Symantec™ ServiceDesk 7.5 Implementation Guide

Symantec™ ServiceDesk 7.5 Implementation Guide

Legal Notice

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT 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 website 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

Section 1

Introducing ServiceDesk

Chapter 1

Introducing ServiceDesk

This chapter includes the following topics:

About ServiceDesk

Symantec ServiceDesk improves your infrastructure's service management.

It is ITIL-based and includes all of the primary ITIL Service Management processes. These processes include Incident Management, Problem Management, Change Management, and Knowledge Management. ServiceDesk also includes a Service Catalog that lets your users choose service items. It also includes an Active Directory Self Service Catalog that lets users easily and securely reset passwords and access network shares.

ServiceDesk uses the Symantec Workflow framework to manage service tickets, provide reports, and integrate with the Configuration Management Database (CMDB).

You can configure ServiceDesk to meet your organization's specific requirements. These configurations include setting up business hours, routing rules for incidents and changes, and email templates and notification rules.

You can implement advanced customizations. These customizations may include creating data types, modifying feeder forms, modifying the Process View page, and adding fields to reports.

For more information, see the following:

See “What you can do with ServiceDesk” on page 16.

See “Components of ServiceDesk” on page 25.

See “How ServiceDesk works” on page 18.

For videos and articles, join the Symantec sponsored ServiceDesk user group on Symantec Connect:

http://www.symantec.com/connect/groups/symantec-servicedesk

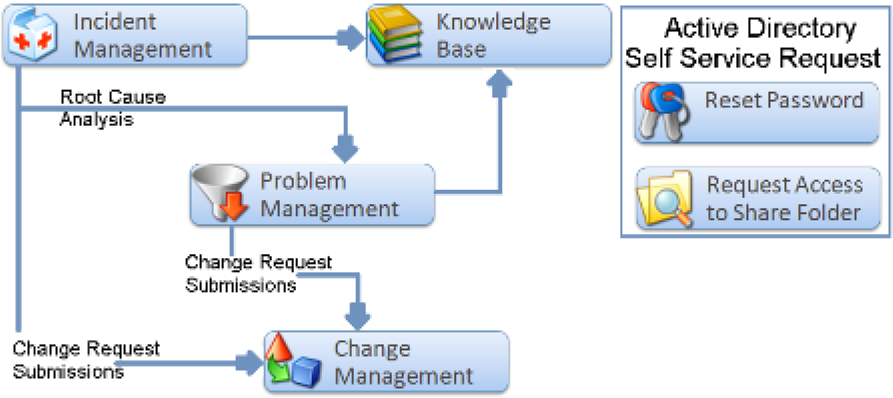
For continuous documentation updates, subscribe to the following forum on Symantec Connect:

www.symantec.com/connect/endpoint-management/

What you can do with ServiceDesk

ServiceDesk contains several predefined ITIL-based modules for managing your service environment. These modules can help you manage incidents, changes, problems, and knowledge. In addition, ServiceDesk provides a module for managing your Active Directory self-service request. When installing ServiceDesk, you can select which of the modules that you want to implement.

Figure 1-1 ServiceDesk modules


Incident Management
Knowledge Base
Active Directory Self Service Request
Root Cause Analysis
Reset Password
Problem Management
Request Access to Share Folder
Change Request Submissions
Change Request Submissions
Change Management

A ServiceDesk module is a collection of workflow processes, administrative interfaces, automation rules, and portal extensions that address a specific business need for your environment. Each ServiceDesk module represents a core process in ServiceDesk. ServiceDesk contains the following modules to help you organize and manage your service environment:

Table 1-1 Modules in ServiceDesk

Module	Description
Incident Management	■ Contains an ITIL-based Incident Management system. ■ Includes the Incident Management workflow process, a specialized **Process View** page, and a report pack. It also includes several administrative interfaces for managing related data like service queues and templates. ■ Provides a process for submitting and resolving incidents. ■ Lets the users submit incidents and lets the technical support workers respond to and resolve the incidents. ■ Includes the ability to create, assign, and manage the subtasks that are related to an incident. ■ Includes an automation library with conditions and actions for use with the Workflow Rules Engine. See "About Incident Management" on page 30.
Problem Management	■ Contains an ITIL-based Problem Management system. ■ Includes the Problem Management workflow process, request forms, and reports. ■ Provides a process for minimizing the effects of incidents and problems. ■ Lets you track and diagnose problems and publish known errors to help with future resolutions. ■ Integrates with the Incident Management and Change Management modules. See "About Problem Management" on page 31.
Change Management	■ Contains an ITIL- based Change Management system. Provides a process for standardizing the methods and procedures for handling changes in the organization to minimize the effect of those changes on services. ■ Includes the Change Management workflow process, a specialized **Process View** page, and a report pack. It also includes several administrative interfaces for managing related data like change advisory boards (CABs) and templates ■ Provides a process for standardizing the methods and procedures for handling changes in the organization to minimize the effect of those changes on services. ■ Includes the ability to create, assign, and manage the subtasks that are related to a change request. ■ Includes an automation library with conditions and actions for use with the Workflow Rules Engine. See "About Change Management" on page 32.

Table 1-1 Modules in ServiceDesk *(continued)*

Module	Description
Knowledge Base Management	■ Provides a process for managing your knowledge base, which includes gathering, analyzing, storing, and sharing knowledge and information within an organization. ■ Provides a data repository that stores information on incidents, problems, and known errors. ■ Provides an area to develop your knowledge base that is based on the information that is gathered from incidents and problem resolution. ■ Improves your efficiency by reducing the need to rediscover knowledge. ■ Enables an organization to match new incidents against previous incidents and reuse the organization-established solutions and approaches that you collect in the knowledge base. See "About Knowledge Management" on page 33.
Active Directory Self Service Catalog	■ Contains a collection of self-service request processes for interacting with an Active Directory domain. ■ Includes the service catalog items for resetting a domain password and requesting access to a network share, along with the processes to support the requests. See "About the Active Directory Self Service Catalog" on page 34.

See "About ServiceDesk" on page 15.

See "How ServiceDesk works" on page 18.

See "Components of ServiceDesk" on page 25.

How ServiceDesk works

ServiceDesk is a bundling of ITIL-based ServiceDesk core processes that run on the Workflow engine. ServiceDesk helps you manage incidents, changes, problems, knowledge, and Active Directory domains.

See "What you can do with ServiceDesk" on page 16.

ServiceDesk has several key features to help you manage your service environment.

Table 1-2 Key features of ServiceDesk

Feature	Description
Ready-to-use ITIL-based process modules	■ All ServiceDesk processes are ITIL-based, which lets you implement an ITIL solution. ■ ServiceDesk includes a set of high-quality, ITIL-based processes that have undergone extensive testing and development effort.

Table 1-2 Key features of ServiceDesk *(continued)*

Feature	Description
Process-driven forms	■ The default forms that ServiceDesk contains are process-driven rather than data-driven. ■ The user is not shown all of the available information for the form. Instead, the user is only shown what is relevant for the particular point they are at in the process. The user is only shown the information they need to see to move forward with the process. ■ This narrowing of focus helps ensure that the process is followed correctly, and makes following the processes easier for new users.
Time zone support	■ The date and time that appear in tickets, alerts, and emails are displayed in the appropriate time zone for the current user's location. ■ This time zone support allows for world-wide support capabilities and supports virtual help desks
Business hours support	■ Business hours support allows for accurate Service Level Agreement reporting and accurate reporting of average response time and resolution time. ■ Lets you define the normal business hours for your organization, which accounts for holidays and weekends.
Email templates and notifications	■ The email notifications, which automation rule sets trigger, keep users aware of changes to ticket status, and allow users to verify that issues are resolved. ■ In any process, email notifications can be used to notify the contacts that are associated with a ticket, to assign tasks, and to send alerts.
Email Monitoring	■ Email Monitoring monitors a specified inbox for all new and all unread emails. ■ Processes the emails by creating incidents or routing them to the service manager for evaluation. ■ Lets you set up an inbox for all new and all unread emails. See "About configuring the email monitoring" on page 234.
Service Level Agreement (SLA)	■ Default SLA time frames can be established and applied based on rule sets. ■ You can define the SLA time frames in ServiceDesk according to your corporate policy. See "Creating and Editing Service Level Agreements (SLAs)" on page 158.

Table 1-2 Key features of ServiceDesk *(continued)*

Feature	Description
Automation rules	■ Automation rules let you configure any process that includes a service automation library. The rulesets for a process are referred to as the automation library. The Incident Management automation library contains 13 default rulesets. The Change Management automation library contains eight default rulesets. ■ You can configure routing and notification rules for specific events within the Incident Management and the Change Management processes. ■ For example, you use the automation rules to route (assign) incidents. You can create a rule that routes all emergency and high priority incidents to one service queue. You can then create another rule that routes all other lower priority incidents to a different service queue.
Escalation rules	■ Escalation rules can be configured so that escalations are triggered when certain types of events occur. ■ For example, an escalation might trigger when an incident approaches the Service Level Agreement limitations. An escalation might trigger when a user has not responded to a Change Management approval task.
Customer Survey	■ Lets the primary contact for an incident complete a Customer Satisfaction Survey to rate the service and the resolution. See "About the Customer Satisfaction Survey" on page 188.
Advanced reporting mechanisms	■ Several out-of-the-box reports are provided, both as reports and Dashboards. ■ A report builder is included to let you create your own reports and Dashboards. ■ Report templates can be created to let groups and users customize and save their own reports. ■ Permissions can be used to manage access to reports. ■ Reports can be defined and scheduled to run periodically. ■ Reports can be emailed to a distribution list. ■ Reports can also be published as a Web service to expose report data.
Full-featured knowledge management	■ A full-featured knowledge management solution is included.
Security at a granular level	■ You can secure processes, forms, and data at the user, group, role, and organizational unit levels.

See "About ServiceDesk" on page 15.

See "Components of ServiceDesk" on page 25.

Where to get more information

Use the following documentation resources to learn and use this product.

Table 1-3 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues. This information is available as an article in the Symantec Knowledge Base .	ServiceDesk Release Notes. Choose the desired ServiceDesk version release notes document link.
Implementation Guide	Information about how to install, configure, and implement this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF Implementation Guide on the Symantec support Web site. ■ Supported Products page
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks. This information is available in PDF format. ServiceDesk has the *ServiceDesk User Guide*. This guide is for the administrator who configures and manages the Process Manager portal and the process workers who use the Process Manager portal.	Links to the documentation are available from the following locations: ■ The Documentation Library, which is available in the **Symantec Management Console** on the **Help** menu. ■ The **Documentation** page, which is available from the **Help** link in the Process Manager portal or at the following URL: ServiceDesk guides The ServiceDesk administrator can download this documentation and provide it to the appropriate users. See "Making the ServiceDesk documentation available to users" on page 236.

Table 1-3 Documentation resources *(continued)*

Document	Description	Location
Help	Information about how to use the **ServiceDesk Solution Console**. Help is not available in the Process Manager portal. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the **Symantec Management Console** on the **Help** menu. Context-sensitive Help is available for most screens in the Symantec Management Console. You can open context-sensitive Help in the following ways: ■ The **F1** key ■ The **Context** command, which is available in the **Symantec Management Console** on the **Help** menu

In addition to the product documentation, you can use the following resources to learn about Altiris products.

Table 1-4 Symantec information resources

Resource	Description	Location
Knowledge base	Articles, incidents, and issues about Symantec products.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, forums, and articles for users of this product.	Symantec Connect page

Understanding ServiceDesk concepts

This chapter includes the following topics:

Core architectural components of ServiceDesk

ServiceDesk has three main architectural components.

Table 2-1 Architectural components of ServiceDesk

Architectural component	Description
ServiceDesk Server	■ The Workflow Platform and the ServiceDesk modules are installed on a 64-bit server. ■ The Workflow Platform includes Workflow Server software, Workflow Designer, and the Process Manager portal.
SQL Server	■ Microsoft SQL Server is installed on either a 32-bit server or a 64-bit server. The Process Manager database is installed on the SQL server. ■ The Symantec Management Platform and ServiceDesk server can either share an off-box SQL server, or they can each have their own off-box SQL server. How you plan to use the Symantec Management Platform products dictates which configuration you should use. See "Server configuration options for ServiceDesk" on page 55.
Notification Server (Symantec Management Platform)	■ The Symantec Management Platform is installed on a 64-bit server. The ServiceDesk solution software is installed on the same 64-bit server. ■ The Symantec Management Platform includes its Web-based Symantec Management Console. The Symantec Management Console lets you access the ServiceDesk Solution Console page. See "Accessing the ServiceDesk Solution Console page" on page 37. ■ The Symantec Management Platform includes the Configuration Management Database (CMDB. When you install the CMDB, you can install it on the same server as Symantec Management Platform. You can also install it on a different server than the Symantec Management Platform. ■ For more information about Notification Server configurations for version 7.1 SP2, see the Symantec™ Management Platform 7.1 SP2 Installation Guide. ■ For more information about Notification Server configurations for version 7.5, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

See "Components of ServiceDesk" on page 25.

Components of ServiceDesk

The components of ServiceDesk combine to let you use ITIL-based processes to manage service tickets and your organization's knowledge.

Table 2-2 Components of ServiceDesk

Component	Description
ServiceDesk Solution software	■ Installed on the Symantec Management Platform computer. ■ Lets you manage the ServiceDesk licensing. See "About ServiceDesk licenses" on page 29. ■ Contains the installation file that is used to install the Workflow Platform and ServiceDesk modules on the ServiceDesk server computer. ■ Contains the ServiceDesk pages that appear in the Symantec Management Console. In the Symantec Management Console, you can access the **ServiceDesk Solution Console** page that lets you download the ServiceDesk installation file. ■ Lets you integrate between the ServiceDesk application software and the Configuration Management Database (CMDB). See "About ServiceDesk Solution software" on page 36.
Workflow Platform	■ Incorporates all the Symantec Workflow technologies that manage service tickets and provide reporting capabilities. ■ Includes the Workflow Server software, Workflow Designer, Process Manager database, and Process Manager portal. ■ Installed on the ServiceDesk server computer. It must not be installed on the same computer as Helpdesk Solution.
ServiceDesk modules	■ Contain the predefined, ITIL-based processes. These processes let you manage incidents, changes, problems, and knowledge. ■ Installed on the ServiceDesk server computer. After installation, you must configure these processes to meet the needs of your organization. See "What you can do with ServiceDesk" on page 16.
Workflow Designer	■ Tool that is included with the Workflow Platform. ■ Lets an administrator implement advanced ServiceDesk customizations to better meet the needs of the organization.
Process Manager Portal	■ A Web-based interface that resides on the ServiceDesk server and provides access to the ServiceDesk processes. ■ Lets the users access the Process Manager portal from a Web browser to run the ServiceDesk processes. See "About the Process Manager portal" on page 182.

Table 2-2 Components of ServiceDesk *(continued)*

Component	Description
Workflow Server software	▪ Includes the workflow extensions that are required to run the ServiceDesk core processes. ▪ Must run on the ServiceDesk server computer.
Process Manager database	▪ Stores the Process Manager details such as groups, users, and permissions and stores persistent Workflow data. ▪ Must reside on the SQL Server computer.
Configuration Management Database (CMDB)	▪ A repository of the information that is related to all the components or resources of an information system. ▪ In the ITIL context, the CMDB represents the authorized configurations of the significant components (configuration items) of the IT environment. See "About ServiceDesk and the Configuration Management Database (CMDB)" on page 27.
Configuration item (CI)	▪ Component of your organization's infrastructure that is under the control of Configuration Management. ▪ Can represent hardware, software, or associated documentation. See "About configuration items" on page 26.

See "Core architectural components of ServiceDesk" on page 23.

See "How ServiceDesk works" on page 18.

About configuration items

A configuration item (CI) is a component of your organization's infrastructure that is under the control of Configuration Management. A configuration item can represent hardware, software, or associated documentation. For example, configuration items can include services, servers, equipment, network components, desktop and mobile computers, applications, licenses, telecommunication services, and facilities.

When you work a change request, you can associate it with one or more configuration items. ITIL recommends that each change should reference one or more configuration items.

The configuration items are modeled in the Configuration Management Database (CMDB).

See "About ServiceDesk and the Configuration Management Database (CMDB)" on page 27.

See "Components of ServiceDesk" on page 25.

See "About populating the CMDB for ServiceDesk" on page 28.

About ServiceDesk and the Configuration Management Database (CMDB)

The Configuration Management Database (CMDB) is a repository of the information that is related to all the components or resources of an information system. In the ITIL context, the CMDB represents the authorized configurations of the significant components (configuration items) of the IT environment. For example, the CMDB can contain information about hardware, software, associated documentation, assets, contracts, and users.

For more information about CMDB Solution 7.1 SP2, see the Altiris™ CMDB Solution 7.1 SP2 User Guide.

For more information about CMDB Solution 7.5, see the Altiris™ CMDB Solution 7.5 User Guide.

The CMDB lets you manage the resources throughout their lifecycle, which helps your organization understand the relationships between these resources and track their configuration.

In the Symantec Management Platform, configuration items are typically referred to as resources.

See "About configuration items" on page 26.

The CMDB is a standard component of the Symantec Management Platform. CMDB Solution, which is a requirement for installing ServiceDesk, provides additional capabilities for managing the data in the CMDB.

For a CMDB implementation to be successful, the CMDB must be able to automatically discover and update information about the organization's resources. The Symantec Management Platform provides the tools to perform these tasks.

Examples of the resource management tasks that can be performed are as follows:

- Automatically discover resources such as computers and software.
  For example, the Symantec Management Platform can discover the computers in an organization and add them to the CMDB.
- Import resources.
- Create resources manually.
- Create associations between resources.
  For example, associations can be created between users, computers, and departments.
- Create customized actions and rules to manage and manipulate data.

See "About populating the CMDB for ServiceDesk" on page 28.

See “Components of ServiceDesk” on page 25.

About populating the CMDB for ServiceDesk

The Configuration Management Database (CMDB) represents the authorized configurations of the significant components (configuration items) of the IT environment. For example, the CMDB can contain information about hardware, software, associated documentation, assets, and contracts.

See “About ServiceDesk and the Configuration Management Database (CMDB)” on page 27.

In the Symantec Management Platform, configuration items are typically referred to as resources.

See “About configuration items” on page 26.

