools that is installed

with Workflow Solution and ServiceDesk. These global business hour settings are then picked up and used as the default settings by every new workflow and monitoring project that is created.

The project level represents the second level of business hour and holiday settings. Although initially drawn from the global settings, the business hours can be modified on project-by-project by basis, if necessary. The project level settings can be found on the project attributes screen under the **Publishing** tab and labeled "Business Time Span Config". The ability to incorporate business hours respective to individual projects may be beneficial. For example, if an organization has a department that operates through the weekend while the majority of other departments operate only during the business week. The retail industry would be a prime example.

Finally, business hours can be further customized at the component level (within workflow projects only).

On their own, the business hour settings do not affect the way a workflow project is executed. But when appropriate they may be incorporated at the component level to allow or prevent certain actions from occurring based on established business hours. For example, you may want to consider weekends and holidays when you establish timeout and escalation rules, and the Emergency track of the default SLA.

On the **Edit Value** dialog box, you can set up the proper timeout and escalation schedules for the activity. The following settings refer to the business hours to ensure proper execution:

- **Allow End Time To Fall Outside Business Hours**
- **Skip Weekends**
- **Skip Holidays**
- **Business Time Span Config Usage**

Use “Allow End Time To Fall Outside Business Hours” to ensure that a process can auto-escalate or timeout between workdays even if the critical time threshold is reached outside of normal business hours. For most businesses, this setting means that an activity can escalate or timeout overnight.

The “Skip Weekends” and “Skip Holidays” settings ensure that only business days are counted in the escalation and the timeout processes.

Finally, use the drop-down box labeled "Business Time Span Config Usage" to specify whether the component should look to the global business hour settings, the project settings, or the custom settings.

Set up “Follow the Sun”

The `SD.FollowTheSun` project is where groups to assign to an incident are defined when the incident is marked to “follow the sun.” In the primary model of this project, it is necessary to: Verify/change the default time of day evaluation (set in increments of six hours by default)

Establish the location names that would cause an incident to move for each time range (edit the **Build List of Locations to Move** Add New Data Element components).

Establish group assignment for each location (edit the **Build List of New Group Assignments** Add Items to Collection components).

Verify/change the value of the “Set New Task Duration in Hours” **Add New Data Element** component (default value is six hours).

Each of these items to configure is pointed out within the model.

Change the Frequency of the customer satisfaction Survey

In ServiceDesk , a task is assigned to the customer after the incident is resolved. The customer has the option to either reopen the issue or resolve it.

On picking the “Issue Resolved” path in the Confirm Incident Resolved form, the process hits the Random Rule component.

By default, this Random Rule component is set to 100. The setting means that the Customer Satisfaction Survey is sent after every incident is confirmed as resolved by an end user.

ServiceDesk may not always want to send a survey to a customer every time a ticket is resolved. Any process that sends out a survey form to the customer can be modified. You can modify the process in such a way that it sends out surveys only for a particular percentage of time. For example, a process can be set up to send surveys for 30% of the time. For every 10 tickets that are resolved, only three customers (assuming that 10 different customers submit the 10 tickets) get the survey. The random rule would be set to 30 in this case.

To disable the survey entirely, set the Random Rule to zero, or disable the Random Rule component and set its execution outcome to “false.”

To configure the Random Rule component

1. Open the `SD.IncidentManagement` project in Symantec Workflow.
2. In the **Projects** list on the left, click **Customer Confirm Resolution** model.

3 Double-click the **Have Customer Confirm Resolution** Dialog Workflow component to edit it.

4 Select the **Interaction Setup** tab.

5 Double-click the **Random Rule** component that follows the **Confirm Incident Resolved** Form Builder component.

6 Click on the ellipse in front of True Percentage. Type the desired constant value. Or, instead of using a constant value for the True Percentage variable, you can use process variables or a dynamic model.

You can use different rules in your process for sending out the customer survey in place of the Random Rule component as desired. For example, if the incident is of a certain type or priority, then always send the survey. You can set up this type of rule using Matches Rule or a Decision Table component.

Define Quick Incident Templates

A ServiceDesk 7 feature that speeds up the processing of incidents is Quick Incident Templates. Quick Incidents Templates are the pre-populated incident submission templates that have predefined, standard values for common issues. For example, server restarts or password resets are frequently requested in most organizations. These incidents have many values that are set the same way every time. The ServiceDesk 7 worker does not need to set all of these values manually every time a password is reset. Instead, the worker can select a Quick Incident Template for password reset. By using the Quick Incident Template all of the fields in the incident are set to the proper values. Set up as many different Quick Incidents Templates as you need. They can be modified at any time based upon the changes that occur within your environment.

Quick Incident Templates can be specific to a user, group, or organization, or shared globally. End users do not use quick incident templates, rather technicians through the “Advanced” incident submission process.

You can also create quick incident for sub-tasks.

To create a quick incident template

1 In ServiceDesk on the Service Catalog select **Submit Incident (Advanced)**.

2 Populate the form with the standard information and give it a name and description.

3 Click the **Save As Template** button.

4 Enter the template name, then decide if it's user-specific or to be shared. If it is shared, set the appropriate permissions. The next time you create an incident with the "Advanced" form, it is possible for the user(s) with permission to select the template from the "Select Template" drop-down menu.

Define E-mail Content

Email content is handled in two ways in ServiceDesk. Sometimes the content is housed in a **Send Email** component within a process. But more often than not, processes in ServiceDesk make a call to the `SD.EmailServices` application to generate an email.

E-mail templates are stored in the `SD.EmailServices` project. Think of a template as a definition of the content within an email message .

This section covers both editing directly in the **Send Email** component and in the template within the `SD.EmailServices` project.

To modify the customer confirmation email (Send Email component)

1 Open the `SD.IncidentManagement` project in Symantec Workflow.

2 In the **Projects** list on the left, click on the Customer Confirm Resolution model.

3 Double-click the **Have Customer Confirm Resolution** Dialog Workflow component to edit it.

4 Click the **Event Configuration** tab and click the ellipse next to Start Process.

5 Double-click the **Thank You Subject Merge Text** component, or the **Thank You Body Merge HTML** component.

6 On the **Configuration** tab, click the ellipse next to Merge Data.

7 In the **Advanced Text Creator** window, add, modify, or delete text as appropriate.

To customize the global header and footer for emails

1 Open the `SD.DataServices` project in Symantec Workflow.

2 Scroll down to the bottom of the models list, and open the GetEmailTemplateParts model.

3 Configure the **Build Email Header** and **Build Email Footer** components as desired. You can add a project property for a logo, then populate these components with that property to have a corporate logo appear.

To add a new email template

1 Open the `SD.EmailServices` project in Symantec Workflow.

Note that the existing templates are named according to the content and only have components for the subject line, body, and header.

2 In the **Projects** tree view on the left, right-click `SD.EmailServices` (the top-level node in the tree view) and select **New Model**.

3 In the **Create New Model** dialog box, provide the following information to name and categorize the new email template:

Name	Use the Parent model name as the prefix in the new model name. Use a naming convention that reflects the function of the template. For example, you want to add an email template to **Incident Templates**. This template lets you send an email to notify the submitter that the incident has been postponed. An appropriate name for the template might be *Incident.Postponed*. Note that you can always rename the template. Right-click the new template and select **Rename Model**.
Parent	In the **Parent** drop-down list, select the Parent model as the respective project. For example, you want *Incident.Postponed* to appear in the **Incident Templates** branch of the **Projects** tree view. Select **Incident Templates** in the drop-down list.

4 When you are satisfied with the name and the Parent category, click **OK**.

5 To add the subject line, body, and header components to the new template use one of the following methods:

Copy and paste	■ Copy and paste the subject line, body, and header components from an existing template. ■ Configure the template components: Subject line, body, and header.
Manually add **Merge Text** components	■ Add a **Merge Text** component for the subject line and configure the component. ■ Add a **Merge HTML** component for the body of the email and configure the component. ■ Add a **Merge Text** component for the head and configure the component.

To modify an email template

1. Within the `SD.EmailServices` project in Symantec Workflow, review the subject, body, and header for the existing emails sent. Particularly pay attention to the ones interfacing with end users.
2. Modify text as needed, in addition to adding variables to include more data if needed.

About How the E-mail Templates are Selected in ServiceDesk

When the emails service is required, the email services application either automatically uses a template based on the parameters that are passed, or it proceeds in a generic fashion that makes it possible for the technician to select a template.

Email services first looks for process ID and tracking ID variables and if either of those are found, it acquires the corresponding data. The templates made available are specific to the type of project that corresponds with the process ID. For example, if the process ID is IM-000001, then the list of templates is from Incident Management.

If no process ID or tracking ID variables are found, the service presents the user with an email form that requires manual population of data.

Customize E-mail Monitoring

ServiceDesk 7 can accept new incidents or updates to current incidents through the inbound email interface. The email process is found in the `SD.Email.Monitor` project. The email address, user name, password, email type, and server information is all set up during the installation process. (Changes can be made however from the **Admin > Data > Application Properties**).

Brief Overview of How it Works & Ideas for Customization

The `SD.Email.Monitor` process allows for anyone to send in an incident using a standard email. If the subject line includes the words “New Incident” or “New Ticket,” the email monitoring process automatically creates a new incident. Then it sends the mailer a return email that an incident was created. You can add additional words to look for that would qualify the creation of a new ticket, or additional rules.

You can also set up monitoring to look for strange characters to do additional spam filtering if unwanted emails make it into the ServiceDesk Inbox.

To set up additional words acceptable as subject text

1. Open the `SD.Email.Monitor` project in Symantec Workflow.
2. Click on the ProcessMessage model in the Project tree.
3. Double-click the **Is New Incident Request?** Embedded Model component.
4. Copy and paste the existing **Looking for New Incident:** Text Contains Rule component. This component follows the "does not contain" output path of the **Looking for New Ticket:** Text Contains Rule component.
5. Connect the "contains" path to the **New Incident** End component.
6. Connect the "does not contain" path to the **Not New Incident** End component.
7. You can also change the existing "New Ticket" and "New Incident" text as desired.

If the email does not contain the words "New Incident" in the subject line, a task is created for the Service Managers. The Service Manager must review the data and classify it as either an incident, problem, change, or knowledge base request. Note that the task is created in the `SD.Email.InboundManagement` project. Therefore, the assignee for this task can be customized in the `SD.Email.InboundManagement` project.

The system identifies the user based on the "From" address. If the user is not listed as a contact, it can be automatically added and an incident created based upon the information the email contains. The email subject line becomes the title for the incident, and default values, such as queue, status, urgency and the like are assigned.

You can use an incident rule to parse the body of the message to look for specific words or phrases: "windows," Word, Excel, printer, corporate headquarters, etc. If specific words or phrases are identified, then specific ticket types or field values can be set within the incident.

The Email process relies on an automatically-generated reply code to link email correspondence to an incident. Email correspondence becomes a part of the incident history; it is not necessary for a technician to check an Inbox. If a reply code is deleted, the Service Manager by default receives a task to review the email. The Service Manager can associate the email to an existing ticket.

Processing Large Amounts of E-mail

The `SD.Email.Monitoring` process allows for quick processing of emails. If you have large quantities of emails to process, it is recommended to modify the email monitoring process and change it to a Windows Service.

To set up email monitoring as a Windows Service

1. Open the `SD.Email.Monitor` process in Symantec Workflow.
2. Click on the main model in the Project tree.
3. Click on the **Publishing** tab, and change the deployment type under Deployment to Windows Service.
4. Publish the project as an Installer.
5. Copy the installer file to the server.
6. Execute the installer.

Implement Multiple Mailbox Monitoring

The `SD.Email.Monitor` project is set up to watch or monitor a single mailbox for inbound email. The process can be modified should your organization use multiple mailboxes that each serve a particular role or function for email collection.

The easiest way to implement multiple mailbox monitoring, however, is to set routing up on the mail server-side so emails go to the monitored inbox. But if you want to do it using Symantec Workflow, follow the instructions in this section.

To set up a second email box to monitor (high-level steps)

1. Open the **SD.Email.Monitor** project in Symantec Workflow.
2. Update each mail component to reflect the additional inbox and mail server.
3. Publish the new process, but rename the virtual directory. For example, SD.Email.Monitoring.Server2.

Modify the Time span for end users to Confirm Incident Resolution

By default, end users are given two days to provide confirmation of incident resolution. Confirmation means either answering that the incident is resolved satisfactorily, or reopening the incident. The incident remains at 90% complete and therefore remains open until it is resolved with end-user satisfaction. The two-day duration can be modified.

To modify the time span for incident resolution

1. Open the `SD.IncidentManagement` project in Symantec Workflow.
2. In the **Projects** list on the left, click on the Customer Confirm Resolution model.