ServiceDesk uses the following configuration items (resources) that are defined in the CMDB: equipment, locations, and services. This information provides additional details to incidents that can help the resolution. For example, during the creation of an incident, the technician can select the user’s location and any related configuration items that the issue affects.

Technically, you can use ServiceDesk without the CMDB data, but doing so limits the amount of information that can be included in incidents. For example, if the CMDB does not contain equipment data, the user cannot specify the affected equipment in the incident.

If you upgrade from a 6.x Altiris product, the CMDB is upgraded at the same time. Otherwise, you must populate it after you install the Symantec Management Platform.

For more information about populating the CMDB, see the Altiris™ CMDB Solution 7.1 SP2 from Symantec™ User Guide.

For more information about populating the CMDB, see the Altiris™ CMDB Solution 7.5 from Symantec™ User Guide.

Examples of how you can add resource data to the CMDB are as follows:

- Create the resources manually.
- Discover computers.
- Import computers from Active Directory.
- Discover network devices.
  For example, the Network Discovery function can discover routers, switches, network printers, Novell NetWare servers, and the computers that run Windows, UNIX, Linux, and Macintosh.

- Import resource associations from Active Directory.
  Microsoft Active Directory not only stores objects, it also stores relationships between objects. Microsoft Active Directory Import can extract these relationships from Active Directory and create the appropriate resources and resource associations in the CMDB
- Import data from several other solutions in the Symantec Management Platform.
  For example, you can import software resources from Inventory Solution.

This instruction is part of the following installation processes:

See “Installing ServiceDesk for the first time” on page 66.

See “Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2” on page 67.

This instruction is part of the following migration processes:

See “Migrating from ServiceDesk 7.0” on page 73.

See “Migrating from Helpdesk Solution 6.x to ServiceDesk” on page 71.

About ServiceDesk licenses

The ServiceDesk licenses that you purchased determine the number of people who can work in the ServiceDesk portal at one time. A license is consumed when a logged-on user has a ServiceDesk **Process View** page open to work a ticket for any of the ServiceDesk processes.

The ServiceDesk licensing is IP-based. Therefore, a user can run multiple instances of ServiceDesk on one computer but consume only one license.

When all the licenses are in use, the next user who tries to edit a ticket is denied access until a license becomes available.

A license is released in the following instances:

- When a user closes a **Process View** page.
  Note that it might take a few minutes for the license to become available.
- When a **Process View** page is open and inactive for a certain amount of time, and the Web session times out.
  IIS settings determine the timeout period.

Certain activities do not consume a license, as follows:

- The user enters and submits a ticket.
- The user is engaged in the ServiceDesk activities that are not related to a ticket.
  For example, a license is not consumed when the user browses documents or reads a knowledge base article.

- The primary contact has the **Process View** page open for any of the tickets that they submitted.

See “Components of ServiceDesk” on page 25.

See “About ServiceDesk Solution software” on page 36.

About Incident Management

Incident Management is one of the core ITIL-based processes, and one that ServiceDesk users work with the most frequently. With the Incident Management process, users can manage and quickly resolve incidents themselves, and analysts can manage, track, and prioritize issues.

See “What you can do with ServiceDesk” on page 16.

The goal of Incident Management is to recover from incidents and restore service to users as quickly as possible.

Incident Management includes the following key features:

- The Automation rules designer lets you execute actions based on 13 potential decision points.
- The 13 decision points, or rulesets, let you create rules for routing, email, and other actions. When the ruleset is initiated, the rules execute automatically.
- In addition to the 13 default rulesets, you can create your own rulesets based on your organization's requirements.
- An intuitive form for users to submit incidents from the self-service portal.
- The ability to include information about the user and the user’s assets in the incident data in the incident form.
- The inclusion of specialized tasks that help the technician diagnosing the issue and provide opportunities to either resolve or escalate the issue.
- Opportunities to use the knowledge base to help the technician resolve an incident and to provide additional information to the user.
- The inclusion of the user in the Incident Management process, by letting the user decide if an issue is resolved to their satisfaction. The user can also provide feedback on their service experience.

The Incident Management process provides information to the other ServiceDesk processes as follows:

- A collection of incidents that can be used in Problem Management to identify root causes of incidents. When the root causes are identified, they can be resolved to prevent further incidents from occurring.

- Information from the incidents, which is used in Change Management to determine how to standardize methods and procedures for efficient handling of all changes.
- Serves as a source of information for future knowledge base articles.

About Problem Management

The Problem Management process looks at the root causes of the problems that cause multiple incidents. Problem Management then seeks to take actions to fix the situation and prevent it from recurring. The goal of the process is to minimize the effect of incidents and problems on the business.

To manage problems successfully, you need the ability to perform the following actions:

- Track problems.
- Diagnose the problems.
- Fix the problems through change requests.
- Publish known errors to help with future resolutions.

Part of the Problem Management process is to group related incidents for additional analysis and discovery of root causes. This analysis and discovery lets Problem Management take Incident Management a step further. Incident Management seeks to resolve the single issue at hand, so that a user can get up and running again. Problem Management goes deeper and seeks to take the actions that prevent that issue from happening again. When the problem is identified, a change request can be created or a knowledge base article can be requested.

In general, Problem Management deals with the issues that multiple users have encountered. For example, multiple users may experience an issue with a certain software program. Each of these issues can be resolved individually through the Incident Management process. However, the Problem Management process might suggest a Service Pack update for all users of that software. This solution would solve the individual incidents and prevent other users from encountering the issue and creating new incidents.

Problem Management includes the following key features:

- The ability to group incidents so that the root cause that is common to all the incidents can be analyzed.

  The information in the problem request can be forwarded for use in a change request, or sent back to support technicians as a resolution.
- One notification can be sent for all the incidents that are associated with the problem.

- The knowledge base can be used as part of a resolution for a problem, and problems can provide information for the knowledge base.

The Problem Management process provides information to the other ServiceDesk processes as follows:

- Obtains the initial context of a problem from the Incident Management process.
- Provides the context that is related to the problem to assist in the decision making during the Change Management process.
- Provides the documentation from problems to the knowledge base.

See “What you can do with ServiceDesk” on page 16.

About Change Management

The goal of Change Management is to standardize methods and procedures to ensure the most efficient handling of the changes that an organization requires. An effective Change Management process minimizes how changes affect service and improves the reliability and responsiveness of IT services and processes. This improvement leads to a quicker turnaround on changes and reduces unplanned work, rework, and duplicated efforts.

Change Management includes the following key features:

- Problems can be escalated to a change request or change requests can be initiated independently.
- The Automation rules designer lets you execute actions based on eight potential decision points.
- The eight decision points, or rulesets, let you create rules for routing, email, and other actions. When the ruleset is initiated, the rules execute automatically.
- In addition to the eight default rulesets, you can create your own rulesets based on your organization's requirements.
- The change approval board analyzes the risk that is associated with the change as part of the process.
- Supports multiple change managers, each with their own customized rights to tickets and actions.
- All participants review the proposed schedule.
- All the plans that are created as part of the Change Management process are stored with the change request and easily accessible to all participants.
- Users can consult the Forward Schedule of Change calendar to avoid scheduling conflicts when they plan changes. The Forward Schedule of Change calendar

provides visibility into other planned changes, outages, change freeze periods, and holidays.

- When the plans are finalized, the change approval board provides final approval, and the implementation task is assigned based on the scheduled date and time.
- When a change request is completed, the problems and incidents that are associated with that change request are automatically updated with a resolution and closed.

The Change Management process interacts with the other ServiceDesk processes as follows:

- Obtains incident information from the Incident Management process.
- Obtains the documentation of the proposed change from the Problem Management process.
- Serves as a source of information for future knowledge base articles.

See "About the Change Management process" on page 218.

See "What you can do with ServiceDesk" on page 16.

About Knowledge Management

The Knowledge Management process gathers, analyzes, stores, and shares knowledge and information within an organization. The goal of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge. Collecting information in the knowledge base lets organizations match new incidents against previous ones and reuse established solutions and approaches.

When the knowledge base is implemented correctly, it can significantly improve incident resolution time and customer satisfaction. The knowledge base can contain information about the best practices that address the most common issues that users encounter. Instead of having to solve the same customer issues repeatedly, incident technicians can search the knowledge base for information about similar issues. Providing established methods for addressing common incidents reduces response time.

Users can access the knowledge base to obtain self-service resolution of common problems. By providing users with the knowledge resources to solve problems on their own, you can greatly reduce the number of incidents that they submit. When a user submits an incident, they can search the knowledge base to determine if there is a solution to the incident. If the user finds a solution, they might be able to implement the solution on their own. This self-service reduces the number of incidents that are submitted to the ServiceDesk.

In ServiceDesk, the Knowledge Management process provides a means to submit, review, approve, and post information to the knowledge base. The process increases the reliability of the knowledge base so that it can be used to improve the other processes in your organization.

The Knowledge Management process includes the following key features:

- The Bulletin Board, which facilitates proactive notification of important issues.

  For example, if the Internet access is down, you can let users know that IT is aware of the problem. As a result, you minimize further incident submissions for that issue.
- The ability to set up a nested category hierarchy to organize knowledge base items and make them easier for users to find.
- The ability to set permissions at both the category level and the individual document level.
- A knowledge base approval process that helps to ensure that the content is relevant and accurate before publication.
- The ability for users to rate knowledge base items based on their usefulness. ServiceDesk automatically gives higher ratings to the articles that are most often used to resolve issues. You can run reports on the ratings to determine which knowledge base items should be removed or modified to improve their content.
- A fully-audited content management system that stores the knowledge base content. You can run reports to analyze this content. For example, you can report the number of times a knowledge base item was viewed and how recently it was viewed.
- The accessibility of the knowledge base information from within the ServiceDesk processes. Easy access from processes lets users take full advantage of the knowledge base, as well as easily add new content to the knowledge base.

See “What you can do with ServiceDesk” on page 16.

About the Active Directory Self Service Catalog

The **Active Directory Self Service Catalog** provides end users with a collection of request processes for interacting with the Active Directory domain. The associated workflow project files are also available for each Active Directory self-service catalog request.

With the **Active Directory Self Service Catalog**, you can perform the following actions in the Process Manager portal:

- Request an Active Directory password reset

- Request access to an Active Directory network share

Introducing ServiceDesk Solution software

This chapter includes the following topics:

- About ServiceDesk Solution software
- About the ServiceDesk Solution Console page
- Accessing the ServiceDesk Solution Console page

About ServiceDesk Solution software

The ServiceDesk Solution software is a component of the ServiceDesk product. It is different from the ServiceDesk application software, which provides the interface for managing service tickets and performing other service tasks. The ServiceDesk Solution software is installed on the Symantec Management Platform computer and the ServiceDesk application software is installed on the ServiceDesk server computer.

See "Components of ServiceDesk" on page 25.

The ServiceDesk Solution software provides the following functions:

- Management of the ServiceDesk licenses
  The Symantec Installation Manager (SIM) installs the ServiceDesk Solution software on the Symantec Management Platform and applies the ServiceDesk licenses. The ServiceDesk solution software manages the consumption of the ServiceDesk licenses.
  See "About ServiceDesk licenses" on page 29.
- Download of the installation file that is used to install ServiceDesk on the ServiceDesk server.

In the Symantec Management Console, you can access the **ServiceDesk Solution Console** page that lets you download the ServiceDesk installation file to the ServiceDesk server. The ServiceDesk server is different from the Symantec Management Platform.

On the **ServiceDesk Solution Console** page, you can also download the Screen Capture Utility Installer.

- Creation of ServiceDesk incidents for the specific resources that are defined in the CMDB (Configuration Management Database).
- Integration between ServiceDesk and the CMDB.
  See "About ServiceDesk and the Configuration Management Database (CMDB)" on page 27.

About the ServiceDesk Solution Console page

The **ServiceDesk Solution Console** page lets you perform the following tasks:

- View the number of ServiceDesk licenses that are available.
- Download the ServiceDesk installation file.
  See "Downloading the ServiceDesk installation file" on page 98.
- View all incidents that are associated with a resource and that have been reported from the ServiceDesk server.

The **ServiceDesk Solution Console** page appears in the Symantec Management Console.

See "Accessing the ServiceDesk Solution Console page" on page 37.

The ServiceDesk solution software is a component of the ServiceDesk product

See "About ServiceDesk Solution software" on page 36.

The ServiceDesk solution software lets you view all changes, incidents, or problems that are associated with a resource.

Accessing the ServiceDesk Solution Console page

The **ServiceDesk Solution Console** page displays your ServiceDesk licenses, lets you download installation files for ServiceDesk, and provides information about incidents.

See "About the ServiceDesk Solution Console page" on page 37.

To access the ServiceDesk Solution Console page

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, expand **Settings > Service and Asset Management > ServiceDesk** and then click **ServiceDesk**.

Section 2

Planning the ServiceDesk Implementation

Preparing your ServiceDesk implementation

This chapter includes the following topics:

About developing your ServiceDesk installation plan

You use the Symantec Installation Manager (SIM) to install your instance of the Symantec Management Platform and the ServiceDesk Solution Software on the Symantec Management Platform server. After the ServiceDesk Solution software is installed, you can then download the ServiceDesk installation file onto the ServiceDesk server and install ServiceDesk.

Before you install your instance of the Symantec Management Platform you should develop an installation plan.

For information about the Symantec Management Platform 7.5 installation plan, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

For information about the Symantec Management Platform 7.1 SP2 installation plan, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

Before you download the ServiceDesk installation file to your ServiceDesk server and install ServiceDesk, you should develop an installation plan.

As you develop an installation plan, you should answer the following questions:

Table 4-1 Questions for developing your ServiceDesk installation plan

Question	Description
What type of installation should you perform?	■ Are you installing ServiceDesk 7.5 for the first time? ■ Are you installing ServiceDesk 7.5 in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2? ■ Are you migrating from ServiceDesk 7.0 or 7.1x to ServiceDesk 7.5? ■ Are you migrating from ServiceDesk 7.1 SP2 to ServiceDesk 7.5? ■ Are you migrating from Helpdesk Solution 6.x?
How many technicians do you employ to work incidents, changes, and problems and what is your volume of incident, change, and problem tickets?	■ You configure your installation of ServiceDesk differently depending on the size of your environment. ■ For example, you plan to install and use several of the Symantec Management products. For this environment, you do not want to use the same off-box SQL Server for both the Symantec Management Platform and ServiceDesk Server . Instead, you want them each to have their own off-box SQL server.
Does my installation plan leave room for future growth?	■ If possible, your installation plan should reflect both the current organization and the vision for the organization over the next three years.
Does my server meet the minimum system requirements?	■ During the installation process, the ServiceDesk Installation and Configuration Wizard performs a system readiness check. ■ During this check, the wizard determines if the server is ready for installation. ■ This check only verifies that the server meets the minimum requirements. ■ Before you install ServiceDesk, you should make sure that the server meets the system requirements that are appropriate for your environment.
Is the installation for a production environment or for evaluation purposes?	■ If you are an evaluator, you can quickly install, configure, and begin testing ServiceDesk. ■ In a production environment, Symantec recommends that you install ServiceDesk in a test environment before you install it in a production environment. ■ Your test environment should be identical to your production environment.

For additional installation plan information, see the following:

See “Core architectural components of ServiceDesk” on page 23.

See “Assembling your ServiceDesk implementation team” on page 42.

See “ServiceDesk scalability” on page 44.

See “Server configuration options for ServiceDesk” on page 55.

See "System requirements for ServiceDesk" on page 59.

See "ServiceDesk 7.5 support matrix" on page 57.

For information about the different installation scenarios, see the following:

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

For information about the different migration scenarios, see the following:

See "Before you migrate from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 76.

See "Before you migrate from ServiceDesk 7.1x" on page 75.

See "Before you migrate from ServiceDesk 7.0" on page 72.

See "Before you migrate from Helpdesk Solution 6.x to ServiceDesk" on page 70.

Assembling your ServiceDesk implementation team

During ServiceDesk installation and implementation, verify that the right personnel with the proper skill sets and knowledge are available during the process. Installation entails installing the Workflow Platform and ServiceDesk modules. Before you introduce ServiceDesk into your environment, you must configure it to meet the needs of your organization. In some cases, you may even need to implement some advanced customizations.

Table 4-2 Required roles and skills

Role	Skills	Description
Network administrator with IIS knowledge	Ensures that the IIS process functions correctly.	You need someone on your team who possesses IIS-specific skills and can ensure that the processes have the correct security and rights.
Network administrator with SQL knowledge	Ensures that the SQL Server is installed, configured, and functions correctly.	You need someone on your team who possesses SQL-specific skills and can ensure that the processes have the correct security and rights.
(optional) Network administrator with Active Directory knowledge This role is only needed if you plan to use Active Directory authentication for ServiceDesk.	Ensures the Active Directory connections and sync profiles function correctly.	You need someone your team who possesses Active Directory-specific skills and can ensure that the processes have the correct security and rights.

Table 4-2 Required roles and skills *(continued)*

Role	Skills	Description
Workflow administrator	Ensures that advanced customizations to ServiceDesk processes function correctly.	You need someone on your team who has a solid working knowledge of the following software: ■ SQL Needs to understand the background processes that run as part of the ServiceDesk workflows. ■ Workflow Designer Needs to understand how to use the tool that lets you implement advanced customizations to the ServiceDesk workflow processes.
Business analyst	Ensures that ServiceDesk configurations meet organizational standards and that Incident and Change Management function correctly after configuration.	You need someone on your team who possesses the following knowledge: ■ Service Level Agreements (business hours and holidays) ■ Prioritization methodology ■ Rules requirements ■ Organizational look and feel (logos and email formats)
Test team	Ensures that ServiceDesk functions properly after it is installed and configured.	You need a test team that contains at least one representative from all the major groups that use ServiceDesk. For example a test team may include technicians, administrators, end users, a change manager, and a problem analyst. The test team performs the following functions: ■ Reviews the recommendations by the business analyst for SLAs and rulesets, before implementation. ■ Test the specific policies that are related to those SLAs and rulesets.

Table 4-2 Required roles and skills *(continued)*

Role	Skills	Description
Pilot group	Ensures that ServiceDesk functions properly before it is fully introduced into the production environment.	You need a small number of preselected end users that begin using ServiceDesk before it is rolled out into the production environment. Use this time to do the following: ■ Work out any process issues, such as routing rules or SLAs ■ Make sure that technicians and administrators are prepared to roll ServiceDesk out to the rest of the organization.

See "About developing your ServiceDesk installation plan" on page 40.