3 Double-click the **Have Customer Confirm Resolution** Dialog Workflow component to edit it.

4 Click on the **Event Configuration** tab, and scroll to the Timeout Configuration section at the bottom.

5 Click the ellipse next to Timeout Time Span.

6 Change the value from two days to the desired duration.

Establish Change Management Groups

If Change Management is to be used, the user groups that are associated with it such as the CAB, need to be defined in ServiceDesk. Modify the default groups to include the appropriate individuals responsible for making the change. Modifications to the default group are done from **Admin > Users > Accounts > List Groups**. Create change groups as needed and add the respective users. Be sure to name the groups that are prefixed with "Change-" otherwise the change templates cannot pull in that group. For example, name the group `Change Team-Norfolk`.

Note: If the new groups do not show up in the respective form in ServiceDesk, restart IIS.

Change Risk Assessment Participation for Change Management

By default, 100% of participants at each step in the ITIL change type must participate and approve in order for a change to occur. You can modify the number of participants that are needed for a change to proceed. You can allow the change to proceed after one person approves, after a specific user name approves, or after a majority approves. This example shows how to modify the process so it proceeds after one member of the CAB provides risk assessment.

To modify the risk assessment task so when one risk assessor completes the task, the Change process moves forward

1 Open the `SD.ChangeManagement` project.

2 Go to the **Risk Assessment** model.

3 Zoom out to find the **Risk and Impact Assessment** Dialog Workflow component.

4 Change the connection from the **10% Risk Assessment** component so it connects to the **Risk and Impact Assessment** Dialog Workflow component, rather than the **Iterate Risk Assessors** component.

5 Instead of deleting the **Iterate Risk Assessors** and the **Loop Back** components, opt to disable them as follows:

- Double-click the **Iterate Risk Assessors** component.
- From the **Settings** tab, clear Is Enabled and select finished as the Execution Outcome. The finished path must connect to the **Wait for All Workflow Components (Merge)** component.
- Click **OK**.
- Double-click the **Loop Back** component.
- From the **Settings** tab, clear Is Enabled.
- Click **OK**.

6 Double-click the **Risk and Impact Assessment** Dialog Workflow component. Configure as follows:

- From the **Assignments** tab, click the Person Assignments field Browse button.
  - Click AllParticipantsRow.EmailAddress and click **Remove**.
  - Click **Add > From Process**.
  - Click **Pick Array**.
  - Select RiskAssessors[ ] > [*] > EmailAddress and click **OK**. The Variable name field shows RiskAssessors[*].EmailAddress.
  - Click **OK**, then **OK** again.
- Click **OK** to close the Variable Assignments screen.
- Click the **Interaction Setup** tab.
- Click the Dialog Model field **Browse** button.
  - Scroll right and double-click the **Rename Risk Assessment Doc File Name** component. This component is a renamed **Merge Text** component).
  - Click the Merge Data field **Browse** button.
  - Click AllParticipantsRow.ParticipantName and press the **Delete** key.
  - From the **Data** tab on the left, expand EnsembleSecurityToken and then select **Name**.

- Drag and drop EnsembleSecurityToken.Name in the previous location of AllParticipantsRow.ParticipantName.
- Click **OK**, then **OK** again.

- Click **OK** to close the **Edit Embedded Decision Model** screen.
- Click **OK** to close the **Risk and Impact Assessment Editor**.

7 Double-click the **Wait for All Workflow Components (Merge)** component. Configure as follows:

- Click the Data Merge Model field **Browse** button.
- Right-click the **Merge Impact Risk Assessment Merge Data** component and select **Copy**.
- Click **OK** to close the submodel.
- Click the **Settings** tab.
- At the bottom, clear Is Enabled and select done as the Execution Outcome.
- Click **OK**.

8 Right-click the bottom of the Designer screen and select **Paste** to paste the copied **Merge Impact Risk Assessment Merge Data** component.

9 Connect the copied **Merge Impact Risk Assessment Merge Data** component to the **End** component.

10 Connect the timed out path of the **Risk and Impact Assessment Dialog Workflow** component to the copied **Merge Impact Risk Assessment Merge Data** component.

11 Connect the **Add Process Message** component (the one following the default output path from the **Risk and Impact Assessment Dialog Workflow** component) at the bottom of the **Designer** screen , to the copied **Merge Impact Risk Assessment Merge Data** component.

12 Double-click the copied **Merge Impact Risk Assessment Merge Data** component. Configure as follows:

- Click the Merge Data field **Browse** button.
- Delete the AllParticipantsRow.ParticipantName data from the editor screen.
- From the **Data** tab on the left, expand EnsembleSecurityToken and then select **Name**.
- Drag and drop EnsembleSecurityToken.Name in the previous location of AllParticipantsRow.ParticipantName.

- Delete the piece of previous data for the risk score.
- From the **Data** tab on the left, drag RiskScore and drop in the location of the previous risk score.
- Delete the piece of previous data for the risk assessment.
- From the **Data** tab on the left, drag ImpactAndRiskAssessment and drop it in the location of the previous risk assessment.
- Click **OK**, then **OK** again.

13 Click **Save**.

Verify Problem Categories

You learned that you can update Incident resolution codes without ramification. You can do the same with problem categories. The default categories are:

- Add - Install.
- Break - Fix.
- Request.

To change problem categories

1 Open the `SD.ProblemManagement` project.

2 Go to the **Problem Analysis model > Problem Analysis Dialog Workflow** component > **Interaction Setup > Dialog Model > Verify Problem Form Builder** component.

3 Double-click the drop-down list component that houses the categories.

4 Update the list of values as desired.

Chapter 4

Phase 3: Advanced Customization

This chapter includes the following topics:

Extend Data/Profiles

About SD.Data

The integration library `SD.Data` exposes data types in ServiceDesk that are meant to be modified. This library is meant to be used particularly for the introduction of new data. The core library houses the core data types in ServiceDesk. This core library is intentionally inaccessible by users for protection purposes. Therefore Symantec exposed `SD.Data` for users to change without jeopardizing the core data types, thus protecting the integrity and functionality of ServiceDesk.

Extend the ServiceDesk Incident Data Type

The ServiceDesk Incident data type is the central unifying element within Incident Management. This data type is predefined to include properties relative to working incidents: name, description, closure code, affect, SLA, etc. Your organization may require the inclusion of specific properties to better refine how your incidents are handled.

Add Cost Center to Incident Data Type

This example demonstrates the addition of the data “cost center” to the Incident data type. The addition of the data cost center lets technicians enter a cost center value upon creating an incident. First the data is created, then the form for submitting an incident are modified to collect the cost center. Note that Cost Center is used arbitrarily as an example. Because Cost Center is a value in Notification Server , it is likely true cost center would come from that source.

To add cost center to the incident data type

1. In Symantec Workflow, open the `SD.Data` integration library.
2. Select the **Advanced** option at the bottom of the window then **Edit Advanced Settings**.
3. Select **Edit Included Assemblies**.
4. Browse the Included Assemblies path and insure that the following path has been selected, (for the respective disk drive): `C:\Program Files (x86)\Altiris\Workflow Designer\WorkflowProjects\SD.Data\libs`.
5. Select `SD.DataTypesCore.dll`, Select **Open**, then **OK**.
6. Select **OK** to exit the **Dynamic Type Editor** Form.
7. Return to the SD.Data section of the Integration **Library** screen and click on **Adjust Definitions**.

8 In the **Generators Management** window, expand Generators then double-click **SD.Data**. The **Generate Components** wizard opens.

9 Highlight **ServiceDesk Incident** and click on **Add Property**.

10 The **Edit Property** window opens. Type a name for the property then select the property **Type** from the drop-down list. For example, name the property **CostCode** and set its data type to **Number** (integer).

11 Add as many new properties as needed, and then click **Next** in the wizard.

12 Click within the **Name** column for each added index, and rename the property accordingly.

13 Click **Next** on the **Indexes** screen and **Next** again to move past the **Settings** section.

14 In the Components section, click **Finish**.

15 In the **Integration Library** window, click **Recompile** and **Close**.

The new attribute of the Incident data type should now be available. It may be necessary to reload any open projects if the data type does not show up.

Add Cost Center to Incident Form

To add a cost center field to the Submit Incident (Advanced) form

1 In Symantec Workflow, open the `SD.Feeder.GeneralIncidentSubmitForm` project.

2 If you recently added the new attribute, a prompt appears asking you to overwrite the local library with the server version. Leave the check boxes unchecked to keep the local library. Click **OK**.

3 Right-click the **Create New Incident** Form Builder component and select **Web Form Editor**.

4 Resize the text box for the incident description to make room for the new field.

5 From the **Variables** pane in the lower left, expand Incident and scroll down to find **CostCode**.

6 Drag **CostCode** to the space made available in the form.

7 Choose the most suitable builder option, which in this example is **InputBuilder** (Decimal).

8 Click on **Next**.

9 Choose the appropriate output paths. In this example, make the **CostCode** value optional for users choosing **Continue** and ignore it for everything else.

10 Double-click the **Cost Code** label to edit it, then click **OK**.

11 Resize and reposition the field if necessary.

12 Click **OK** to close the form editor.

Using Custom Data in Reporting

Custom data appears as an available field in reporting only after that piece of data has been used (i.e., populated) once.

Use Custom Data in Process View Page

This step is necessary if you want users to be able to show a new custom value in the **Process View** page.

To enable users to display custom data on a Process View Page

1 Log in to ServiceDesk as the administrator.

2 Go to the **Admin tab > Data > Lists/Profiles**.

3 For Incident Management, select **Edit Profile Definition**.

4 Place a checkmark next to the new field.

Note: SQL likely renamed the new field based on uppercase letters to lower-case.

---

5 Click on **Generate**.

Extend the CustomerServiceSurvey Data Type

You can modify the Customer Satisfaction Survey to reflect what is important to the organization.

ServiceDesk has a data type for the Customer Satisfaction Survey , called CustomerSerivceSurvey. This data type also resides in the `SD.Data` integration library. If you want to add a question to the survey, it is required to add the attribute for that question to the CustomerServiceSurvey data type.

Then, add a field for the new attribute in the survey itself. The survey is found in the `SD.CustomerServiceSurvey` project, in the **Customer Service Survey Main Form** Form Builder component.

One idea for customization is to add comment fields for each question, rather than having one general comments field at the end of the survey. For example,

capture a specific comment for a specific question if the rating for that question is less than 3.

Extend the ServiceDesk Problem Data Type

Modifications in the ProblemTicket Data Type

A data type can be thought of as a constraint that is placed upon the interpretation of data in a process. ProblemTicket data type is the data type we associate with any problem in the Problem Management process. The data type is associated with properties such as title, urgency, description, SLA, etc. These properties move around in the process with the data type.

Add new attributes as needed to the ProblemTicket data type in the **SD.Data** project.

Add & Customize Pages

Pages in ServiceDesk can be added as needed to make additional data available to users. Also, pages can be customized. The goal is to make information available and presented in a way that makes handling tickets quick and effective. Examples of customization include:

- Adding new web parts to pages.
- Reorganizing existing web parts.
- Creating Process View pages for handling incidents (for example, a different **Process View** page for a change ticket vs. a ticket in Incident Management).

Pages are created under **Admin > Portal > Manage Pages**.

Users with page customization permission can edit their pages from the **Site Actions** menu. Administrators can edit pages from the **Admin > Portal > Manage Pages** page.

The ServiceDesk contains over a hundred Web parts many of them are categorized under **Admin > Portal > Web Parts Catalog**. Additional Web parts are available by clicking the **Add** icon on that page and making a selection from the **Class Name** drop-down menu. That is the full list of Web parts available.

Plugins can be added in ServiceDesk as well under **Admin > Portal > Plugin Upload**.

Modify Types of Changes

Within the Change Management main model, SD.ChangeManagement, a form provides the type of change for a proposed change request. If your organization only uses a few of the change types, you may want to modify the **Type of Change**

form and outgoing paths. The default types of changes available are: ITIL, Moderate, Simple, and Emergency.

You have two options. You can delete the components for the one(s) you don't want, or you can have the component always use one change type.

To remove types of changes

1. In Symantec Workflow, open the `SD.ChangeManagement` project.
2. In the Change Management Main model, double-click the **CM (Gatekeeper)** Dialog Workflow component.
3. On the **Interaction Setup** tab, open the **Dialog Model**.
4. Double-click the **Type of Change** Form Builder component.
5. In the **Web Form Editor**, select the specific components to remove then click **Delete**.
6. Click **OK** to close the form when editing is complete.
7. Immediately following the **Type of Change** Form Builder component are Add New Data Type components for each change type. Note the Add New Data Type component with the validation break (since its type of change was removed).
8. Delete the errant component. If it is possible you may need the component, double-click the component. Then go to its **Settings** tab, and uncheck the **Is Enabled** checkbox.
9. Delete the change type option from the **Matches Rule**.

Note: You may want to remove the entire change type section from the embedded decision model. However, if you do not remove the related components but do delete the initial entry into the path, the process does not migrate to that area of the workflow.