ServiceDesk scalability

ServiceDesk has three main architectural components that you must consider when scaling ServiceDesk to meet the needs of your environment and for optimal performance. The main architectural components are the ServiceDesk server, Notification Server (Symantec Management Platform), and SQL Server.

See "Core architectural components of ServiceDesk" on page 23.

See "Recommendations for scaling the ServiceDesk server and its dedicated SQL Server" on page 46.

When scaling your ServiceDesk environment, you must consider the following principal factors:

Table 4-3 Principal factors for scaling the ServiceDesk environment

Factor	Description
Future growth	■ Considerations for scaling your ServiceDesk environment should include any expansion plans for the next three years, if possible. ■ As your organization grows, your number of incidents, changes, and problems grows in accordance. ■ As your incidents, changes, and problems grow, so does the number of technicians that are needed to handle your service needs.

Table 4-3 Principal factors for scaling the ServiceDesk environment *(continued)*

Factor	Description
Symantec Management Platform	■ ServiceDesk 7.5 requires a running installation of a 7.5 instance or a 7.1 SP2 instance of the Symantec Management Platform. ■ You must also scale your instance of the Symantec Management Platform to meet the needs of your environment and for optimal performance. For information about the Symantec Management Platform 7.5 requirements, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide. For information about the Symantec Management Platform 7.1 SP2 requirements, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.
ServiceDesk servers	■ You install the Process Manager portal on the ServiceDesk server. ■ The Process Manager portal is where you manage and resolve incidents, problems, and changes. This portal is also where you manage and add to your knowledge base. ■ The maximum number of technicians working in the Process Manager portal at one time determines the number of ServiceDesk servers your environment needs. The number of technicians is the primary scaling factor used to determine how many ServiceDesk servers that you install. See "Recommendations for the number of ServiceDesk servers" on page 47.
SQL Server configuration	■ You install the Process Manager database on the SQL Server. The throughput of the SQL Server is the primary consideration for configuring your SQL Server for optimal performance to meet your ServiceDesk needs. ■ The throughput considerations are Input/ Output per second and concurrent SQL transactions, which relate to the peak number of tickets that are processed each day. See "SQL Server configuration options for ServiceDesk" on page 49. See "Recommended SQL Server hardware" on page 54.

Recommendations for scaling the ServiceDesk server and its dedicated SQL Server

Symantec recommends that the ServiceDesk server has its own dedicated off-box SQL Server. The SQL Server information that is provided addresses the needs of ServiceDesk only. It does not address the needs of the Symantec Management Platform and any other solutions you may have installed in your environment.

The number of technicians influences the peak number of tickets processed each day. The peak number of tickets that are processed influences your Input/Output per second and SQL concurrent transactions. These factors determine how you configure your SQL Server.

When scaling your ServiceDesk environment, you must consider the following components:

Table 4-4 Principal ServiceDesk and SQL Server components for scaling the ServiceDesk environment

Component	Evaluation	0 - 25 Technicians	26 - 50 Technicians	51 - 75 Technicians	76+ Technicians
ServiceDesk server	Single ServiceDesk server	Single ServiceDesk server	Single ServiceDesk server	Single ServiceDesk server	Load balanced: A ServiceDesk server for every 75 technicians
Processor	Two cores	Four cores	Eight cores	Eight cores	Eight cores per server
RAM	8 GB	8 GB	16 GB	32 GB	32 GB per server
SQL Server	On-box	Off-box	Off-box	Off-box Separate channel for database, Transactions, and TempDB database	Off-box Separate channel for database, Transactions, and TempDB database
Processor	One core	Four cores	Eight cores	Eight cores	Eight cores
Disk speed	SAS 10k	SAS 10k in high-performance disk array	SSD or SAS in RAID 10 configuration	SAS 15k in high-performance disk array	SSD or SAS 15k equivalent in a high-performance disk array
Disk capacity	80 GB	80 GB	120 GB	200 GB	400 GB

Table 4-4 Principal ServiceDesk and SQL Server components for scaling the ServiceDesk environment *(continued)*

Component	Evaluation	0 - 25 Technicians	26 - 50 Technicians	51 - 75 Technicians	76+ Technicians
RAM	16 GB	16 GB	24 GB	32 GB	48 GB

See "ServiceDesk scalability" on page 44.

See "Recommendations for the number of ServiceDesk servers" on page 47.

See "SQL Server configuration options for ServiceDesk" on page 49.

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

Recommendations for the number of ServiceDesk servers

The following information provides guidelines for determining the number of ServiceDesk server installations that you need in your ServiceDesk environment. These guidelines are not rigid. You may discover that additional environmental conditions are present that may dictate the need for additional ServiceDesk servers despite the suggestions in these guidelines.

Table 4-5 Recommendations for the number ServiceDesk servers

Number of Technicians	Description
Evaluation	■ Requires a single installation of the ServiceDesk server.
0-25	■ Requires a single installation of the ServiceDesk server.
26-50	■ Requires a single installation of the ServiceDesk server.
51-75	■ Typically requires a single instance or installation of the ServiceDesk server. ■ The maximum number of technicians recommend for a single instance of the ServiceDesk server is 75. ■ When you approach the maximum number of technicians per server, you may want to consider a second installation of the ServiceDesk server on new hardware. The second installation may be needed to keep your application performance optimal.
76+	■ Requires two installations of the ServiceDesk server.

Table 4-5 Recommendations for the number ServiceDesk servers *(continued)*

Number of Technicians	Description
Every additional 75	■ As your number of technicians grows, so does your need for additional ServiceDesk server installations. For every 75 technicians, you need an installation of the ServiceDesk server. ■ For example, if you have 150+ technicians, you need two installations of the ServiceDesk server. If you have 400 technicians, you need six installations of the ServiceDesk server.

The number of technicians influences the peak number of tickets processed each day. The peak number of the tickets processed influences to your Input/Output per second/SQL concurrent transactions, which determines how you configure your SQL Server.

See "SQL Server configuration options for ServiceDesk" on page 49.

If your environment requires more than one installation of the ServiceDesk server, you may consider implementing load balancing. Load balancing allows your ServiceDesk servers to share data, such as incident ticket data, change ticket data, and knowledge base articles. If you do not set up load balancing, then your ServiceDesk servers do not share this data.

Before you decide to use load balancing, you must determine if it is necessary for your environment.

See "About load balancing your ServiceDesk environment" on page 48.

See "ServiceDesk scalability" on page 44.

See "Recommendations for scaling the ServiceDesk server and its dedicated SQL Server" on page 46.

About load balancing your ServiceDesk environment

Load balancing lets you prepare for scalability and growth to your ServiceDesk environment. Setting up a load-balanced environment requires preparation and planning. It also adds some additional maintenance overhead. You must consider load balancing before installation, upgrades, and updates.

Note: You must set up your load-balanced environment before you install ServiceDesk. You cannot introduce load balancing during or afterwards.

You should plan your implementation schedule to allow for adequate testing. You should set up an environment that resembles the proposed production implementation.

The main reason for setting up a load-balanced environment is that you need additional server resources to keep up with your environment's load.

The following are examples of increased loads:

- Each additional installation of the ServiceDesk server, you put more of a load on your SQL server.
- The more technicians you have processing tickets, the greater the number of concurrent SQL transactions.
- The more process tickets that are generated each day, the more SQL server resources are required. Additional ServiceDesk servers can help to maintain system responsiveness as your usage levels increase.

For more information about load balancing, refer to the Symantec™ Workflow 7.5 User Guide.

See “Recommendations for the number of ServiceDesk servers” on page 47.

SQL Server configuration options for ServiceDesk

The following information provides guidelines for SQL Server configuration for a ServiceDesk (Process Manager) Database server. You can follow these guidelines to tune the performance of the SQL Server that hosts the Process Manager database. These guidelines are not exclusive, and additional configuration options may be appropriate depending on the specifics of your environment. For detailed information about SQL Server configuration, refer to Microsoft’s documentation.

Table 4-6 SQL Server configuration options

Consideration	Description
Hardware: processors and memory	Having sufficient processors and memory lets you tune the performance of your SQL Server. 4 to 8 cores are common in well-performing environments.
Disk drive channel configuration	The way that you configure the disk drives and the controllers that interface those to your SQL server has one of the largest influences on your overall performance. You can use disk drive channel configuration recommendations to maximize throughput and tune the performance of your SQL Server. See “Hard drive configuration options for an off-box SQL Server” on page 50.

Table 4-6 SQL Server configuration options *(continued)*

Consideration	Description
Database sizing	You can use database sizing guidelines to help tune the performance of your SQL Server. See "Database sizing for SQL Server for ServiceDesk" on page 52.
Memory management	You can use memory management guidelines to help tune the performance of your SQL Server. See "Memory management options for SQL Server performance" on page 53.

See "ServiceDesk scalability" on page 44.

See "Recommendations for the number of ServiceDesk servers" on page 47.

See "Recommendations for scaling the ServiceDesk server and its dedicated SQL Server" on page 46.

Hard drive configuration options for an off-box SQL Server

Data throughput of the SQL Server is a key consideration for ServiceDesk performance. The way that you configure your disk drives in SQL Server has a key influence on throughput. The hard drive speed also has an influence on throughput. It is recommended to use high performance hard disks. For example, you can use 10k rpm to 15k rpm SAS drives in a striped array.

For the best performance, make sure that the operating system, SQL data file, TempDB database, and the log file each have a dedicated volume, and associated controller channel. The data file requires both high read-write performance and redundancy. RAID 10 and RAID 0+1 are good configurations for the data file. RAID 0+1 has similar throughput as RAID 10, but its configuration helps simplify additional storage growth. RAID level 5 is not ideal for the database performance because it requires additional Read/Write activities for parity.

The TempDB database needs high read-write performance, but redundancy is not necessary. The TempDB database acts as a temporary working area for many processes. The TempDB database requires very high speed; however, it is not used for storage, and it is cleared regularly.

The transaction log also requires high disk throughput for optimal system performance. It should be hosted on a RAID 10.

In all of these options, the key factor is the end result that resides on separate physical disk and drive controller hardware. The best performance and maximum efficiencies are when that configuration rule is applied. Care should be taken if SAN or NAS storage is used to assure performance and efficiency. SAN and NAS storage arrays are often carved into logical volumes. These logical volumes are for optimizing space usage, and allowing multiple servers and applications to access (share) the same physical devices. This causes disk contention and slow performance. If you plan to use SAN or NAS, it is best to have this requirement discussed and planned for during implementation. Include the storage administrators in the planning.

Table 4-7 Example of an off-box SQL Server disk configuration

Component	Configuration
Operating system RAID 1 Mirror	RAID 1 Mirror
Data file	RAID 10 or RAID 0+1
TempDB database	RAID 0 (Striping)
Transaction log	RAID 10 or RAID 0+1

See “SQL Server configuration options for ServiceDesk” on page 49.

See “Throughput metrics of SQL Server for ServiceDesk” on page 51.

Throughput metrics of SQL Server for ServiceDesk

The Process Manager database has high throughput requirements. Input/Outputs per second (IOPS) are used to measure the throughput. You can use the following IOPS metrics to select the right disk performance for your SQL Server.

The database that is represented here serves 20,000 endpoints and 20 concurrent console sessions and 45 maximum persistent connections over 2311 concurrent transactions. It represents SQL performance statistics during a one hour time period during peak hour processing.

Table 4-8 SQL data file Input/Output per second

Metric	Value
Number of I/O per second	238.7
Percent of writer I/O per second	98%
Percent of read I/O per second	2%

Table 4-9 TempDB database Input/Output per second

Metric	Value
Number of I/O per second	130
Percent of writer I/O per second	49%
Percent of read I/O per second	51%

Table 4-10 Log files Input/Output per second

Metric	Value
Number of I/O per second	593.8
Percent of writer I/O per second	100%
Percent of read I/O per second	0%

See “SQL Server configuration options for ServiceDesk” on page 49.

See “Hard drive configuration options for an off-box SQL Server” on page 50.

Database sizing for SQL Server for ServiceDesk

Limited concerns exist in the sizing of the ServiceDesk database. Most customers even with large environments seldom see database file sizes grow much larger than 20-40 GB. The average database size ranges from 4-15GB.

Allow between 750KB and 1 MB of space in the database for every 1,000 service tickets. This sizing does not account for database fragmentation beyond initial creation. The database maintenance strategy that you use also influences your database size.

Autogrow is a SQL Server setting you can use to help with unexpected data growth. However, do not rely on autogrow to manage your database file sizes. As with any key application, you must monitor the database and have proper maintenance tasks in place.

To choose your autogrow setting, estimate the expected maximum sizes of the data file and the transaction log file. To estimate this size you can monitor the growth of these files in a pre-production environment. Set the autogrow increment for your data file and transaction log files to 10 to 20 percent higher than your initial estimate.

Do not use the autoshrink feature with ServiceDesk. Auto shrink runs periodically in the background. It consumes CPU and I/O cycles, which can cause unexpected performance degradation. Autoshrink can continually shrink and re-grow the data files. This process causes fragmentation of the database file. This fragmentation may degrade both sequential transfers and random accesses. If Autoshrink is required in your environment, please schedule it to run only after normal work hours.

To further improve performance, you should defragment and re-index the database after its initial installation.

The Process Manager SQL Server should not host additional third-party database applications. For best performance, Symantec recommends that the Process Manager SQL Server not host any additional databases. The load and I/O traffic of ServiceDesk are sufficient to require a dedicated SQL Server. You can have a single SQL instance that shares a single TempDB database, or multiple database instances can each have a dedicated TempDB database. Multiple database instances minimize risk for potential contention but require more disk arrays.

You may require the individual Process Manager databases of each ServiceDesk server to exist on a separate instance. They may need to be separate instances to avoid TempDB database contention.

See “SQL Server configuration options for ServiceDesk” on page 49.

Memory management options for SQL Server performance

Memory management is an important part of tuning SQL Server performance. Various options are provided for your review and consideration. However, using 64-bit SQL and configuring SQL to use all of the memory that is provided is recommended for optimal ServiceDesk performance.

Table 4-11 SQL Server memory configuration options

Option	Description
3GB	■ This 32-bit Windows boot option limits the operating system to 1GB of RAM, reserving 3GB for applications.
Maximum server memory	■ This SQL setting limits the memory that SQL can consume.
PAE	■ This 32-bit Windows boot option allows SQL Server to use more than 4GB of RAM.

Table 4-11 SQL Server memory configuration options *(continued)*

Option	Description
AWE	■ This SQL option allows SQL Server to use more than 2GB of RAM. ■ If the server has more than 2GB of physical memory, enable AWE memory in SQL Server. This memory mode is recommended. ■ When AWE is enabled, SQL Server always attempts to use AWE-mapped memory. It uses wrapped memory or all memory configurations, including computers that provide applications with less than 3 GB of user mode address space. ■ If AWE memory is enabled in SQL, make sure that the SQL Server account has the correct Lock Pages in Memory setting. Both AWE and the Lock Pages in Memory setting can benefit 64-bit SQL Servers as well as 32-bit SQL Servers.
Windows memory usage	■ Set Windows memory usage to favor Programs over System Cache. SQL Server does its own data caching to improve performance.
32-bit OS	■ If you use a 32-bit OS, make sure that PAE is enabled at the hardware level. ■ Enabling PAE lets SQL Server use AWE to map physical memory addresses higher than 4GB.
64-bit SQL (Recommended SQL configuration)	■ This option eliminates the memory limitations that are associated with 32-bit systems. ■ By using a 64-bit operating system (Windows Server 2008 R2 SP1) and 64-bit SQL, you do not need to use PAE or AWE. ■ SQL Server 2008 x64 is recommended for dedicated SQL Servers with more than 4 GB of physical memory.

See “SQL Server configuration options for ServiceDesk” on page 49.

Recommended SQL Server hardware

The following are general hardware recommendations for most environments with ServiceDesk 7.5. Depending on your specific circumstances, the appropriate hardware may vary.

Table 4-12 ServiceDesk hardware recommendations for Microsoft SQL Server

Component	Evaluation	25 Users	50 Users	75 Users	100+ Users
Processor	One core	Four cores	Eight cores	Eight cores	Eight cores

Table 4-12 ServiceDesk hardware recommendations for Microsoft SQL Server *(continued)*

Component	Evaluation	25 Users	50 Users	75 Users	100+ Users
Disk Speed	SAS 10k	SAS 10k in high-performance disk array	SSD or SAS in RAID 10 configuration	SAS 15k in high-performance disk array	SSD or SAS 15k equivalent in a high-performance disk array
Disk Capacity	80 GB	80 GB	120 GB	200 GB	400 GB
RAM	16 GB	16 GB	24 GB	32 GB	48 GB

See “ServiceDesk scalability” on page 44.

Server configuration options for ServiceDesk

The ServiceDesk installation requires that you dedicate certain servers: a Symantec Management Platform, a ServiceDesk server, and a SQL Server.

See “System requirements for ServiceDesk” on page 59.

The server configuration that you use for a ServiceDesk installation depends on your environment, datacenter design, and budget.

Requirements for server configurations	A server configuration is valid if it meets the following requirements: ■ Microsoft SQL Server is installed on either a 32-bit server or a 64-bit server. Symantec recommends that you use a 64-bit server. ■ The Symantec Management Platform and the ServiceDesk Solution software are installed on a 64-bit server. ■ ServiceDesk is installed on a 64-bit server. Separate from the Symantec Management Platform
Typical server configurations	The most commonly-used configurations are as follows: ■ SQL Server is installed off-box for both the Symantec Management Platform and ServiceDesk. See Figure 4-1. ■ The Symantec Management Platform and ServiceDesk share an off-box SQL Server installation. See Figure 4-2.

Additional server configurations	Examples of additional configurations are as follows: ■ SQL Server is installed off-box for either the Symantec Management Platform or ServiceDesk. ■ SQL Server is installed on-box for either the Symantec Management Platform or ServiceDesk, or both. ■ One of the applications uses an on-box installation of SQL Server and shares it with the other application. ■ One of the applications uses an on-box installation of SQL Server and the other application uses an off-box installation of SQL Server.
Unsupported server configurations	Symantec does not support the following server configuration: ■ Symantec Management Platform with ServiceDesk Solution software installed on the same server as the ServiceDesk application software. **Note:** The Symantec Management Platform with ServiceDesk Solution must be installed to a separate server than the actual ServiceDesk application server.