To enforce one type of change

1. In Symantec Workflow, open the `SD.ChangeManagement` project.
2. In the Change Management Main model, double-click the **CM (Gatekeeper)** Dialog Workflow component.
3. On the **Interaction Setup** tab, open the **Dialog Model**.
4. Right-click the **Type of Change** Form Builder component and select **Edit Component**.
5. Click on the **Settings** tab.

6 Uncheck the **Is Enabled** checkbox.

7 From the **Execution Outcome** drop-down menu that appears, select the desired change type. Now the component always uses this type of change as its outcome, as if the user selected it.

8 Click **OK** to close the component. The component appears inactive. However it functions by setting the execution outcome therefore causing the process to follow the respective path.

Define Smart Tasks

Smart Tasks are the tools that ServiceDesk 7 workers can use to help work a ticket. These tools can execute a program, invoke a web service, trigger a task server job, or call a Web page , for example. Here are some examples of ways to use Smart Tasks:

- Run the resource association diagram to see how the computers are logically set up.
- Show a list of in-stock computers.
- List all the incidents that are associated with a specific asset.
- Send a request for approval.
- Search the Altiris Knowledgebase Web site .

Add Smart Tasks to the Initial Diagnosis Dialog Workflow

Create smart tasks for the actions that are performed often. You can add as many smart tasks as needed to Incident Management. Conceivably, each smart task expands your ability to work an incident.

This example creates a smart task for automatically searching the Altiris Knowledgebase using the ticket's description.

To create a smart task for searching the Altiris Knowledgebase Web site

1 In Symantec Workflow, open the `SD.IncidentManagement` project.

2 Within the Main Incident Work model, double-click the **Diagnose and Work Incident** Linked Model component.

3 Double-click the **Initial Diagnosis** Dialog Workflow component.

4 Select the **Interaction Setup** tab. The existing smart tasks are listed as dialog models.

5 Click **Add**.

6. From the **Setup** tab, set the Category as **Tools** and provide a name for the new smart task. In this example, the name is "Search Altiris KB."
7. Open the **Dialog Model**, which is where the process itself is configured.
8. Add a **Merge Text** component to the new dialog model and double-click the component to edit it.
9. Open the Merge Data model. It is easiest to paste in the URL of the Altiris KB rather than type it, therefore go to the Altiris KB site: `http://kb.altiris.com`. (Leave the Merge Text component open.)
10. Do a search. For example, type "test" in the **Search Terms** field then click on **Search**.
11. On the right, under **Last Searches**, right-click the "test" link and copy the URL to the clipboard.
12. Back in Symantec Workflow, in the **Advanced Text Creator** window of the **Merge Text** component, paste or type the URL of the site.
13. Where the URL has "test," delete "test" and add the variable for incident name. Drag and drop the Incident.IncidentName variable from the **Data** tab on the left into its respective position within the string.
14. Click **OK** and provide an output variable name. For this example, we use "AltirisKBURL."
15. Click **OK**, and back in the **Decision Model** editor, add a **Terminate and Transfer** Dialog Flow component.
16. Double-click the component, and in the URL field, select **Process Variables**, then **Add**.
17. Select the output variable name that you created in the **Merge Data** component, in this example, **AltirisKBURL**. Click **OK**.
18. Connect all of the components together.
19. Click **OK** three times to exit the component editors. The new smart task will be applied the next time you deploy the process.

Note: Smart tasks may or may not complete the task to which they are associated. If the checkbox **Resolve Workflow Task on Exit** is selected, the smart task resolves the task. If the checkbox is left unchecked, the smart task can be run as many times and the task remains unresolved.

You can configure smart tasks to appear conditionally, so they only appear when appropriate. This example demonstrates how to configure the "Search Altiris KB" smart task so it only appears when the ticket name contains the word "Altiris."

Additionally, a date range can be specified for making the smart task available by using the "Date Validity" setting for the smart task.

To enable smart tasks to appear conditionally

1. In Symantec Workflow, open the `SD.IncidentManagement` project.
2. Within the Main Incident Work model, double-click the **Diagnose and Work Incident** Linked Model component.
3. Double-click the **Initial Diagnosis** Dialog Workflow component.
4. Select the **Interaction Setup** tab.
5. Click on the **Search Altiris KB** smart task and click on **Edit**.
6. From the Setup tab, check the **Conditionally Use** checkbox.
7. Open the Conditional Use Model. For this model, only the **Text Contains Rule** component is needed to evaluate the incident name for the word "Altiris."
8. Add a **Text Contains Rule** component to the model.
9. Since the **Text Contains Rule** component has two outcomes, another **End** component is needed. Add an **End** component.
10. Connect the components accordingly.
11. Double-click the **Text Contains Rule** component and in the **Contains** field, select **Constant Value**, and in the value field type "Altiris." Click **OK**.
12. In the **Variable Name** field, select the variable Incident.IncidentName. Click **OK**.
13. Click **OK** to close the **Text Contains Rule** editor.
14. Double-click the **End** component that connects to the "Contains" output path.
15. Open its Mapping field, select **Create Value**, and set the value to "true" by checking the **Value** checkbox.
16. In the other **End** component, open its Mapping field, and select **Create Value**, but leave the **Value** checkbox unchecked.
17. Click **OK** to close.

Add to the Service Catalog

Incident Management is intended for break/fix-type of issues. The Service Catalog is intended for managing processes: HR onboarding, password reset, equipment requests, things of that nature.

The Service Catalog provides a means for end users to help themselves, therefore reducing the load on IT. The processes that are added perform consistently and can be reported against using the built-in reporting capability in ServiceDesk.

Adding to the Service Catalog requires the new process be built in Symantec Workflow, then added to the "menu" found in the ServiceCatalogCategoryInfo integration library. Examples of process you can build are:

- An automated software request and approval process
  A process where the end user selects the needed software. Then the process does automatic checking of licenses and automatic approval. The final result is software is delivered and installed without IT personnel involvement.
- A reset password process
  A process that automatically goes into Active Directory and updates that user's information.

To add a process to the Service Catalog

1. Create the process in Symantec Workflow. When the process is tested and ready to publish, choose the option to **Publish to Process Manager Forms**, or **Publish to Process Manager Services**, depending on the type of project.
2. Select the catalog location and deploy. During deployment, set the permissions for the process from the **Permissions** tab. You can also set permissions for the service catalog process in the portal from the **Admin tab > Service Catalog Settings**. Select the **Service Catalog** item for which you want to set permissions, and select the **Edit Form** icon. Add users or groups from the **Permissions** tab accordingly.

Define New Reports

Several predefined reports present useful information right out of the box. However, the administrator can modify these reports or create entirely new reports in from the Reports tab in ServiceDesk.

Reports are also used to filter the task list for a user.

Create a Standard Report

This example creates a standard report that lists all resolved incidents by the Respond Type. Additionally, it demonstrates the primary contact, phone number, email, priority, and description of the incident.

To create a new report based off an existing report

1. Go to the **Reports** tab and select **Incident Management** from the **Report Categories**.
2. Select the **plus** icon and select **Add Standard Report**.
3. Add a name to your report: List Resolved Incidents by Respond Type.
4. The left pane of the report design screen is the **Data List**. The **Data List** represents data available to include in the report. As you select data items, the table displays on the right-hand pane under **Columns**. Under the **Data List** select the following options:
   - **Process Management - Add Processes to Report**
   - **Process Management - Include Process Actions**
   - **Process Management - Not Completed**
   - **Incident Management - Add Incident Management to Report**
   - **Incident Management - Add Custom Incident Data** (leave additional filter criteria blank by clicking **OK**)
   - **Incident Management - Add Custom Incident Data** (leave additional filter criteria blank by selecting **OK**)
   - **Process Contacts - Add Process Contacts to Report**
   - **Process Contacts - Primary Contact** (leave additional filter blank by selecting **OK**)
   - **User - Add Users to Report**
5. From the **Columns List** (right pane), select the following columns to display on your report:
   - **User Table - First Name**
   - **User Table - Last Name**
   - **User Table - Primary Email**
   - **Process - Status**
   - **Incident - Description**
   - **Incident - ID**
   - **Incident - Priority**
6. The middle pane is intended to show a preview of returned data, not all of the data that the report returns.

7 Adjust your report by using the arrows on the columns that are displayed in middle pane. Or Adjust your report by using the arrows next to the column labels in the column list on the right pane. You can also adjust the column width by using the sliding width function on the column.

8 Use the **Options** tab on the **Data** list to further customize your report. Select **Group By = Respond Type** (if available in your image otherwise select **Priority**) and **Sort By= Priority**.

9 Select the **Description** tab and create a description for your report: A list of all the resolved incidents listed by respond type.

10 Select the **Permissions** tab and select the **Add New Permissions** button.

11 Search for and add Support I as a group that can view and edit this report.

12 Generate the report.

13 To make this report a chart rather than a graph, select the **Chart** option in the middle pane. From here you can select what type of chart you want to use along with other attributes. The view last selected for the report, chart, or grid, is the view for the report when run in ServiceDesk.

14 Save the report.

15 Check your report by making sure that you have some resolved incidents. Log in as a Support 1 user (technician1 or technician2) and check your report.

About Creating a Child Report

Child reports are important for permissions and performance reasons. Child reports do not change the original report definition. The user that designs the report can only add data. Since data cannot be removed, the report always contains the data that the administrator intends the user to see. Child reports inherit the data and security of the parent report.

It is recommended to create child reports for users. The **Add Child Report** is available from the **Actions** menu (orange lightning-bolt) for the particular report.

Configure Automatic Generation of Reports

You can configure reports to be written to a file or emailed automatically by defining a reporting schedule.

To set up a reports schedule

1 In ServiceDesk, click **Admin > Reports > Reports Schedule List**.

2 On the right side of the **Report Schedule List** page, click the Add button.

3 Set up the schedule as desired and click Save.

4 On the schedule's actions (lightning-bolt) icon, click **Reports**.

5 Click **Add Report** and select the reports(s) to include.

6 Select or enter the following information:

- Select the user to run the reports, if necessary.
- Select the destination type (file or email).
- Enter the recipients email address.
  Separate multiple address using a semicolon.
- Select the output format.
- Name the report, as desired.

7 Click **Add**.

8 Next, it is necessary to enable the report for programmatic access, which creates a Web service for the report. For each report you want automatically generated, you must generate a Web service for it.

See "Making a Report a Web Service" on page 67.

Making a Report a Web Service

Every report in ServiceDesk has the ability to become a web service. The report is accessible like any other ServiceDesk process that is deployed as a Web service. Follow these instructions if you want to expose report data so a Web service can call it.

To generate a web service for a report

1 From the **Reports** tab, select **Edit Report Definition** from the **Actions** menu for the particular report.

2 At the top of the **Designer** screen, click on **Web Services**.

3 Check the **Enable for Programmatic Access** checkbox, and populate the web service information fields.

4 Click on **Generate**.

Replicating ServiceDesk Data

The replication schedule tells ServiceDesk how often to either move or copy certain data to either a file or a database. You can set up as many schedules as needed to

handle data. You can set up replication at any time (does not have to be upon initial implementation of ServiceDesk).

To set up data replication

1. In ServiceDesk, go to Admin > Reports > Replication Schedule List.
2. Click the **Add New Replication Schedule** icon.
3. Set up the schedule as desired.

Create a New Schedule

Schedules are used to record various ServiceDesk activities (primarily scheduled releases and scheduled changes). The core processes for Change Management and Release Management directly update the schedule/calendar visible under **Knowledge Base > Schedules**.

An administrator can create a new schedule and allow users to add entries to track events entirely separate from the default schedule. You can also call the new schedule directly from a process.

To create a new schedule

1. In ServiceDesk, go to the **Knowledge Base > Schedules** page.
2. In the **Schedule** pane on the left, click on the **Add Schedule** icon. Note the icon does not appear unless the user has permission.
3. Enter a name for the new schedule. If you want, select a color for scheduled items. For example, enter the name “Training Class Schedule.”
4. Select **Permissions > Add Permissions** to set the criteria for schedule accessibility.
5. Click on **Save**. The new schedule appears in the **Schedules** pane.
6. Select the check boxes for the schedules you want to make visible in the calendar.

To call the schedule from a process and add an entry

1. You can add entries to any schedule from within a process using the **AddScheduleEntry** component. Open a ServiceDesk project in Symantec Workflow through which an entry to the schedule can be justifiably created. For example, a smart task that accesses a form to sign up users for training. The form UI feeds the **AddScheduleEntry** component its data, then that component makes the connection to the calendar and creates the entry.
2. Add an **AddScheduleEntry** component to the appropriate model and make the necessary connections.

3 Double-click the **AddScheduleEntry** component.

4 On the **Inputs** tab, set the **Service URL Source** field to **Use Default**. This source field uses the source location to which the process is deployed.

5 For the **Scheduled Source**, select **From Picker**.

6 For **Schedule**, browse and select the appropriate schedule from the **ScheduleEditorForm** list. The entry inherits the appearance and the permissions of the selected schedule.