Figure 4-1 Both Symantec Management Platform and ServiceDesk have their own off-box SQL Server

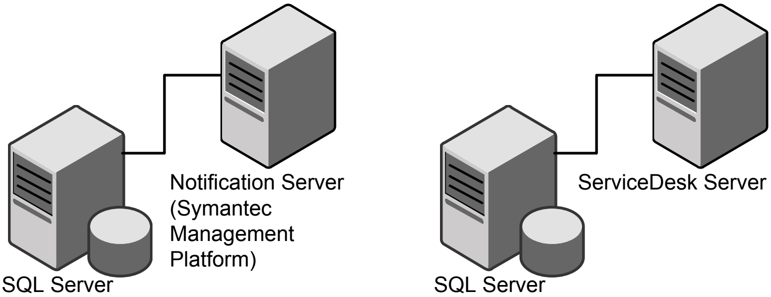
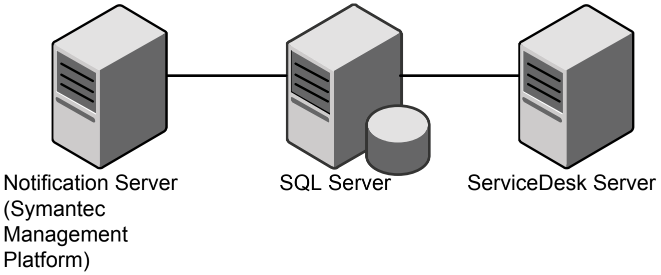


Figure 4-2 Symantec Management Platform and ServiceDesk share an off-box SQL Server



ServiceDesk 7.5 support matrix

The support matrix provides an overview of the primary ServiceDesk components and their supported operating systems. It displays the versions of the operating systems that are supported and the versions that are not supported in ServiceDesk 7.5.

See "System requirements for ServiceDesk" on page 59.

Table 4-13 ServiceDesk support matrix

Component	Supported in ServiceDesk 7.5	Support new to ServiceDesk 7.5	Not Supported in ServiceDesk 7.5
Symantec Management Platform (for ServiceDesk)	■ 7.5 ■ 7.1 SP2	N/A	■ 7.1 ■ 7.1 SP1
ServiceDesk Server/Process Manager portal operating system (OS)	■ Windows Server 2008 R2 SP1	N/A	■ Windows Server 2003 (all versions) ■ Windows Server 2008 (pre-R2) ■ Windows Server 2008 R2

Table 4-13 ServiceDesk support matrix *(continued)*

Component	Supported in ServiceDesk 7.5	Support new to ServiceDesk 7.5	Not Supported in ServiceDesk 7.5
Microsoft SQL Server	▪ Microsoft SQL Server 2005 SP4 ▪ Microsoft SQL Server 2008 SP2 ▪ Microsoft SQL Server 2008 SP3 ▪ Microsoft SQL Server 2008 R2 SP1 ▪ Microsoft SQL Server 2008 R2 SP2 ▪ Microsoft SQL Server 2012	▪ Microsoft SQL Server 2008 SP3 ▪ Microsoft SQL Server 2008 R2 SP2 ▪ Microsoft SQL Server 2012	▪ Microsoft SQL Server 2005 SP2 ▪ Microsoft SQL Server 2005 SP3 ▪ Microsoft SQL Server 2008 ▪ Microsoft SQL Server 2008 SP1
Workflow Designer operating system (OS)	▪ Windows XP SP3 x86 ▪ Windows 7 x86 and x64 ▪ Windows 7 SP1 x86 and x64 ▪ All ServiceDesk Server supported OS versions	N/A	▪ Windows XP SP2 ▪ Windows Vista SP1 ▪ Windows Vista SP2 x86 and x64
Process Manager portal browsers	▪ Microsoft Internet Explorer versions 7, 8, and 9 **Note:** Active Directory auto-authentication is only supported with Internet Explorer. ▪ Firefox version 13 and later ▪ Google Chrome version 17 and later ▪ Safari version 5 and later	N/A	N/A

System requirements for ServiceDesk

ServiceDesk requires that you dedicate certain servers.

See "About developing your ServiceDesk installation plan" on page 40.

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

See "Server configuration options for ServiceDesk" on page 55.

Table 4-14 The dedicated servers that ServiceDesk requires

Server	Description
Symantec Management Platform	ServiceDesk requires a 7.5 instance or a 7.1 SP2 instance of the Symantec Management Platform. See "ServiceDesk requirements for the Symantec Management Platform" on page 59.
ServiceDesk server	The ServiceDesk server is a 64-bit server on which you install the Workflow Platform and the ServiceDesk modules. This server might also be referred to as the Process Manager server or the Workflow Server. This server cannot contain an installation of Helpdesk Solution. See "System requirements for the ServiceDesk server" on page 60.
SQL Server	The Process Manager databases must reside on a SQL Server. Symantec recommends that ServiceDesk has its own dedicated off-box SQL Server. See "System requirements for the SQL Server" on page 63. See "About supported SQL Server collations for the Process Manager database" on page 64.

See "Requirements for the ServiceDesk client computers" on page 64.

See "Installing the ServiceDesk application software" on page 90.

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

ServiceDesk requirements for the Symantec Management Platform

ServiceDesk requires a 7.1 SP2 instance of the Symantec Management Platform to be installed and running. The Symantec Management Platform must always be installed on its own 64-bit server.

Table 4-15 ServiceDesk requirements for the Symantec Management Platform

Item	Requirement
Hardware and base software	For information about the Symantec Management Platform 7.1 SP2 hardware and the software requirements, see the chapter *Performance and scalability recommendations for IT Management Suite* in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide. For information about the Symantec Management Platform 7.5 hardware and the software requirements, see the chapter *System requirements for the Symantec Management Platform* in the Altiris™ IT Management Suite 7.5 Installation and Upgrade Guide.
Symantec Management Platform	A 7.1 SP2 instance of the Symantec Management Platform must be installed and running. The installation of your instance of the Symantec Management Platform is managed through the Symantec Installation Manager.
Altiris Configuration Management Database Solution (CMDB Solution)	If the Configuration Management Database Solution is not already installed, it is included in the installation of the ServiceDesk solution software. You do not need to perform a separate installation.

See "System requirements for ServiceDesk" on page 59.

System requirements for the ServiceDesk server

The ServiceDesk software is installed on the ServiceDesk server. This server cannot contain an installation of Helpdesk Solution.

When you install the ServiceDesk software and SQL Server on different servers, the servers must meet the following requirements:

- Both servers must be members of the same domain.
- This configuration must be installed in an Active Directory environment.

Table 4-16 System requirements for the ServiceDesk server

Item	Requirement
Server and processor	Multi-core or multiple processors, 64-bit
RAM	▪ Minimum: 8 GB (recommended for test servers only) ▪ Minimum recommended: 16 GB ▪ Preferred: 32 GB
Operating system	Windows Server 2008 R2 SP1, 64 bit

Table 4-16 System requirements for the ServiceDesk server *(continued)*

Item	Requirement
Network configuration	■ IP v4 ■ Static IP address ■ Name resolution services (DNS) ■ Internet connectivity ■ Connectivity to the Symantec Management Platform server ■ Gigabit Network Interface Controller (GB NIC)
Installation account	ServiceDesk requires an installation account: ■ **Windows** (Windows Integrated Security) Use a domain account with the *sysadmin* server role on the target SQL instance. ■ **SQL** (Microsoft SQL Server Security) Use a SQL account with the *sysadmin* server role for that target SQL instance. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Operation service account	ServiceDesk requires a run-time service account. ■ **Windows** (Windows Integrated Security) Use a domain service account that is set up in that SQL instance. This account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database. **Note:** This authentication method is the recommended authentication method. Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security. ■ **SQL** (Microsoft SQL Server Security) Use an account in the target SQL instance. This account is added to the *db_owner* role on the Process Manager database. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Email account	■ Primary email account for the ServiceDesk mailbox for monitoring the system and sending email from the system ■ SMTP server connectivity ■ (Optional) POP or IMAP mailbox for monitoring

Table 4-16 System requirements for the ServiceDesk server *(continued)*

Item	Requirement
SQL Server components	The ServiceDesk server requires the SQL Server ADOMD.NET. This SQL Server component is a Microsoft .NET Framework data provider. It facilitates communication with the Microsoft SQL Server Analysis Services. If SQL Server is installed on a server that is separate from the ServiceDesk server (off-box), the ServiceDesk server requires the following SQL Server components: ■ SQL Management Objects (SMO) site ■ SQL Server Analysis Management Objects (AMO) ■ Microsoft ADOMD.NET ■ SQL Native client This component is a prerequisite for installing the SQL Management Objects. See "Installing SQL Server support components on the ServiceDesk server" on page 97.
Microsoft Internet Information Services (IIS)	IIS 7 (IIS 6 Management Compatibility mode)
.NET Framework	.NET 3.5 with ASP.NET
Internet browser	ServiceDesk is intended to work with all of the major Internet browsers. We have tested ServiceDesk with the following browsers: ■ Microsoft Internet Explorer versions 7, 8, and 9 **Note:** Active Directory auto-authentication is only supported with Internet Explorer. ■ Firefox version 13 and later ■ Google Chrome version 17 and later ■ Safari version 5 and later

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

See "Server configuration options for ServiceDesk" on page 55.

See "System requirements for ServiceDesk" on page 59.

This instruction is a step in the following migration processes:

See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

See "Migrating from ServiceDesk 7.1x" on page 75.

See "Migrating from ServiceDesk 7.0" on page 73.

See "Migrating from Helpdesk Solution 6.x to ServiceDesk" on page 71.

System requirements for the SQL Server

ServiceDesk requires an installation of Microsoft SQL Server.

When you install the ServiceDesk software and SQL Server on different servers, the servers must meet the following requirements:

- Both servers must be members of the same domain.
- This configuration must be installed in an Active Directory environment.

Table 4-17 System requirements for the SQL Server

Item	Requirement
Processor	32-bit or 64-bit Symantec recommends that you use a 64-bit.
Operating system	Windows Server 2008 R2 SP1
Database	Microsoft SQL Server Supported versions of SQL Server: ■ SQL Server 2005 SP4 ■ SQL Server 2008 SP2 or 2008 SP3 ■ SQL Server 2008 R2, 2008 R2 SP1, or 2008 R2 SP2 ■ SQL Server 2012
Database	ServiceDesk requires the following components of Microsoft SQL Server: ■ SQL Server Reporting Services ■ SQL Server Analysis Services
Additional requirements	When you use one SQL Server for both the Symantec Management Platform and the ServiceDesk software, follow the Symantec Management Platform's SQL Server requirements. For information about the Symantec Management Platform 7.1 P2 recommended hardware configurations, see the chapter *Performance and scalability recommendations for IT Management Suite* in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide. For information about the Symantec Management Platform 7.5 recommended hardware configurations, see the chapter *System requirements for the Symantec Management Platform* in the Altiris™ IT Management Suite 7.5 Installation and Upgrade Guide.

You can use any of several configurations for setting up the Symantec Management Platform, the ServiceDesk server, and the SQL Server.

See "Server configuration options for ServiceDesk" on page 55.

See "System requirements for ServiceDesk" on page 59.

See “Before you migrate from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform version 7.5 or 7.1 SP2” on page 76.

See “Before you migrate from ServiceDesk 7.1x” on page 75.

See “Before you migrate from ServiceDesk 7.0” on page 72.

See “Before you migrate from Helpdesk Solution 6.x to ServiceDesk” on page 70.

About supported SQL Server collations for the Process Manager database

The Process Manager database supports the following SQL Server collations:

- SQL_Latin1_General_CP1_CI_AS - Latin alphabet, case insensitive, accent sensitive
  By default, the Process Manager database is created with this collation.
- SQL_Latin1_General_CP1_CS_AS - Latin alphabet, case sensitive, accent sensitive
  If during installation the user checks the option to make the database case sensitive, the Process Manager database is created with this collation.

See “System requirements for ServiceDesk” on page 59.

Requirements for the ServiceDesk client computers

The client computers access ServiceDesk from an Internet browser. ServiceDesk is intended to work with all the major Internet browsers.

We have tested ServiceDesk with the following browsers:

- Microsoft Internet Explorer versions 7, 8, and 9

  Note: Active Directory auto-authentication is only supported with Internet Explorer.

- Firefox version 13 and later
- Google Chrome version 17 and later
- Safari version 5 and later

See “System requirements for ServiceDesk” on page 59.

Chapter 5

Planning to install ServiceDesk

This chapter includes the following topics:

Installing ServiceDesk 7.5

The installation of ServiceDesk requires that you follow a specific process. The process that you follow depends on your situation.

Table 5-1 Scenarios for installing ServiceDesk 7.5

Scenario	Description
New installation of ServiceDesk	■ You plan install ServiceDesk 7.5 along with a 7.5 instance or a 7.1 SP2 instance of the Symantec Management Platform. ■ You do not have ServiceDesk or any instance of the Symantec Management Platform installed in your environment. See "Installing ServiceDesk for the first time" on page 66.

Table 5-1 Scenarios for installing ServiceDesk 7.5 *(continued)*

Scenario	Description
New installation of ServiceDesk in an environment with an existing instance of the Symantec Management Platform 7.5 or 7.1 SP2	■ You plan to install ServiceDesk 7.5. ■ You have already implemented a 7.5 instance or a 7.1 SP2 instance of the Symantec Management Platform in your environment. See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

Installing ServiceDesk for the first time

Use these instructions if you plan to install ServiceDesk for the first time. ServiceDesk 7.5 is compatible with Symantec Management Platform version 7.5 and 7.1 SP2.

Before you begin your installation of ServiceDesk 7.5, consider the following:

See "About developing your ServiceDesk installation plan" on page 40.

See "Recommendations for scaling the ServiceDesk server and its dedicated SQL Server" on page 46.

See "System requirements for ServiceDesk" on page 59.

See "Installing ServiceDesk 7.5" on page 65.

Table 5-2 Process for installing ServiceDesk for the first time

Step	Process	Description
Step 1	Install the Symantec Management Platform and the ServiceDesk Solution software on the Symantec Management Platform server.	Use Symantec Installation Manager (SIM) to install the Symantec Management Platform product and the ServiceDesk Solution software. See "Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server" on page 80.
Step 2	(Optional) Populate the Configuration Management Database (CMDB)	ServiceDesk uses some of the configuration items (resources) that are defined in the CMDB. Although you can use ServiceDesk without the CMDB data, it limits the amount of information that can be included in incidents. See "About populating the CMDB for ServiceDesk" on page 28.

Table 5-2 Process for installing ServiceDesk for the first time *(continued)*

Step	Process	Description
Step 3	Install the ServiceDesk application software.	Use the ServiceDesk Installation and Configuration Wizard to install the Workflow Platform and the ServiceDesk modules. See "Installing the ServiceDesk application software" on page 90.
Step 4	(Optional) Install the Screen Capture Utility on the client computers.	Install the Screen Capture utility. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2

Use these instructions if you plan to install ServiceDesk on an existing instance of the Symantec Management Platform. ServiceDesk 7.5 is compatible with Symantec Management Platform version 7.5 and 7.1 SP2.

Before you begin installing ServiceDesk 7.5, consider the following:

See "About developing your ServiceDesk installation plan" on page 40.

See "Recommendations for scaling the ServiceDesk server and its dedicated SQL Server" on page 46.

See "System requirements for ServiceDesk" on page 59.

See "Installing ServiceDesk 7.5" on page 65.

Table 5-3 Process for installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2

Step	Process	Description
Step1	Install the ServiceDesk solution software on the Symantec Management Platform.	Use Symantec Installation Manager (SIM) to install the ServiceDesk solution software on the Symantec Management Platform. See "Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server" on page 80.
Step 2	(Optional) Populate the Configuration Management Database (CMDB)	ServiceDesk uses some of the configuration items (resources) that are defined in the CMDB. Although you can use ServiceDesk without the CMDB data, it limits the amount of information that can be included in incidents. See "About populating the CMDB for ServiceDesk" on page 28.
Step 3	Install the ServiceDesk application software on the ServiceDesk server.	Install the ServiceDesk application software on the ServiceDesk server. See "Installing the ServiceDesk application software" on page 90.
Step 4	(Optional) Install the Screen Capture Utility on the client computers.	Install the Screen Capture Utility. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Chapter 6

Planning to migrate to ServiceDesk 7.5

This chapter includes the following topics:

Migrating to ServiceDesk 7.5

The migration to ServiceDesk requires that you follow a specific process. The process that you follow depends on your previous version.

Table 6-1 Scenarios for migrating to ServiceDesk 7.5

Version	Description
Helpdesk Solution 6.x	Migrate to ServiceDesk and migrate your Altiris 6.x infrastructure to the Symantec Management Platform. See "Migrating from Helpdesk Solution 6.x to ServiceDesk" on page 71.
ServiceDesk 7.0	Migrate to ServiceDesk and migrate your instance of the Symantec Management Platform. See "Migrating from ServiceDesk 7.0" on page 73.
ServiceDesk 7.1	Migrate to ServiceDesk and upgrade your instance of the Symantec Management Platform. See "Migrating from ServiceDesk 7.1x" on page 75.
ServiceDesk 7.1 SP1	Migrate to ServiceDesk and upgrade your instance of the Symantec Management Platform. See "Migrating from ServiceDesk 7.1x" on page 75.
ServiceDesk 7.1 SP2.	Migrate to ServiceDesk without upgrading your instance of the Symantec Management Platform version 7.1 SP2. See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

Before you migrate from Helpdesk Solution 6.x to ServiceDesk

You can migrate from Helpdesk Solution 6.x.

Before you do this migration, consider the following:

- Before you migrate, you must set up a ServiceDesk server and install ServiceDesk 7.5. You can migrate data from your Helpdesk Solution over to your ServiceDesk 7.5.
  Symantec does not support an in-place same-server upgrade from Helpdesk Solution to ServiceDesk 7.5. ServiceDesk does not install over Helpdesk Solution.
  See "About developing your ServiceDesk installation plan" on page 40.
- Although you can install a new SQL server, it is not required. Your ServiceDesk SQL server must meet the requirements of ServiceDesk 7.5 before you install your Process Manager database.

See “System requirements for the SQL Server” on page 63.

- You must migrate your Altiris 6.x product to an instance of the Symantec Management Platform. ServiceDesk 7.5 is compatible with versions 7.5 and 7.1 SP2.
  For information about installing a 7.5 instance of the Symantec Management Platform, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.
  For information about installing a 7.1 SP2 instance of the Symantec Management Platform, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

For instructions on migrating from Helpdesk Solution 6.x, see the following:

See “Migrating from Helpdesk Solution 6.x to ServiceDesk” on page 71.

Migrating from Helpdesk Solution 6.x to ServiceDesk

Use these instructions to migrate from Helpdesk Solution 6.x and migrate to an instance of the Symantec Management Platform.

Before you begin migrating to ServiceDesk 7.5, consider the following:

See “Before you migrate from Helpdesk Solution 6.x to ServiceDesk” on page 70.

See “Migrating to ServiceDesk 7.5” on page 69.

Table 6-2 Process for migrating from Helpdesk Solution 6.x

Step	Process	Description
Step 1	Install the Symantec Management Platform and the ServiceDesk solution software on the Symantec Management Platform.	Use Symantec Installation Manager (SIM) to install the Symantec Management Platform and ServiceDesk solution software. See “Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server” on page 80.
Step 2	Migrate your Altiris 6.x data to the Symantec Management Platform.	Migrate any Altiris 6.x data to your instance of the Symantec Management Platform. For information about migrating Altiris 6.x data to a 7.5 instance of the Symantec Management Platform, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6.x to 7.5. For information about migrating Altiris 6.x data to a 7.1 SP2 instance of the Symantec Management Platform, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6.x to 7.1 SP2.

Table 6-2 Process for migrating from Helpdesk Solution 6.x *(continued)*

Step	Process	Description
Step 3	(Optional) Populate the Configuration Management Database (CMDB).	ServiceDesk uses some of the configuration items (resources) that are defined in the CMDB. Although you can use ServiceDesk without the CMDB data, it limits the amount of information that can be included in incidents. See "About populating the CMDB for ServiceDesk" on page 28.
Step 4	Set up the ServiceDesk server(s).	Set up the ServiceDesk server. See "System requirements for the ServiceDesk server" on page 60.
Step 5	Install the ServiceDesk application software on the ServiceDesk server.	Install the ServiceDesk application software on the ServiceDesk server. See "Installing the ServiceDesk application software" on page 90.
Step 6	Migrate your data from Helpdesk Solution to ServiceDesk.	Although you cannot upgrade Helpdesk Solution directly, you can use certain Helpdesk Solution data in ServiceDesk. Migrate the Helpdesk Solution data to the ServiceDesk. See "About migrating data from Helpdesk Solution 6.x" on page 288.
Step 7	(Optional) Install the Screen Capture Utility on the client computers.	ServiceDesk provides a Screen Capture utility that lets users capture images of their computer screens. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Before you migrate from ServiceDesk 7.0

You can migrate from ServiceDesk 7.0.

Before you do this migration, consider the following:

- Before you migrate, you must set up a new ServiceDesk server and install Service 7.5. You can migrate data from your existing ServiceDesk server over to your new ServiceDesk server.
  Symantec does not support an in-place same-server upgrade to ServiceDesk 7.5.
  See "About developing your ServiceDesk installation plan" on page 40.

- Although you can install a new ServiceDesk SQL server, it is not required. Your ServiceDesk SQL server must meet the requirements of ServiceDesk 7.5 before you install your new Process Manager database.

  See "System requirements for the SQL Server" on page 63.
- You must migrate your instance of the Symantec Management Platform 7.0 to a later version. ServiceDesk 7.5 is compatible with versions 7.5 and 7.1 SP2.

  For information about installing a 7.5 instance of the Symantec Management Platform, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

  For information about installing a 7.1 SP2 instance of the Symantec Management Platform, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

For instructions on migrating from ServiceDesk 7.0, see the following:

See "Migrating from ServiceDesk 7.0" on page 73.

Migrating from ServiceDesk 7.0

Use these instructions if you plan to migrate from ServiceDesk 7.0 and migrate your instance of the Symantec Management Platform 7.0 to a new version.

Before you begin migrating to ServiceDesk 7.5, consider the following:

See "Before you migrate from ServiceDesk 7.0" on page 72.

See "Migrating to ServiceDesk 7.5" on page 69.

Table 6-3 Process for migrating from ServiceDesk 7.0

Step	Process	Description
Step 1	Install the Symantec Management Platform and the ServiceDesk solution software on the Symantec Management Platform server	Use Symantec Installation Manager (SIM) to install the ServiceDesk solution software on the Symantec Management Platform. See "Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server" on page 80.

Table 6-3 Process for migrating from ServiceDesk 7.0 *(continued)*

Step	Process	Description
Step 2	Migrate your data to the newer instance of the Symantec Management Platform.	Migrate any 7.0 data to your newer instance of the Symantec Management Platform. For information about migrating data to a 7.5 instance of the Symantec Management Platform, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.5. For information about migrating data to a 7.1 SP2 instance of the Symantec Management Platform, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1 SP2.
Step 3	(Optional) Populate the Configuration Management Database (CMDB).	ServiceDesk uses some of the configuration items (resources) that are defined in the CMDB. Although you can use ServiceDesk without the CMDB data, it limits the amount of information that can be included in incidents. See "About populating the CMDB for ServiceDesk" on page 28.
Step 4	Set up your new ServiceDesk 7.5 server(s).	Set up the ServiceDesk server. See "System requirements for the ServiceDesk server" on page 60.
Step 5	Install the ServiceDesk application software on the ServiceDesk server.	Install the ServiceDesk application software on the ServiceDesk server. See "Installing the ServiceDesk application software" on page 90.
Step 6	(Optional) Install the Screen Capture Utility on the client computers.	Install the Screen Capture utility. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Before you migrate from ServiceDesk 7.1x

You can migrate from ServiceDesk 7.1x.

Before you do this migration, consider the following:

- Before you migrate, you must set up a new ServiceDesk server and install ServiceDesk 7.5. You can migrate data from your existing ServiceDesk server over to your new ServiceDesk server.
  Symantec does not support an in-place same-server upgrade to ServiceDesk 7.5.
  See "About developing your ServiceDesk installation plan" on page 40.
- Although you can install a new ServiceDesk SQL server, it is not required. Your ServiceDesk SQL server must meet the requirements of ServiceDesk 7.5 before you install your new Process Manager database.
  See "System requirements for the SQL Server" on page 63.
- You may need to upgrade your instance of the Symantec Management Platform 7.1x. ServiceDesk 7.5 is compatible with versions 7.5 and 7.1 SP2.
  For more information about upgrading to a 7.5 version of the Symantec Management Platform, see the Symantec™ IT Management suite Installation and Upgrade Guide.
  For more information about upgrading to a 7.1 SP2 version of the Symantec Management Platform, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

For instructions on migrating from ServiceDesk 7.1x, see the following:

See "Migrating from ServiceDesk 7.1x" on page 75.

Migrating from ServiceDesk 7.1x

Use these instructions if you plan to migrate from ServiceDesk 7.1x and upgrade your instance of the Symantec Management Platform 7.1x.

Before you begin migrating to ServiceDesk 7.5, consider the following:

See "Before you migrate from ServiceDesk 7.1x" on page 75.

See "Migrating to ServiceDesk 7.5" on page 69.

Table 6-4 Process for migrating from ServiceDesk 7.1x

Step	Process	Description
Step 1	Upgrade the Symantec Management Platform and the ServiceDesk Solution software.	Use the Symantec Installation Manager (SIM) to upgrade your instance of the Symantec Management Platform and the ServiceDesk Solution software. See "Upgrading the Symantec Management Platform and the ServiceDesk Solution software" on page 85.
Step 2	Set up your new ServiceDesk 7.5 server(s)	Set up the ServiceDesk server. See "System requirements for the ServiceDesk server" on page 60.
Step 3	Install the ServiceDesk application software.	Install the ServiceDesk application software on the new ServiceDesk server. See "Installing the ServiceDesk application software" on page 90.
Step 4	(Optional) Install the Screen Capture Utility on the client computers.	Install the Screen Capture utility. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Before you migrate from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform version 7.5 or 7.1 SP2

You can migrate from ServiceDesk 7.1 SP2 without upgrading your 7.5 instance or 7.1 SP2 instance of the Symantec Management Platform.

Before you do this migration, consider the following:

- Before you migrate, you must set up a new ServiceDesk server and install ServiceDesk 7.5. You can migrate data from your existing ServiceDesk server over to your new ServiceDesk server.
  Symantec does not support an in-place same-server upgrade to ServiceDesk 7.5.

See "About developing your ServiceDesk installation plan" on page 40.

- Although you can install a new ServiceDesk SQL server, it is not required. Your ServiceDesk SQL server must meet the requirements of ServiceDesk 7.5 before you install your new Process Manager database.
  See "System requirements for the SQL Server" on page 63.
- You do not need to upgrade your instance of the Symantec Management Platform 7.5 or 7.1 SP2.

For instructions on migrating from ServiceDesk 7.1 SP2, see the following:

See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2

Use these instructions if you plan to migrate from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform. ServiceDesk 7.5 is compatible with Symantec Management Platform version 7.5 and 7.1 SP2.

Before you begin migrating to ServiceDesk 7.5, consider the following:

See "Before you migrate from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 76.

See "Migrating to ServiceDesk 7.5" on page 69.

Table 6-5 Process for migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.5 or7.1 SP2

Step	Process	Description
Step 1	Upgrade the ServiceDesk solution software on the Symantec Management Platform.	Use the Symantec Installation Manager (SIM) to upgrade the ServiceDesk Solution software on the Symantec Management Platform. See "Upgrading the Symantec Management Platform and the ServiceDesk Solution software" on page 85.
Step 2	Set up the new ServiceDesk 7.5 server(s).	Set up the ServiceDesk server. See "System requirements for the ServiceDesk server" on page 60.

Table 6-5 Process for migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.5 or7.1 SP2 *(continued)*

Step	Process	Description
Step 3	Install the ServiceDesk application software on the ServiceDesk server.	Install the ServiceDesk application software on the ServiceDesk server. See "Installing the ServiceDesk application software" on page 90.
Step 4	(Optional) Install the Screen Capture Utility on the client computers.	Install the Screen Capture Utility. See "About installing the Screen Capture utility" on page 141.

After you complete the installation and before you start to use ServiceDesk, complete the steps for configuring ServiceDesk.

See "Configuring ServiceDesk" on page 147.

Section 3

Installing ServiceDesk

Chapter 7

Installing ServiceDesk

This chapter includes the following topics:

Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server

You can install the ServiceDesk Solution software at the same time as the Symantec Management Platform. You can install the Symantec Management Platform first and then later install the ServiceDesk Solution software on the Symantec Management Platform. You install the Symantec Management Platform and the ServiceDesk Solution software with an installation utility called the Symantec Installation Manager (SIM).

After you install the ServiceDesk Solution software you can download the ServiceDesk installation file on the ServiceDesk server. After you download the installation file you can then install the ServiceDesk application software.

See "Downloading the ServiceDesk installation file" on page 98.

See "Installing the ServiceDesk application software" on page 90.

This instruction is a step in the following installation processes:

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

This instruction is a step in the following migration processes:

See "Migrating from ServiceDesk 7.0" on page 73.

See "Migrating from Helpdesk Solution 6.x to ServiceDesk" on page 71.

To install the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server

1 Install the Symantec Installation Manager (SIM) on the server on which you plan to install the Symantec Management Platform.

  For more information about installing the Symantec Management Platform version 7.5, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

  For more information about installing the Symantec Management Platform version 7.1 SP2, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

2 Launch the **Symantec Installation Manager**.

3 On the **Install New Products** page, in the **Filter by: Product Type** drop-down list, click **None** to see all products.

4 In the **Available Products** pane, do one of the following actions:

Install the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Server.	Check **Symantec ServiceDesk Solution 7.5** and then click **Next**. When you check **Symantec ServiceDesk Solution 7.5**, the Symantec Management Platform and Altiris CMDB Solution are checked automatically.
Install the ServiceDesk Solution software on your Symantec Management Platform.	Check **Symantec ServiceDesk Solution 7.5** and then click **Next**.

Note: If **Symantec ServiceDesk Solution 7.5** does not appear in the list of products, make sure that SIM points to the correct Product Listing (pl.xml) file. For more information, see the section *Other things to know* in the Symantec™ ServiceDesk 7.5 Release Notes.

5 On the **Optional Installations** page select any of the following components that you want to install and then click **Next:**

Install Documentation	Lets you install the documentation for ServiceDesk. The **Install Documentation** check box is checked by default.
Install Language Support	Lets you install language packs for ServiceDesk.

Install Migration Wizard

Lets you install the migration wizard.

The migration wizard is used to migrate data from the Symantec Management Platform 7.0 or Notification Server 6.x to the Symantec Management Platform 7.1 SP2.

The migration wizard does not migrate data from Helpdesk Solution or ServiceDesk 7.x to ServiceDesk 7.5.

- For more information on migrating data from ServiceDesk 7.x to ServiceDesk 7.5, see the Symantec ServiceDesk 7.5 Release Notes.
- For more information on migrating data from Helpdesk Solution to ServiceDesk 7.5:
  See “About migrating data from Helpdesk Solution 6.x” on page 288.

For more information on migrating data from Symantec Management Platform 7.0 to Symantec Management Platform 7.5, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.5.

For more information on migrating data from Symantec Management Platform 6.x to Symantec Management Platform 7.5, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6.x to 7.5.

For more information on migrating data from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 SP2, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1 SP2.

For more information on migrating data from Notification Server 6.x to Symantec Management Platform 7.1 SP2, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6x to 7.1 SP2.

6. On the **Install Location** page, select the drive on which you want to install the Symantec Management Platform products. Then, select the folder to in which to install them. Then click **Next**.

7. On the **End User License Agreement** page, click **I accept the terms in the license agreements** and then click **Next**.

8. On the **Contact Information** page, type your contact information and then click **Next**.

9. On the **Install Readiness Check** page, verify that your server meets the minimum requirements and click **Next**.

10. On the **Notification Server Configuration** page, configure Notification Server and click **Next**.

11. On the **Database Configuration** page, configure the database and click **Next**.

12. On the **Review Installation Details** page, review the details of the installation and perform one of the following actions:

After the install files are downloaded and validated, click **Begin install** .	Install the Symantec Management Platform, the CMDB, and the ServiceDesk Solution software. Install the ServiceDesk Solution software on your existing instance of the Symantec Management Platform.
Click **Back**.	Go back and modify the details of your installation

13. (Optional) On the **Back up Notification Server Cryptographic Keys** page, perform one of the following actions:

Back up Notification Server cryptographic keys.	■ Type or browse for a location to back up Notification Server cryptographic keys. ■ Type a password and confirm the password. ■ Click **Next**. ■ In the **Symantec Installation Manager** dialog box, click **OK**.

Click **Skip**.	If you do not back up Notification Server cryptographic keys during installation, you can use the Symantec Installation Manager (SIM) to back them up later. ■ Launch the **Symantec Installation Manager**. ■ On the **Install Products** page, click **Back up Notification Server cryptographic keys**.

14 (Optional) On the **Product Licensing** page, click **Install Licenses** and install your licenses.

If you do not install licenses, trial licenses are applied. You can use the Symantec Installation Manager (SIM) to install licenses at any time.

For more information about licenses for the Symantec Management Platform 7.5 and ServiceDesk 7.5, see topics about licenses in the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

For more information about licenses for the Symantec Management Platform 7.1 SP2 and ServiceDesk 7.5, see topics about licenses in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide.

15 When you are finished, click **Next**.

16 On the **Installation Complete** page, click **Finish**.

Upgrading the Symantec Management Platform and the ServiceDesk Solution software

You can upgrade the ServiceDesk Solution software at the same time as the Symantec Management Platform. You can upgrade the Symantec Management Platform first and then later upgrade the ServiceDesk Solution software. You can upgrade the ServiceDesk Solution software without upgrading the Symantec Management Platform. You upgrade the Symantec Management Platform and the ServiceDesk Solution software with an installation utility called the Symantec Installation Manager (SIM).

For more information about upgrading to Symantec Management Platform version 7.5, see the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

For more information about upgrading to Symantec Management Platform version 7.1 SP2, see the Symantec™ Management Platform 7.1 SP2 Installation Guide.

After you upgrade the ServiceDesk Solution software, you can download the ServiceDesk installation file on your new ServiceDesk server. After you download the installation file you can then install the ServiceDesk application software.

See "Downloading the ServiceDesk installation file" on page 98.

See "Installing the ServiceDesk application software" on page 90.

This instruction is a step in the following migration processes:

See "Migrating from ServiceDesk 7.1x" on page 75.

See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

To upgrade the Symantec Management Platform and the ServiceDesk Solution software

1. Launch the **Symantec Installation Manager**.
2. On the **Install Products** page, click **Install new products**.
3. On the **Install New Products** page, in the **Filter by: Product Type** drop-down list, click **None** to see all products.
4. In the **Available Products** pane, do one of the following actions:

Upgrade the Symantec Management Platform, CMDB, and ServiceDesk Solution software.	Perform the necessary actions as follows and then click **Next**: ■ Check **Symantec ServiceDesk Solution 7.5**. ■ If you want to upgrade the Symantec Management Platform to version 7.1 SP2, check **Symantec Management Platform 7.1 SP2**. ■ If you want to upgrade the Configuration Management Database to version 7.1 SP2, check **Altiris CMDB Solution 7.1 SP2**.
Upgrade the ServiceDesk Solution software on your Symantec Management Platform.	Check **Symantec ServiceDesk Solution 7.5** and then click **Next**.

Note: If **Symantec ServiceDesk Solution 7.5** does not appear in the list of products, make sure that SIM points to the correct Product Listing (pl.xml) file. For more information, see the section *Other things to know* in the Symantec™ ServiceDesk 7.5 Release Notes.

5 On the **Optional Installations** page check any of the following components that you want to install and then click **Next:**

Install Documentation

Lets you install the documentation for ServiceDesk.

The **Install Documentation** check box is checked by default.

Install Language Support

Lets you install language packs for ServiceDesk.

Install Migration Wizard

Lets you install the migration wizard.

The migration wizard is used to migrate data from the Symantec Management Platform 7.0 or Notification Server 6.x to the Symantec Management Platform 7.1 SP2.

The migration wizard does not migrate data from Helpdesk Solution or ServiceDesk 7.x to ServiceDesk 7.5.

- For more information on migrating data from ServiceDesk 7.x to ServiceDesk 7.5, see Symantec ServiceDesk 7.5 Release Notes
- For more information on migrating data from Helpdesk Solution to ServiceDesk 7.5:

  See "About migrating data from Helpdesk Solution 6.x" on page 288.