7 Populate the Schedule Entry Title, Start Date, End Date, Description, Pop-Up Description, and Item Color fields.

8 Enter a name for the output variable on the **Outputs** tab.

Adding & Removing E-mail Notification

Several email notifications are set up throughout Incident, Change, Problem, and Release Management, and the Knowledge Base process. You can add and remove these as needed. You can use the following methods for adding notifications:

- Use the **Terminate and Transfer Dialog Flow** component to call SD.EmailServices
- Use the **Merge Text and HTTP Post** components to call SD.EmailServices.
- Use the **Send Email** component within the process.
- Create a custom **Web Service Caller** component to call SD.EmailServices. Note that this method requires an upgraded version of Symantec Workflow.

The recommended method for notifications is by calling SD.EmailServices. This way the behavior and appearance is consistent. The link to SD.EmailServices uses variables to provide the “Create Email URL,” process ID, workflow tracking ID, and mail to. Recommended input parameters are: process ID, tracking ID, mail to, template, and an autosend value.

Here is an example of a URL calling SD.EmailServices, which can populate a **Terminate and Transfer** component:

```
[ProfileProperties].service_desk_settings_create_email_url?processid=[Global].
ReportProcessID&trackingID=workflowTrackingId&Mailto=MailTo&InputTemplate=Autosend.
Incident.StartChat&Autosend=True.
```

This string specifies the template name in SD.EmailServices, which is “Autosend.Incident.StartChat.” If you open SD.EmailServices, and look at that model, you see that it contains the email content for inviting a participant to chat.

Disabling a notification is similar to disabling the component that calls SD.EmailServices or disabling the **Send Email** component generating the unwanted notification. Every component has an **Is Enabled** setting that can be disabled to cause the component to become inactive. It is recommended to disable components rather than remove them, in case they are wanted in the future.

Application property for Two Notifications

Two settings in ServiceDesk enable the notifications for incident creation (SendNotificationIncidentCreation) and incident resolution (SendNotificationIncidentResolution). You can disable these notifications by changing the application property for these to False.

Remove an Approval Step

In ServiceDesk, many approvals happen by the **Dialog Workflow** component which presents a user a form to either approve or deny something. For example, there is an approval step for deleting a knowledge base item. You can bypass this approval step by disabling the component that handles the approval.

In general, Symantec recommends disabling unwanted components rather than deleting them. This example shows disabling the **Dialog Workflow** component; the method for disabling is the same for other components as well.

To disable the approval step for removing a knowledge base article

1. In Symantec Workflow, open the `SD.KBSubmission` project.
2. Click on the Removal Approval model in the Project tree on the left.
3. Double-click the **Review Removal Request** Dialog Workflow component.
4. Click on the **Settings** tab.
5. At the bottom, uncheck **Is Enabled** and select **Approved** as the Execution Outcome. Now any time a knowledge base article is to be removed, the removal step always returns “true” as if approval was granted. User interaction is not needed.

Customize the Spell Checking Dictionary

User input in ServiceDesk is validated for spelling typically by a **SpellCheck** component. The component is not visible to the end user, however it creates red underlining for misspelled words. By right-clicking the misspelled word, a list of spelling suggestions appears. Selecting a suggestion corrects the misspelling.

A **SpellCheckButton** component appears as a button in the form. It is often displayed as a **Check Spelling** button. The component targets a specific component (for example, a text box). After you enter information into the form and click this button, a standard spell check dialog window opens. The user can then ignore or change the words that are called out as misspelled.

Symantec Workflow uses "KaramaSoft's Ultimate Spell" technology for these two components. A custom dictionary can be added to Ultimate Spell, but only through altering the directory of the web application in ASP.NET. Therefore another option is to have users edit the spell checking dictionary used by their browser, such as the Google toolbar spell-checking tool.

The spell check tool in the Google toolbar appears as a green checkmark. Once you enter information into any Web form , you can click the **Spell Check** button and form data that is entered is assessed. To add misspelled words to the dictionary, right-click the word and then select **Add to Dictionary**.

To configure the Google dictionary

1. Click **Start > Run**.
2. In the **Run** window, type notepad `%HOMEPATH%\Application Data\Google\User Dictionary.txt`, and click **OK**.

   If it doesn't work, browse to the directory. For example, browse to `C:\Documents and Settings\[user name]\Application Data\Google`. `Application Data` is a hidden folder by default. It may be necessary to make it visible by going to **Tools > Folder Options > View > Advanced Settings > Files and Folders > Hidden Files and Folders** and select **show hidden files and folders**.
3. The dictionary opens as a text file in Notepad. The words that are added to the dictionary display, and you can modify as needed.

Create Incidents from Other Sources

Notification Server

Incidents can be created from within Notification Server directly from an item by right-clicking the item and selecting the **Create Incident in ServiceDesk** option. Doing so launches a **Create New Incident** form that is tailored to Notification Server.

To enable this functionality, it is necessary to manually install the **SD.Feeder.CreateIncidentForAssetInNS** package and deploy it to the production server.

To install the SD.Feeder.CreateIncidentForAssetInNS package

1. In Symantec Workflow, click the **Add** button and browse to the list of ServiceDesk project packages.
2. Open the package for **SD.Feeder.CreateIncidentForAssetInNS**.
3. Deploy the project using the same deployment procedure as for other ServiceDesk projects to introduce this functionality.

Other Systems

The integration library SD.Data shows all the attributes of the Incident Management data type. As long as a system can make the Web service call to Incident Management and provide at a minimum the required data to make an incident, it is possible to create incidents by other access points to ServiceDesk.

Integrate ServiceDesk 7 with Other Systems

Using the Integration Library, you can generate custom components to integrate with databases and Web services. The Integration Library is a powerful option for extending the capability of ServiceDesk. For example, you can create a SoftwarePackagesLibrary SQL table component to read the inventory list of software to incorporate into a **Request Software** Service Catalog process.

Note: The creation of a SoftwarePackagesLibrary SQL table component requires a full Symantec Workflow license.

The Integration Library capabilities provide many ways to take advantage of your existing data sources..

Creating a Web part

These example instructions create a new custom Web part to add to a dashboard in ServiceDesk.

See "Adding a custom Web part to a Process Manager portal page" on page 74.

The Web part is created in a Web forms project in Symantec Workflow. The Web part is a stoplight that reads in a random number and based on the number, shows either red, yellow, or green.