For more information on migrating data from Symantec Management Platform 7.0 to Symantec Management Platform 7.5, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.5.

For more information on migrating data from Symantec Management Platform 6.x to Symantec Management Platform 7.5, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6.x to 7.5.

For more information on migrating data from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 SP2, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1 SP2.

For more information on migrating data from Notification Server 6.x to Symantec Management Platform 7.1 SP2, see the Altiris™ IT Management Suite from Symantec™ Migration Guide version 6x to 7.1 SP2.

6. On the **Install Location** page, select the drive on which you want to install the Symantec Management Platform products. Select the folder to in which to install them. Then click **Next**.
7. On the **End User License Agreement** page, click **I accept the terms in the license agreements** and then click **Next**.
8. On the **Contact Information** page, type your contact information and then click **Next**.
9. On the **Install Readiness Check** page, verify that your server meets the minimum requirements and click **Next**.
10. On the **Notification Server Configuration** page, configure Notification Server and click **Next**.
11. On the **Database Configuration** page, configure the database and click **Next**.
12. On the **Review Installation Details** page, review the details of the installation and perform one of the following actions:

After the install files are downloaded and validated, click **Begin install**.	Upgrade the Symantec Management Platform, the CMDB, and the ServiceDesk Solution software. Upgrade the ServiceDesk Solution software on your existing instance of the Symantec Management Platform.
Click **Back**.	Go back and modify the details of your upgrade.

13. (Optional) On the **Back up Notification Server Cryptographic Keys**, perform one of the following actions:

Back up Notification Server cryptographic keys.	■ Type or browse for a location to back up Notification Server cryptographic keys. ■ Type a password and confirm the password. ■ Click **Next**. ■ In the **Symantec Installation Manager** dialog box, click **OK**.

Click **Skip**.	If you do not back up Notification Server cryptographic keys during installation, you can use the Symantec Installation Manager (SIM) to back them up later. ■ Launch the **Symantec Installation Manager**. ■ On the **Install Products** page, click **Back up Notification Server cryptographic keys**.

14. (Optional) On the **Product Licensing** page, click **Install Licenses**.

    If you do not install licenses, trial licenses are applied. You can use the Symantec Installation Manager (SIM) to install licenses at any time.

    For more information about licenses for the Symantec Management Platform 7.5 and ServiceDesk 7.5, see topics about licenses in the Symantec™ IT Management Suite 7.5 Installation and Upgrade Guide.

    For more information about licenses for the Symantec Management Platform 7.1 SP2 and ServiceDesk 7.5, see topics about licenses in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide.

15. When you are finished, click **Next**.
16. On the **Installation Complete** page, click **Finish**.

Installing the ServiceDesk application software

The ServiceDesk application software is installed on the ServiceDesk server. It cannot be installed on the same server as Helpdesk Solution.

Before you begin, ensure that the following prerequisites are met:

- The ServiceDesk solution software has been installed or upgraded on the Symantec Management Platform.
  See "Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server" on page 80.
  See "Upgrading the Symantec Management Platform and the ServiceDesk Solution software" on page 85.
- The ServiceDesk server, the SQL server, and the ServiceDesk client computers are set up.
  See "System requirements for ServiceDesk" on page 59.

Table 7-1 Process for installing the ServiceDesk application software

Step	Action	Description
Step 1	Collect the information that you need for the ServiceDesk installation and initial configuration.	During the ServiceDesk installation and initial configuration, you must enter certain information about your environment and the type of installation that you plan to perform. See "Information to collect for your ServiceDesk installation" on page 92.
Step 2	Prepare the ServiceDesk server for ServiceDesk installation.	Before you download the ServiceDesk installation file on the ServiceDesk server, specific features of the base operating system must be enabled and configured. For an off-box SQL Server configuration, additional components must be installed on the ServiceDesk server. See "Setting up the ServiceDesk server" on page 95.
Step 3	Download the ServiceDesk installation file.	In the Symantec Management Console, you can access a page that lets you download the ServiceDesk installation file. Download this file to any server on which you plan to install the ServiceDesk application software. See "Downloading the ServiceDesk installation file" on page 98.
Step 4	Install the Workflow Platform and the ServiceDesk modules.	Run the ServiceDesk installation file that you downloaded, which opens the ServiceDesk Installation and Configuration Wizard. First, the wizard lets you install the Workflow Platform, which includes the Process Manager database, the Process Manager portal, and Workflow Designer. Then the wizard let you install the ServiceDesk modules. See "ServiceDesk Installation and Configuration Wizard" on page 99. See "Installing the Workflow Platform and the ServiceDesk modules" on page 103.

This instruction is a step in the following installation processes:

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

This instruction is a step in the following migration processes:

See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

See "Migrating from ServiceDesk 7.1x" on page 75.

See "Migrating from ServiceDesk 7.0" on page 73.

See "Migrating from Helpdesk Solution 6.x to ServiceDesk" on page 71.

Information to collect for your ServiceDesk installation

During the ServiceDesk installation and initial configuration, you must enter certain information about your environment and the type of installation that you plan to perform.

See “Installing the Workflow Platform and the ServiceDesk modules” on page 103.

Collecting this information is a step in the process for installing the ServiceDesk application software.

See “Installing the ServiceDesk application software” on page 90.

Table 7-2 Information to collect for your ServiceDesk installation

Item	Description	Corresponding information from your environment	Notes
Notification Server computer name	The IP address, fully qualified domain name, or common name of the computer on which the Symantec Management Platform is installed.		
Notification Server domain name	The domain name of the computer on which the Symantec Management Platform is installed.		
Symantec Management Platform computer credentials	The user name and password with which the ServiceDesk server computer can access the Symantec Management Platform computer.		
Base URL of the ServiceDesk server	The IP address and the fully qualified domain name of the ServiceDesk server computer. Should be the address that users use to access ServiceDesk.		
Data source for the Process Manager database	The IP address or the domain name of the computer on which to install the Process Manager database. It must reside on the SQL server.		

Table 7-2 Information to collect for your ServiceDesk installation *(continued)*

Item	Description	Corresponding information from your environment	Notes
Process Manager administrator	The user name and password of the administrator who can access the Process Manager portal. You must use an email account format for the user name. For example: *<admin@symantec.com>*		
Installation account and its connection authentication method	ServiceDesk requires an installation account to connect to the target SQL instance during installation only. The connection authentication method determines the type of installation account that is needed. The options are as follows: ■ **Windows** (Windows Integrated Security) authentication Use a domain account with the *sysadmin* server role on the target SQL instance. ■ **SQL** (Microsoft SQL Server Security) authentication Use an SQL account with the *sysadmin* server role for the target SQL instance. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.		

Table 7-2 Information to collect for your ServiceDesk installation *(continued)*

Item	Description	Corresponding information from your environment	Notes
Operation service account and its connection authentication method **Note:** Preferably, you should use a service account that does not change its password. You can also use a service account that includes a password change process that includes updating the ServiceDesk connection as part of the password change.	ServiceDesk requires an operation service account to connect to the target SQL instance during ServiceDesk run-time. The connection authentication method determines the type of operation service account that is needed. The options are as follows: ▪ **Windows** (Windows Integrated Security) authentication Use a domain service account that is set up in the target SQL instance. This account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database. **Note:** This authentication method is the recommended authentication method. Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security. ▪ **SQL** (Microsoft SQL Server Security) authentication Use an account in the target SQL instance. This account is added to the *db_owner* role on the Process Manager database. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.		
Mail server addresses	▪ The name of the mail server from which ServiceDesk receives inbound email. ▪ (Optional) The name of the mail server to monitor for incoming incidents. Obtain this server name if you plan to use the ServiceDesk Inbox monitoring tool.		

Table 7-2 Information to collect for your ServiceDesk installation *(continued)*

Item	Description	Corresponding information from your environment	Notes
Email addresses	■ The email address from which ServiceDesk sends notification emails. ■ (Optional) The email address and password of the mailbox to monitor for incoming incidents. Obtain this address if you plan to use the ServiceDesk Inbox monitoring tool. It should be the same as the email address for sending emails.		
Email protocol and port	The protocol and port for the email transmissions between ServiceDesk and users.		

Setting up the ServiceDesk server

The ServiceDesk server requires specific features of the base operating system to be enabled and configured. Additional components must be installed for off-box SQL Server. Skipping any of the configuration steps may result in a failed installation.

This instruction is a step in the installing the ServiceDesk application software process.

See "Installing the ServiceDesk application software" on page 90.

Table 7-3 Setting up the ServiceDesk server for ServiceDesk application software installation

Step	Action	Description
Step 1	Install and configure server roles and Web services.	Install the Application Server and the Web Server (IIS) roles on the ServiceDesk server. You must also add the **IIS 6 Management Compatibility** role service to the Web Server (IIS) role.
Step 2	Configure Internet Explorer security	Configure or disable the firewall to properly allow HTTP, HTTPS, and email protocol traffic on the ServiceDesk server.
Step 3	Install SQL Server support components.	For off-box SQL instances, ServiceDesk requires you need to install additional SQL Server components on the ServiceDesk server. See "Installing SQL Server support components on the ServiceDesk server" on page 97.

Table 7-3 Setting up the ServiceDesk server for ServiceDesk application software installation *(continued)*

Step	Action	Description
Step 4	Set up the ServiceDesk installation account.	Set up an account to use to connect to the target SQL instance during installation only. The options are as follows: ■ If using **Windows** (Windows Integrated Security) authentication: Set up a domain account with the *sysadmin* server role for the target SQL instance. ■ If using **SQL** (Microsoft SQL Server Security) authentication: Set up a SQL account with the *sysadmin* server role for the target SQL instance. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Step 5	Set up the ServiceDesk run-time service account.	Set up an account to use to connect to the target SQL instance during ServiceDesk run-time. The options are as follows: ■ If using **Windows** (Windows Integrated Security) authentication: Set up a domain service account that is set up in the target SQL instance. This account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database. **Note:** This authentication method is the recommended authentication method. Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security. ■ If using **SQL** (Microsoft SQL Server Security) authentication: Use an account in the target SQL instance. This account is added to the *db_owner* role on the Process Manager database. **Note:** If you plan to use this authentication method, the target database server must be configured to support SQL authentication.

Installing SQL Server support components on the ServiceDesk server

If the SQL Server instance is not on the same server as ServiceDesk, you must install additional SQL Server components on the ServiceDesk server. These components are part of a feature pack for Microsoft SQL Server.

See “System requirements for the ServiceDesk server” on page 60.

This task is a step in a process.

See “Setting up the ServiceDesk server” on page 95.

To install SQL Server support components on the ServiceDesk server

1. Log on to the ServiceDesk server with the ServiceDesk installation account.
2. Depending on your SQL Server version, download the correct feature pack from the following locations:

SQL Server 2005 SP4 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=20101
SQL Server 2008 SP2 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=6375
SQL Server 2008 SP3 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=27596
SQL Server 2008 R2 SP1 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=26728
SQL Server 2008 R2 SP2 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=30440
SQL Server 2012 Feature pack	http://www.microsoft.com/en-us/download/details.aspx?id=29065

3. Install the following components from the feature pack:
   - Microsoft SQL Server Native Client
   - Microsoft ADOMD.NET
   - Microsoft SQL Server Management Objects (SMO)
   - Microsoft SQL Server Analysis Management Objects (AMO)

Note: Depending on your version of SQL Server, Microsoft may require you to install additional feature pack components. For example, you may be required to install SQL Server CLR Types feature pack components before installing Microsoft SQL Server Management Objects (SMO).

Downloading the ServiceDesk installation file

The installation of the ServiceDesk solution software on the Symantec Management Platform includes the ServiceDesk installation file. You use the same installation file to install both the Workflow Platform and the ServiceDesk modules.

In the Symantec Management Console, you can access the **ServiceDesk Solution Console** page. On the **ServiceDesk Solution Console** you can access a link that lets you download the ServiceDesk installation file. To download the ServiceDesk Solution installation file, access the Symantec Management Console from any server on which you plan to install the ServiceDesk application.

See “About the ServiceDesk Solution Console page” on page 37.

This task is a step in the process for installing the ServiceDesk application software.

See “Installing the ServiceDesk application software” on page 90.

Before you begin, ensure that the ServiceDesk solution software has been installed or updated on the Notification Server computer.

See “Installing the Symantec Management Platform and ServiceDesk Solution software on the Symantec Management Platform server” on page 80.

See “Upgrading the Symantec Management Platform and the ServiceDesk Solution software” on page 85.

To download the ServiceDesk installation file

1. On the ServiceDesk server, open a browser and log on to the Symantec Management Console.
   - Open Internet Explorer
   - Type **http://*<FQDN>*/altiris/console**.
   - In the **Windows Security** dialog box, type your credentials and click **OK**.
2. In the **Symantec Management Console**, on the **Settings** menu, click **Settings > All Settings**.
3. In the left pane, expand **Settings > Service and Asset Management > ServiceDesk** and then click **ServiceDesk**.

4 On the **ServiceDesk Solution Console** page, under **Download ServiceDesk Installer**, click **Symantec.ServiceDesk.Setup.msi**.

5 In the **File Download - Security Warning** dialog box, click **Save**.

6 Save the ServiceDesk installation file to your ServiceDesk server.

ServiceDesk Installation and Configuration Wizard

The ServiceDesk Installation and Configuration Wizard guides you through the installation of the ServiceDesk application software. First, the wizard guides you through the installation of the Workflow Platform. The Workflow Platform installation includes the Process Manager database, Process Manager portal, and Workflow Designer. Then the wizard then guides you through the installation of the ServiceDesk modules.

See “Installing the Workflow Platform and the ServiceDesk modules” on page 103.

The ServiceDesk Installation and Configuration Wizard lets you configure the settings for connecting to the Symantec Management Platform. The connection to the Symantec Management Platform lets you manage your ServiceDesk Licenses and use the Configuration Management Database (CMDB). The ServiceDesk Installation and Configuration Wizard also creates the Process Manager database and configures the settings for connecting to that database.

You can use the ServiceDesk Installation and Configuration Wizard to modify your ServiceDesk installation, uninstall ServiceDesk, and uninstall Workflow.

See “About modifying your ServiceDesk installation” on page 125.

See “Uninstalling ServiceDesk from the ServiceDesk server” on page 139.

See “Uninstalling Workflow from the ServiceDesk server” on page 140.

This instruction is part of a step in the process for installing the ServiceDesk application software.

See “Installing the ServiceDesk application software” on page 90.

The main page of the ServiceDesk Installation and Configuration Wizard is the **ServiceDesk Installation and Configuration** page. This page is in the right pane and is the first page that you see whenever you open the ServiceDesk Installation and Configuration Wizard.

Table 7-4 Options on the **ServiceDesk Installation and Configuration** page

Option	Description
Run System Diagnostic **Start Program**	■ Lets you check the current system environment for installation readiness. ■ Lets you check the current system environment for previously installed components. ■ See "Running a system diagnostic" on page 122.
Install, Repair, or Remove Workflow Server and Portal **Start Program**	■ Lets you install the Workflow Platform, including Workflow Designer. ■ Lets you repair or upgrade Workflow. ■ Lets you uninstall Workflow. **Warning:** If you uninstall Workflow, you effectively uninstall ServiceDesk as well. Workflow must be installed for ServiceDesk to run.
Install, Repair, or Remove ServiceDesk **Start Program**	■ Lets you install ServiceDesk. ■ Lets you repair or upgrade ServiceDesk. ■ Lets you uninstall ServiceDesk. **Note:** If you uninstall ServiceDesk, only the ServiceDesk components are removed. Workflow is not removed.

The ServiceDesk Installation and Configuration Wizard consists of a left pane, a right pane, and a bottom pane. The **Setup Programs** pane is on the left. The current page pane is on the right. The view log and ServiceDesk version number pane is on the bottom.

The left pane or **Setup Programs** pane lets you perform all the same actions as the **ServiceDesk Installation and Configuration** page. This pane is always active no matter which page is active in the right pane.

Note: If you select any of the options in the **Setup Programs** pane, you cancel the process in which you are currently involved. Therefore, all options in the **Setup Programs** page function like the **Cancel** option at the bottom of the ServiceDesk Installation and Configuration Wizard pages.

Table 7-5 Options on the **Setup Programs** pane

Option	Description
System Diagnostic	■ Lets you check the current system environment for installation readiness. ■ Lets you check the current system environment for previously installed components. ■ See "Running a system diagnostic" on page 122.
Install, Repair, or Remove Workflow	■ Lets you install the Workflow Platform, including Workflow Designer. ■ Lets you repair or upgrade Workflow. ■ Lets you uninstall Workflow. **Warning:** If you uninstall Workflow, you effectively uninstall ServiceDesk as well. Workflow must be installed for ServiceDesk to run.
Install, Repair, or Remove ServiceDesk	■ Lets you install ServiceDesk. ■ Lets you repair or upgrade ServiceDesk. ■ Lets you uninstall ServiceDesk. **Note:** If you uninstall ServiceDesk, only the ServiceDesk components are removed. Workflow is not removed.
Back to Start Page	Lets you cancel the process in which you are currently involved and return to the **ServiceDesk Installation and Configuration** page.

The pane on the right displays the active page of the ServiceDesk Installation and Configuration Wizard. The ServiceDesk Installation and Configuration Wizard displays several general options that are available on the bottom of each active page. If the option is not active for that page, it is grayed out.

Table 7-6 Options on the bottom of the pages in the ServiceDesk Installation and Configuration Wizard

Option	Description
Cancel	Lets you cancel the installation, repair or upgrade, or removal process and returns you to the **ServiceDesk Installation and Configuration** page. If you cancel a process, you must restart it from the beginning. Depending on how far into the process you are, some of your information may be saved while other information may not be saved. Note that if you click **Cancel** during a new installation, you can click **Start Program** under **Install, Repair, or Remove ServiceDesk** to resume installation. The ServiceDesk Installation and Configuration Wizard restarts installation. If you canceled the Workflow installation, the wizard restarts Workflow installation. If you canceled ServiceDesk installation, the wizard restarts ServiceDesk installation
Back	Lets you return to the previous page of the process in which you are involved.
Next	Lets you advance to the next page of the process in which you are involved.
Finish	Lets you confirm that the process is complete and returns you to the **ServiceDesk Installation and Configuration** page. When you click **Finish**, that process is complete. When you perform a new install, it confirms that you completed that step of the process and returns you to the **ServiceDesk Installation and Configuration** page. For example, you successfully installed the Workflow Platform. On the **Installing the Workflow Server and ProcessManager Portal** page you must click **Finish** before you can continue with ServiceDesk installation.

The bottom pane displays the **View Log** link and ServiceDesk version number. The bottom pane is always active no matter which page is active in the right pane.

Table 7-7 Option and information in the bottom pane of the ServiceDesk Installation and Configuration Wizard

Option or information	Description
View Log link	Lets you view the information in the installation file. This option does not cancel the current process in which you are involved. The ServiceDesk Installation and Configuration Wizard, keeps a log file of your installation process. Click this link at any time to open the log file and review information, such as warnings or failures.
ServiceDesk version number	The version of ServiceDesk that you are in the process of installing or have installed.

Installing the Workflow Platform and the ServiceDesk modules

The installation process consists of the following two parts:

Workflow Platform installation	The ServiceDesk Installation and Configuration Wizard lets you install the Workflow Server, the Process Manager portal, the Process Manager database, and Workflow Designer. It also lets you configure the settings for the ServiceDesk server to Process Manager database connection.
ServiceDesk modules installation.	The ServiceDesk Installation and Configuration Wizard lets you install the ServiceDesk modules and configure the ServiceDesk communication settings.

This task is a step in the process for installing the ServiceDesk application software.

See "Installing the ServiceDesk application software" on page 90.

Table 7-8 Process for installing the Workflow Platform and ServiceDesk modules

Step	Action	Description
Step 1	Open the ServiceDesk Installation and Configuration Wizard.	■ Launches the ServiceDesk Installation and Configuration Wizard. The wizard runs an initial check of your ServiceDesk server to make sure that all necessary server prerequisites are met. Step 1: To open the ServiceDesk Installation and Configuration Wizard ■ For more information about the ServiceDesk Installation and Configuration Wizard, see the following instruction: See "ServiceDesk Installation and Configuration Wizard" on page 99.
Step 2 (Optional)	Run a system diagnostic	■ Lets you see which components are installed and which components remain to be installed before you begin installing the Workflow Platform. Because the ServiceDesk Installation and Configuration Wizard guides you through the complete installation process, running a system check is used more for troubleshooting purposes. Step 2: (Optional) To run a system diagnostic before Workflow Platform installation ■ For more information about the symbols and features on the **Run System Diagnostic** page, see the following instruction: See "Run System Diagnostic page" on page 123.
Step 3	Install the Workflow Platform	■ Lets you install the Workflow Server, the Process Manager database, Process Manager portal, and Workflow Designer. Step 3: To install the Workflow Platform ■ The Workflow Platform must be installed before you install the ServiceDesk modules.

Table 7-8 Process for installing the Workflow Platform and ServiceDesk modules *(continued)*

Step	Action	Description
Step 4 (Optional)	Run a system diagnostic.	- Lets you see which components are installed and which components remain to be installed before you begin installing the ServiceDesk modules. Because the ServiceDesk Installation and Configuration Wizard guides you through the complete installation process, running a system check is used more for troubleshooting purposes. Step 4: (Optional) To run a system diagnostic before ServiceDesk modules installation - For more information about the symbols and features on the **Run System Diagnostic** page, see the following instruction: See "Run System Diagnostic page" on page 123.
Step 5	Install the ServiceDesk modules.	Lets you select which ServiceDesk modules you want to install and then lets you install them. The following modules are available for you to install: - **Change Management** - **Incident Management** - **Problem Management** - **Knowledge Base Management** - **Active Directory Self Service Catalog** Step 5: To install the ServiceDesk modules

After installation is complete, you must perform additional configurations to ServiceDesk before you can begin to use it.

See "About configuring ServiceDesk" on page 146.

Step 1: To open the ServiceDesk Installation and Configuration Wizard

1. On the ServiceDesk server, in the location to which you downloaded the installation file, double-click the following shortcut:

   Symantec.ServiceDesk.Setup.msi

2. (Optional) If a message appears to let you know that the server does not meet all requirements, close the wizard, and install the missing items.

3. In the **Open File - Security Warning** dialog box, click **Run**.

Step 2: (Optional) To run a system diagnostic before Workflow Platform installation

1. On the **ServiceDesk Installation and Configuration** page, in the right pane under **Run System Diagnostic**, click **Start Program.**

   The system diagnostic displays information about the installation process. It displays which items in the process are installed in your system and which items remain to be installed.

2. On the **Run System Diagnostic** page, review the system diagnostic.

3. The system diagnostic displays a message. The message states that it has discovered a problem with your system and that you should click **Next** to continue.

   The problem is that you have not installed the Workflow Platform or the ServiceDesk modules. See the not installed symbol (red square with white x in it) next to **Workflow Server**. When you click **Next**, the ServiceDesk Installation and Configuration Wizard guides you through the installation of the Workflow Platform.

4. After you review the system diagnostic, perform any of the following actions:

Click **Refresh**.	Lets you rerun the system diagnostic.
Click **Next**.	Lets you continue with the installation process. Takes you to the Workflow Platform's **License Agreement** page in the ServiceDesk Installation and Configuration Wizard.
Click **Finish**.	Lets you return to the **ServiceDesk Installation and Configuration** page. Lets you continue with the installation process later, if you not ready at this time.

Step 3: To install the Workflow Platform

1. On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove Workflow Server and Portal**, click **Start Program**.
2. On the **Workflow's License Agreement** page, review the license agreement, and perform the following actions:

Check **I have read and agree to the license terms**.	Lets you accept the license terms and activate the **Next** option. Until you perform this action, the **Next** option is grayed out.
Click **Next**.	Lets you continue to the **Prepare Workflow Platform Installation** page.

3. On the **Connect to SMP** page, specify the following information for the ServiceDesk to Symantec Management Platform connection:

   This connection lets the ServiceDesk Installation and Configuration Wizard download the Workflow Platform installer from the Symantec Management Platform.

SMP Address: (Port)**:**	Lets you type the address of the Symantec Management Platform so that you can download the Workflow Platform installer. Lets you type the port to use for the protocol that you select. ■ The Symantec Management Platform default port is 80. ■ The Symantec Management Platform over SSL default port is 443. If you use multiple versions of the Symantec Management Platform, specify the one on which you installed or upgraded the ServiceDesk solution software.
Domain	Lets you type the domain to which the Symantec Management Platform belongs.
Username **Password**	Lets you type the credentials that the ServiceDesk server can use to interact with the Symantec Management Platform. The credentials must be for a user who has administrative rights.

Use SSL (https://)

Lets you use secure (encrypted) connections from the ServiceDesk server back to the Symantec Management Platform.

If you use SSL on the Symantec Management Platform, you need to check **Use SSL (https://)**.

4 When you are finished typing your information, click **Test Connection**.

Do not leave this page until your connection is confirmed.

5 When you are finished, click **Next**.

6 On the **Download Workflow Installer** page, click **Begin Download**.

7 After the download is complete, click **Next**.

8 On the **Set Server Base URL** page, specify the following information:

Note: For load balancing information concerning this step in the installation process, refer to the load balancing instructions in the Symantec™ Workflow 7.5 User Guide.

Server Address

Lets you type the address that you want to use for the ServiceDesk server. You can use the Fully Qualified Domain Name (FQDN), the IP address of the server, or the NETBIOS equivalent. Should be the address that users use to access ServiceDesk.

After you type this information, be sure that it is resolvable. The base URL lets the server calculate the links that are used throughout ServiceDesk.

You do not need to include the scheme prefix (http:// or https://).

Use SSL (https://)

Lets you use secure (encrypted) connections to the ServiceDesk server.

9 When you are finished, click **Next**.

10 On the **Workflow Installation Options** page, change any of the default information and selections as follows:

Install Location

Lets you specify where to install the Program shortcuts, such as Process Manager and Workflow Designer, on the ServiceDesk server. You can leave the default folder name or type a new folder name.

The default installation folder is as follows:

<drive>`:\Program Files\Symantec\Workflow`

Start Menu Path

Lets you determine where to install the Program shortcuts on the **Start** menu on the ServiceDesk server.

- You can use the default **Start** menu path and folder name: `Symantec\Workflow`.
- You can select or type the path and the folder name in the **Start** menu in which to create the Program shortcuts.

Program Shortcuts

- **On Desktop**
- **In Quick Launch Bar**

Lets you determine if and where the additional Program shortcuts are installed. By default **In Quick Launch Bar** is checked.

- Check **On Desktop** to install program shortcuts on the desktop.
  For example, select this option if you want the Process Manager portal shortcut to appear on the desktop.
- Check **In Quick Launch Bar** to install program shortcuts on the Quick Launch toolbar.
  For example, select this option if you want the Process Manager portal shortcut to appear in the Quick Launch toolbar.
- If you do not want any additional program shortcuts installed, uncheck **On Desktop** and **In Quick Launch Bar**.

Workflow Website

ServiceDesk requires you to use the **Default Web Site** (Site ID1) for installation.

Install Workflow Designer

Lets you install Workflow Designer.

By default, **Install Workflow Designer** is checked. You should leave this option checked.

Admin Account Name

Admin Password

Confirm Admin Password

Lets you specify the credentials of the ServiceDesk administrator account. The administrator account is used to set up and manage groups, users, permissions, and other settings in the Process Manager portal.

You must use an email account format for the **Admin Account Name**.

For example:

<admin@symantec.com>

The account that you specify is created during the installation so that it is available for the administrator who first logs on to ServiceDesk.

If you need or want to change the Administrator Login password, you can change it after the installation is completed. For more information, see How to change Administrator User admin@logicbase.com in 7.0, 7.1 and 7.1 SP1 or admin@symantec.com in 7.1 SP2) password after installation? at the following URL:

http://www.symantec.com/docs/TECH146586

11 When you are finished, click **Next**.

12 On the **Prepare Database Installation** page, provide the following information:

Note: For load balancing information concerning this step in the installation process, refer to the load balancing instructions in the Symantec™ Workflow 7.5 User Guide

Database Installation Account Setup section

Lets you create an account for the installer to use when the installer creates the Process Manager database. This account lets ServiceDesk communicate with SQL Server during installation only. It also lets you specify the authentication method for ServiceDesk to use to connect to the Process Manager database.

Server Name

Lets you type the IP address or the domain name of the server on which to install the Process Manager database.

The Process Manager database must reside on the SQL Server.

Type

Lets you select your authentication method. The options are as follows:

- **Windows** (Windows Integrated Security)
  Lets you use a domain account.
  If you installed SQL Server on its own server, you must select this option.
- **SQL** (Microsoft SQL Server Security)
  Lets you use a SQL account.
  If you installed SQL Server on the same server as ServiceDesk, you can select this option.
  You can use a “SA” or equivalent account here if you want. Document your user name and password.
  If you plan to use this authentication method, the target database server must be configured to support SQL authentication.

Username

Password

Lets you specify the credentials for the Windows or SQL account. This account should have the *sysadmin* server role on the SQL server.

These credentials are not stored or used to run ServiceDesk. They are only used to set up the Process Manager database during installation.

If you install SQL Server on its own server, include the domain prefix as follows:

<domain>\<username>

Database Installation section

Lets you provide information concerning the creation of the Process Manager database.

Database Name

Lets you name the Process Manager database. You should use a unique name, such as <*ProcessManager*>.

Database names cannot contain spaces.

Warning: If you use the same SQL Server to host the new Process Manager database and the previous Process Manager database, give the new Process Manager database a unique name. If you do not give the new Process Manager database a unique name the previous Process Manager database is overwritten. The pre-existing data is then corrupted and it cannot be accessed.

Warning: If you plan to use the same SQL Server for both Helpdesk Solution and ServiceDesk, do not overwrite the existing Helpdesk Solution data. The pre-existing data is then corrupted and it cannot be accessed

Overwrite if Exists check box	Lets you overwrite any existing database data. If you leave **Overwrite if Exists** unchecked, the data is added to the information in the database. **Warning:** If you use the same SQL Server to host the new Process Manager database and the previous Process Manager database, do not overwrite the existing Process Manager database. The pre-existing data is then corrupted and it cannot be accessed. **Warning:** If you use the same SQL Server for both Helpdesk Solution and the Process Manager database, do not overwrite the existing Helpdesk Solution data. The pre-existing data is then corrupted and it cannot be accessed You might have an existing Process Manager database from a previous version of ServiceDesk or from another product that installed the Process Manager database. If the wizard detects an existing Process Manager database, **Overwrite if Exists** is checked by default.
Use Case Sensitive Collation check box	Lets you generate your database using a case-sensitive collation. This check box provides compatibility with other databases that are case-sensitive, and your reporting needs require SQL to query data across both databases. This option is not normally required. The recommended configuration is to leave this box unchecked.

13 When you are finished typing your information, click **Validate Connection Details**.

Do not leave this page until your settings are confirmed.

14 When you are finished, click **Next**.

15 On the **Runtime Database Account Setup** page, provide the following information:

This page lets you create an application pool identity account for ServiceDesk to use during run-time to communicate with the SQL Server. It also lets you select the authentication method for ServiceDesk to use to connect to the Process Manager database.

Type

Lets you select your authentication method. The options are as follows:

- **Windows** (Windows Integrated Security)
  Lets you use a domain account.
  If you installed SQL Server on its own server, you must select this option.
  This authentication method is the recommended authentication method.
  Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security.
- **SQL** (Microsoft SQL Server Security)
  Lets you use a SQL account.
  If you installed SQL Server on the same server as ServiceDesk, you can select this option.
  You can use a “SA” or equivalent account here if you want. Document your user name and password.
  If you plan to use this authentication method, the target database server must be configured to support SQL authentication.

Username

Password

Lets you specify the credentials for the Windows or SQL account.

- If you use Windows authentication, this account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database.
- If you use SQL authentication, this account is added to the *db_owner* role on the Process Manager database.

If you install SQL Server on its own server, include the domain prefix as follows:

<domain>\<username>

16 When you are finished entering your information, click **Test Settings**.

Do not leave this page until your settings are confirmed.

17 When you are finished, click **Next**.

18 On the **Review Installation Settings** page, review your settings.

19 Do not click **Next** until you are ready to begin installation.

If you need to change any of your settings, click **Back** to return to the previous pages.

20 When you are ready to start the Workflow Platform installation, click **Next**.

21 On the **Installing the Workflow Server and ProcessManager Portal** page, the ServiceDesk Installation and Configuration Wizard checks connections. The wizard then installs the Process Manager database, Process Manager portal, and Workflow Designer.

22 After the wizard displays the installed successfully message, click **Finish**.

Step 4: (Optional) To run a system diagnostic before ServiceDesk modules installation

1 On the **ServiceDesk Installation and Configuration** page, under **Run System Diagnostic**, click **Start Program**.

The system diagnostic displays information about the installation process. It displays which items in the process are installed in your system and which items remain to be installed.

2 The system diagnostic displays a message. The message states that it has discovered a problem with your system and that you should click **Next** to continue.

The problem is that you have not installed the ServiceDesk modules. See the not installed symbol (red square with white x in it) next to **ServiceDesk Core**. When you click **Next**, the ServiceDesk Installation and Configuration Wizard guides you through the installation of the ServiceDesk modules.

3 On the **Run System Diagnostic** page, review the system diagnostic.

The following components should be installed and connections should be made:

Workflow Server The server-side software that includes the workflow extensions that are required to run the core workflow processes.

SMP Connection The checkmark represents the connection that was made to the Symantec Management Platform (SMP) to download the Workflow Platform installation file.

The **No SMP connection found** message is displayed because during the ServiceDesk modules installation, you create another SMP connection.

Workflow core service Installed as part of the Workflow Server software.

Workflow Persistence Queue Installed as part of the Workflow Server software.

Timeout and Escalation Processing Installed as part of the Workflow Server software.

ProcessManager Portal Installed as part of the Workflow Server software. After you install the ServiceDesk modules, you use the portal to access ServiceDesk.

Runtime Database Connection Verifies the ServiceDesk run-time connection to the Process Manager database and displays the authentication method.

ProcessManager Session Persistence Installed as part of the Process Manager portal installation.

Workflow Server to ProcessManager Portal Connection Verifies the connection between the Process Manager database and the Process Manager portal.

4 After you review the system diagnostic, perform any of the following actions:

Click **Refresh**.	Lets you rerun the system diagnostic.
Click **Next**.	Lets you continue with the installation process. Takes you to the ServiceDesk's **License Agreement** page in the ServiceDesk Installation and Configuration Wizard.
Click **Finish**.	Lets you return to the **ServiceDesk Installation and Configuration** page. Lets you continue with the installation process later, if you not ready at this time.

Step 5: To install the ServiceDesk modules

1 On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove ServiceDesk**, click **Start Program**.

The ServiceDesk Installation and Configuration Wizard runs a system diagnostic to see what still needs to be installed and opens the ServiceDesk’s **License Agreement** page.

2 On the ServiceDesk's **License Agreement** page, review the license agreement, and perform the following actions:

Check **I have read and agree to the license terms**.	Lets you accept the license terms and activate the **Next** option. Until you perform this action, the **Next** option is grayed out.
Click **Next**.	Lets you continue to the **Select ServiceDesk Modules to Install** page.

3 On the **Select ServiceDesk Modules to Install** page, select the modules that you want to install as follows:

Change Management Standardizes the methods and procedures for handling changes in the organization to minimize the effect of those changes on service.

Incident Management Provides a process for submitting and resolving incidents. Lets the users submit incidents and lets the Support workers respond to and resolve the incidents.

Problem Management Minimizes the effects of incidents and problems by letting you track and diagnose problems and publish known errors to help with future resolutions.

Knowledge Base Management Provides a process for gathering, analyzing, storing, and sharing knowledge and information within an organization. Improves the efficiency by reducing the need to rediscover knowledge.

Active Directory Self Service Catalog Provides the end-user Active Directory requests for password reset and access to network shares.

4 When you are finished, click **Next**.

5 On the **Set SMP Connection** page, provide the following information for the ServiceDesk server to the Symantec Management Platform connection:

This connection lets the ServiceDesk server connect to the Symantec Management Platform to obtain licenses and to integrate with the Configuration Management Database.

SMP Address: Lets you type the address of the Symantec Management Platform so that the ServiceDesk server can connect to it.

(Port)**:** Lets you type the port to use for the protocol that you select.

- The Symantec Management Platform default port is 80.
- The Symantec Management Platform over SSL default port is 443.

If you use multiple instances of the Symantec Management Platform, specify the one from which you intend to manage the ServiceDesk licenses.