To create a new Web part (example)

1. Create a new Web forms project. Name it indicative of what the Web part should do. For example, `MyCompany.Dashboard.StopLight`
2. Add an Add **New Data Element** component and configure as follows:
   - Data Type - Number (Integer).
   - Output variable name - Counter.
3. Add a **Form Builder** component, and connect the components accordingly.
4. Open the **Form Builder** component and configure as follows:
   - When you are prompted, answer no to creating an outcome component.
   - Add a **Stoplight** component to the form and resize it as desired. Configure it as follows:
     - Image states can remain as they are by default (red, yellow, green).
     - Set the default state to red
     - Open the Image Selection model for configuration.
       - Clone the existing **End** component twice and rename them to Red, Yellow, and Green. Then open each one to select the corresponding color option based on the name of the component
       - Add a **Create Random Number** component, and connect the Start component to it. Configure the **Create Random Number** component as follows:
       - Result name - ColorDecision
       - Check **Use min and max**.
       - Min value = 1
       - Max value = 3
       - Add a **Number Range Rule** component and connect the **Create Random Rule** component to it. Configure the **Number Range Rule** component as follows:
       - Compare variable - ColorDecision (use the browse capability to pick this variable).
       - Handle Equals by - Make Explicit
       - Enter values 1, 2 and 3 in separate lines for comparison purposes.
       - Connect the "Number Range Rule" output paths in the following manner:

- Less than 1, Equals 1 and 1..2 connected to Green end component.
- Equals 2 and 2...3 connected to Yellow.
- Equals 3 and Greater than 3 connected to Red.
- Click **OK** to return to the **Stoplight** configuration dialog.
- Add an **Auto Exit Page on Timer** component to the form, and configure as follows:
- Refresh minutes = 0.
- Refresh seconds = 5.

- Click **OK** to return to the main model.

5 Add an **Add Values** component after the Form Builder, and connect the Form Builder component to the **Add Values** component. Configure as follows:

- First value = Counter (use the browse capability to pick this variable).
- Second value = 1 (constant).
- Output value = Counter (use the browse capability to pick this variable).

6 Add an **Equals Rule** component after the **Add Values** component, and connect the **Add Values** component to the **Equals Rule**. Configure the **Equals Rule** as follows:

- Data Type = Number (integer).
- Variable Name = Counter (use the browse capability to pick this variable).
- Compare to = 10.

7 Configure the output from the **Equals Rule** in the following manner:

- Not equals connected to the Form Builder.
- Equals connected to the **End** Component

Adding a custom Web part to a Process Manager portal page

After you create a custom Web part, you can then add it to a Process Manager portal page.

See “Creating a Web part ” on page 72.

To add a custom Web part to a Process Manager portal page

1. Publish a Web form to the Process Manager portal.

   Note the category in which you published the Web form. The category is where the Web form is located in the Process Manager portal

2. Log in to the Process Manager portal.

   Make sure that you have permissions to edit the page to which you want to add the Web part.

3. After you log in to the portal, click **Admin > Service Catalog Settings**.
4. On the **Service Catalog Settings** page, in the **Browse Category** section, select the category where the form was published.
5. To the right of the Web form that you want to add, click the **Actions** symbol (orange lightning) and then click **Edit Form**.
6. On the **Service Catalog Edit Form** dialog box, on the **WebPart Information** tab, check **Is Web Part**.
7. On the **Permissions** tab, set up necessary permissions.
8. When you are finished editing the Web form, click **Save**.
9. Click **Admin > Portal > Manage Pages**.
10. On the **Manage Pages** page, select the page to which you want to add the form and then click **Go To Page**.
11. In the upper right corner of the page that you selected, click **Site Actions > Modify Page**.
12. Click **Site Actions > Add Web Part**.
13. In the **Catalog Zone** dialog box, click **Service Catalog**.
14. In the **Service Catalog** section of the dialog box, check **FormFrameWebPart**.
15. In the **Add to** drop-down list, select the zone to which you want to add the Web part, click **Add**, and then click **Close**.
16. In the upper right corner of the new Web part, click the **Actions** symbol (orange lightening) and click **Edit**.
17. In the **Editor Zone** dialog box, under **Settings**, in the **Forms** drop-down list, select the required form.
18. Edit the required settings, such as renaming the Web part, click **Apply**, and then click **OK**.

Non-Changeable Items in Symantec Workflow projects

While Symantec Workflow lets you configure components and settings to correspond with the needs of your organization, some items should be left intact. These items should be left intact to maintain the integrity of the processes.

The following areas and items should not be modified at the project level:

- **Main Project Settings** - The name and Service ID of your project settings should never be modified or removed.
- **Publishing** –The Initialization and Workflow Type settings should be left as-is. These dictate how the process launches. Altering these can cause the process to fail.
- **Reporting** – The project reporting is configured specifically for data collection by Process Viewer. Altering the settings on this tab compromises the reporting capabilities of your project.
- **Libraries** – Removing libraries from your project and in turn removes certain components and causes the process to fail.
- **Global Data** – Global data is data that is used throughout various stages of your process. Removing an item from the Global Data tab compromises the output of the process and potentially cause failure to launch and run.
- **Application Properties** – This should be left enabled to maintain the link to ServiceDesk settings within the process.

The following areas and items should not be modified at the component level:

- **Start** – Removal of this component causes the process to fail.
- **End** – Removal of this component causes the process to fail.
- **SetUp Process** – This component establishes much of the criteria that the Process Viewer uses. Deleting or editing the component compromises the reporting structure of your process.
- **Global Logging Capture** – This component turns on logging for your process. Removal of this component means that no exceptions or errors are logged when your process is run.
- **Create Log Message/Create Log Entry** – These components allow for errors and issues to be properly logged and classified.
- **Set Process State/Status** – This component is placed after dialog workflows and is intended to be used to capture data for Process Viewer. The message that is associated with this component is displayed in Process Viewer to indicate what stage the process is in and has passed. While this component can be modified, particularly if the action being recorded needs to be clarified further,

the actual status of “started”, “in progress”, or “completed” should not be altered.

- **Add Process Reference** – This component establishes the criteria that is used in Process Viewer, such as what type of business service an incident affects. Deleting or editing the component compromises the reporting structure of your process.
- **Exception Component/Exception Trigger/Exception Trigger By Component/Exception Trigger By Exception Type** – These components are necessary for logging and reporting on any exception or issue that occurs while your process runs. Removal of these compromises your reporting capabilities as well as prevent you from troubleshooting properly.
- **Add New Data Element** – This component most likely is configured so as to create a variable which is used throughout the process. Removing this component compromises the integrity of your project.