Username

Password

Lets you type the credentials that the ServiceDesk server can use to interact with the Symantec Management Platform.

The credentials must be for a user who has administrative rights.

Use SSL (https://)

Lets you use secure (encrypted) connections from the ServiceDesk server back to the Symantec Management Platform.

If you use SSL on the Symantec Management Platform, you need to check **Use SSL (https://)**.

6 Click **Test Connection** to test the connection.

If the connection fails, check to make sure that the Symantec Management Platform address, user name, password, port, and SSL selection are correct.

7 When you are finished, click **Next**.

8 On the **Configure Mail Settings** page, provide the information so that the ServiceDesk Installation and Configuration Wizard can configure your outbound and your inbound mail settings.

9 In the **Outbound Mail Settings** section, specify the outbound mail settings section for email communication to and from ServiceDesk.

SMTP Server Address:

(Port)**:**

Lets you type the name of the mail server that ServiceDesk uses to send and receive emails. Use the following format:

<mail.domain_name.com>

Lets you specify the port to use for the protocol that you select.

- The SMTP default port is 25.
- The Secure SMTP (SSMTP) default port is 465.

Use SSL

Lets you use secure (encrypted) protocol to secure the email transmissions to and from ServiceDesk.

Send Mail From

Lets you type the email address from which ServiceDesk sends emails.

For example:

- *<No-reply@domain_name.com>*
- *<Support@domain_name.com>*
  If you plan to respond to emails that are sent from ServiceDesk, Symantec recommends that you use a more specific address like this one.

If you choose to monitor inbound email, use the same address that you use in the **Username** field under the **Inbound Mail Settings** section. That way, the responses are sent to the Inbox that ServiceDesk monitors.

Send Errors To

Lets you type the email address to which ServiceDesk errors are sent.

10 Click **Test** to test the outbound mail settings connection.

The ServiceDesk Installation and Configuration Wizard lets you precede with invalid outbound mail settings. Symantec recommends that you click Test to ensure that your settings are correct.

11 In the **Inbound Mail Settings** section, specify the settings for the Inbox monitor tool. This tool lets you monitor a specific mailbox for the incidents that users submit to ServiceDesk by email.

Inbound Mail Protocol

Lets you select the protocol for the email transmissions to ServiceDesk.

Select one of the following options:

- **IMAP**
- **POP**

Symantec recommends that you use the POP protocol. Using IMAP might cause problems with some mail server programs, including Microsoft Exchange.

Inbound Mail Server

(Port)**:**

Lets you type the name of the mail server that the ServiceDesk Inbox monitoring tool monitors for incidents. Use the following format:

<mail.domain_name.com>

Lets you specify the port to use for the protocol that you select.

- The IMAP default port is 143.
- The IMAP4 over SSL (IMAPS) default port is 993.
- The POP3default port is 110.
- The Secure POP3 (SSL-POP) default port is 995.

Username

Password

Lets you type the address and password for the mailbox that the ServiceDesk Inbox monitoring tool monitors for the incidents that users submit by email.

Depending on your mail server , use one of the following formats:

- *<Support@domain_name.com>*
- *<Support>*

Also, use the same address in the **Username** field as you used in **Send Mail From** field under the **Outbound Mail Settings** section

Use SSL

Lets you use secure (encrypted) protocol to secure the email transmissions to ServiceDesk.

Quarantine Folder (IMAP)

(IMAP protocol only) Lets you type the folder name where ServiceDesk places unprocessed emails when the IMAP protocol is used.

For example, *<UnprocessedInboundEmails>*

If an error occurs while ServiceDesk processes an inbound email, the email is removed from the monitored inbox and moved to the specified folder.

If you do not provide a name for the folder, ServiceDesk (SD.Email.Monitor Project) continues to process the error-prone email. Each time the email is processed, an error occurs, and email notifications are sent. This routine continues until either the message gets processed or it is manually deleted from the inbox.

12 Click **Test** to test the inbound mail settings.

The ServiceDesk Installation and Configuration Wizard lets you precede with invalid inbound mail settings. Symantec recommends that you click **Test** to ensure that your settings are correct

13 When you are finished, click **Next**.

Even if your settings are incorrect at this time, you can proceed with ServiceDesk installation. You can change your outbound and your inbound mail settings after installation in the Process Manager portal.

On the **Master Settings** page, in the **Email Settings** section, you can edit the outbound email settings. On the **Application Properties** page in the **ServiceDesk Settings** section, in the **Mail Settings** category, you can edit both the inbound and the outbound email monitoring settings.

14 On the **Additional Options** page, specify the following information:

Critical Error Handling section	Lets you provide the contact information that is used to display a message to the user for any error message that appears in ServiceDesk.
Critical Error Contact Name	Lets you type the name for the group or individual who provide your ServiceDesk support. For Example, a typical contact is the network administrator; however, you can specify any other individual or group
Critical Error Contact Info	Lets you type the email address, telephone number, or other information for the group or individual who provides your ServiceDesk support.
Email Inbox Monitoring section **Enable Email Inbox Monitoring** check box	Lets you enable email inbox monitoring.

You can modify the information after installation. In the Process Manager portal, on the **Application Properties** page, in the **ServiceDesk Setting** section, you can edit the information and enable or disable email inbox monitoring.

15 When you are finished, click **Next**.

16 On the **ServiceDesk Installation** page, click **Begin Installation**.

If you need to change any of your settings, click **Back** to return to the previous pages.

17 After the following message is displayed, click **Finish**:

Installation was successful.

Running a system diagnostic

The **Run System Diagnostic** feature of the ServiceDesk Installation and Configuration Wizard lets you check your current system environment for installation readiness and previously installed components. You can run a system diagnostic to see the results of your installation process. For example, you install the Workflow Platform. You want to see what is installed and what remains to be installed before you install the ServiceDesk modules.

See "ServiceDesk Installation and Configuration Wizard" on page 99.

You can also run a system diagnostic to help troubleshoot a problem. For example, you installed the Workflow Platform, but when you try to install the ServiceDesk modules, you discover that you cannot. To find out if the necessary Workflow Platform components were installed, you can run a system diagnostic.

For information about the symbols and features of the **Run System Diagnostic** page in the ServiceDesk Installation and Configuration Wizard, see the following instruction:

See "Run System Diagnostic page" on page 123.

To run a system diagnostic

1 On the **ServiceDesk Installation and Configuration** page, in the right pane under **Run System Diagnostic**, click **Start Program**.

2 On the **Run System Diagnostic** page, review the system diagnostic.

3 After you review the system diagnostic, perform any of the following actions:

Click **Refresh**.	Lets you rerun the system diagnostic.
Click **Next**.	If this option is active, it lets you continue with the installation process.
Click **Finish**.	Lets you return to the **ServiceDesk Installation and Configuration** page.

Run System Diagnostic page

The **Run System Diagnostic** page displays the results from a system diagnostic. This page lets you verify what components are installed and what components remain to be installed for ServiceDesk installation. The **Run System Diagnostic** page is one of the pages in the ServiceDesk Installation and Configuration Wizard.

See “Installing the Workflow Platform and the ServiceDesk modules” on page 103.

See “Running a system diagnostic” on page 122.

A symbol precedes each component as follows:

Table 7-9 Symbols on the **Run System Diagnostic** page

Symbol	s u
✓	e m e t c i t s s d e i t a s i t n e r s d e l l n r u . t n e m
✖	s i t n e r s t d e l l n r u . t n e m

Table 7-9 Symbols on the **Run System Diagnostic** page *(continued)*

Symbol	s u
⚠	e m e t c i t s d t t s r u t n e m r r s i . t n e
ℹ	s i t n e r s d e l l d n o i t a n , e u n t e r e e m s n o i t a o . r e c

The **Run System Diagnostic** page contains the following options:

Table 7-10 Options on the **Run System Diagnostic** page

Options	Description
✖	Lets you hide the information to the left of the **Hide** symbol (red X).
ℹ	Lets you view the description of the recommendations about the installation of the component.
Refresh	Lets you rerun the system diagnostic. Also, lets you refresh the page and unhide any information that you chose to hide.

Table 7-10 Options on the **Run System Diagnostic** page *(continued)*

Options	Description
Cancel	Lets you cancel the **Run System Diagnostic** page and return to the **ServiceDesk Installation and Configuration** page and continue with the installation process when you are ready.
Next	If this option is active, it lets you continue with the installation process. Lets you advance to the next page of the ServiceDesk Installation and Configuration Wizard.
Finish	Lets you return to the **ServiceDesk Installation and Configuration** page and continue with the installation process when you are ready.

About modifying your ServiceDesk installation

In some situations, you may need to modify your ServiceDesk installation. You can rerun the ServiceDesk Installation and Configuration Wizard to modify your ServiceDesk installation for the following situations:

To add a ServiceDesk module	During the installation of the ServiceDesk modules, you did not install a ServiceDesk module. Later, you decide that you want to use that ServiceDesk process. See “Adding a ServiceDesk module” on page 125.
To repair your ServiceDesk installation	During your ServiceDesk usage, you delete a Process Manager portal setting. You can repair your portal settings, by restoring then to their default state. See “Repairing Process Manager portal settings” on page 133.

Adding a ServiceDesk module

During your initial installation process, you can select which ServiceDesk modules to install. If you chose not install a module, you can always add the module later. You can rerun the ServiceDesk Installation and Configuration Wizard to add an uninstalled module.

To add a ServiceDesk module

1 On the ServiceDesk server, in the location to which you downloaded the installation file, double-click the following shortcut:

Symantec.ServiceDesk.Setup.msi

2 In the **Open File - Security Warning** dialog box, click **Run**.

3. On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove ServiceDesk**, click **Start Program**.
4. On the **Please Provide Windows Auth Credentials** page, under **Runtime Database Account Info**, type your run-time database credentials: the user name and password.
5. Click **Test Settings**.

   Do not leave this page until your settings are confirmed.
6. When you are finished, click **Next**.
7. On the **Start ServiceDesk Installation Program** page, click **Install or Repair ServiceDesk** and then click **Next**.
8. On the ServiceDesk's **License Agreement** page, review the license agreement, and perform the following actions:

Check **I have read and agree to the license terms**.	Lets you accept the license terms and activate the **Next** option. Until you perform this action, the **Next** option is grayed out.
Click **Next**.	Lets you continue to the **Select ServiceDesk Modules to Install** page.

9. On the **Select ServiceDesk Modules to Install** page, the ServiceDesk Installation and Configuration Wizard displays which modules are already installed on your ServiceDesk server.

10 Select the module that you want to install:

Change Management Standardizes the methods and procedures for handling changes in the organization to minimize the effect of those changes on service.

Incident Management Provides a process for submitting and resolving incidents. Lets the users submit incidents and lets the Support workers respond to and resolve the incidents.

Problem Management Minimizes the effects of incidents and problems by letting you track and diagnose problems and publish known errors to help with future resolutions.

Knowledge Base Management Provides a process for gathering, analyzing, storing, and sharing knowledge and information within an organization. Improves the efficiency by reducing the need to rediscover knowledge.

Active Directory Self Service Catalog Provides the end-user Active Directory requests for password reset and access to network shares.

11 When you are finished, click **Next**.

12 On the **Upgrade Options** page, click **Next**.

Warning: Do not check any of the boxes. All necessary items are installed with the module. If you check any of the boxes, you overwrite any changes that you have made to those setting in the Process Manager portal.

13 If necessary, on the **Set SMP Connection** page, provide or change the following information for the ServiceDesk to the Symantec Management Platform connection:

This connection lets the ServiceDesk server connect to the Symantec Management Platform to obtain licenses and to integrate with the Configuration Management Database.

SMP Address: (Port)**:**	Lets you type the address of the Symantec Management Platform so that the ServiceDesk server can connect to it. Lets you type the port to use for the protocol that you select. ■ The Symantec Management Platform default port is 80. ■ The Symantec Management Platform over SSL default port is 443. If you use multiple instances of the Symantec Management Platform, specify the Symantec Management Platform from which you intend to manage the ServiceDesk licenses.
Username **Password**	Lets you type the credentials that the ServiceDesk server can use to interact with the Symantec Management Platform. The credentials must be for a user who has administrative rights.
Use SSL (https://)	Lets you use secure (encrypted) connections from the ServiceDesk server back to the Symantec Management Platform. If you use SSL on the Symantec Management Platform, you need to check **Use SSL (https://)**.

14 Click **Test Connection** to test the connection.

If the connection fails, check to make sure that the Symantec Management Platform address, user name, password, port, and SSL selection are correct.

15 When you are finished, click **Next**.

16 If necessary, on the **Configure Mail Settings** page, provide or change the information for your outbound and your inbound mail settings.

17 If necessary, in the **Outbound Mail Settings** section, provide or change the outbound mail settings section for email communication to and from ServiceDesk.

SMTP Server Address: (Port)**:**	Lets you type the name of the mail server that ServiceDesk uses to send and receive emails. Use the following format: *<mail.domain_name.com>* Lets you specify the port to use for the protocol that you select. 1 The SMTP default port is 25. 2 The Secure SMTP (SSMTP) default port is 465.

Use SSL

Lets you use secure (encrypted) protocol to secure the email transmissions to and from ServiceDesk.

Send Mail From

Lets you type the email address from which ServiceDesk sends emails.

For example:

- *<No-reply@domain_name.com>*
- *<Support@domain_name.com>*
  If you plan to respond to emails that are sent from ServiceDesk, Symantec recommends that you use a more specific address like this one.

If you choose to monitor inbound email, use the same address that you use in the **Username** field under the **Inbound Mail Settings** section. That way, the responses are sent to the Inbox that ServiceDesk monitors.

Send Errors To

Lets you type the email address to which ServiceDesk errors are sent.

18 Click **Test** to test the outbound mail settings connection.

The ServiceDesk Installation and Configuration Wizard lets you precede with invalid outbound mail settings. Symantec recommends that you click Test to ensure that your settings are correct.

19 If necessary, in the **Inbound Mail Settings** section, provide or change the settings for the Inbox monitor tool. This tool lets you monitor a specific mailbox for the incidents that users submit to ServiceDesk by email.

Inbound Mail Protocol

Lets you select the protocol for the email transmissions to ServiceDesk.

Select one of the following options:

- **IMAP**
- **POP**

Symantec recommends that you use the POP protocol. Using IMAP might cause problems with some mail server programs, including Microsoft Exchange.

Inbound Mail Server

(Port)**:**

Lets you type the name of the mail server that the ServiceDesk Inbox monitoring tool monitors for incidents. Use the following format:

<mail.domain_name.com>

Lets you specify the port to use for the protocol that you select.

- The IMAP default port is 143.
- The IMAP4 over SSL (IMAPS) default port is 993.
- The POP3default port is 110.
- The Secure POP3 (SSL-POP) default port is 995.

Username

Password

Lets you type the address and password for the mailbox that the ServiceDesk Inbox monitoring tool monitors for the incidents that users submit by email.

Depending on your mail server , use one of the following formats:

- *<Support@domain_name.com>*
- *<Support>*

Also, use the same address in the **Username** field as you used in **Send Mail From** field under the **Outbound Mail Settings** section.

Use SSL

Lets you use secure (encrypted) protocol to secure the email transmissions to ServiceDesk.

Quarantine Folder (IMAP)

(IMAP only) Lets you type the folder name where ServiceDesk places unprocessed emails when the IMAP protocol is used.

For example, *<UnprocessedInboundEmails>*

If an error occurs while ServiceDesk processes an inbound email, the email is removed from the monitored inbox and moved to the specified folder.

If you do not provide a name for the folder, ServiceDesk (SD.Email.Monitor Project) continues to process the error-prone email. Each time the email is processed, an error occurs, and email notifications are sent. This routine continues until either the message gets processed or it is manually deleted from the inbox.

20 Click **Test** to test the inbound mail settings.

The ServiceDesk Installation and Configuration Wizard lets you precede with invalid inbound mail settings. Symantec recommends that you click **Test** to ensure that your settings are correct

21 When you are finished, click **Next**.

Even if your settings are incorrect at this time, you can proceed with ServiceDesk module installation. You can change your outbound and your inbound mail settings in the Process Manager portal.

On the **Master Settings** page, in the **Email Settings** section, you can edit the outbound email settings. On the **Application Properties** page and in the **ServiceDesk Settings** section, you can edit both the inbound and the outbound email monitoring settings.

22 If necessary, on the **Additional Options** page, change the following information:

Critical Error Handling section	Lets you provide the contact information that is used to display a message to the user for any error message that appears in ServiceDesk.
Critical Error Contact Name	Lets you type the name for the group or individual who provide your ServiceDesk support. For Example, a typical contact is the network administrator; however, you can specify any other individual or group.
Critical Error Contact Info	Lets you type the email address, telephone number, or other information for the group or individual who provides your ServiceDesk support.
Email Inbox Monitoring section **Enable Email Inbox Monitoring** check box	Lets you enable email inbox monitoring.

You can modify the information after installation. In the Process Manager portal, on the **Application Properties** page, in the **ServiceDesk Setting** section, you can edit the information and enable or disable email inbox monitoring.

23 When you are finished, click **Next**.

24 On the **ServiceDesk Installation** page, click **Begin Installation**.

If you need to change any of your settings, click **Back** to return to the previous pages.

25 After the following message is displayed, click **Finish**:

Installation was successful.

About repairing Process Manager portal settings

ServiceDesk lets you modify, configure, and customize many aspects of your ServiceDesk processes. You can restore many settings to their default states. To restore these settings you use the **Install or Repair** option in the ServiceDesk Installation and Configuration Wizard.

See "Repairing Process Manager portal settings" on page 133.

Table 7-11 Settings that you can repair in the Process Manager portal

Settings	Location in the portal	Description
Process Types	**Admin > Data > Process Type Actions**	Lets you repair the following: ■ Deleted **Process Types** with default settings and actions ■ **Process Types** default settings ■ Deleted **Process Type Actions** ■ Default settings for **Process Type Actions**
Data Profiles	**Admin > Data > List and Profiles**	Lets you repair the following: ■ Deleted **Data Profiles** ■ Default settings for **Data Profiles**
Service Catalog	**Admin > Service Catalog Settings**	Lets you repair the following: ■ Deleted **Service Catalog** categories ■ Modified **Service Catalog** categories with default settings and permissions ■ Default permissions for **Service Catalog** categories ■ Deleted **Service Catalog** items ■ Modified **Service Catalog** items with default settings and permissions. ■ Default permissions for **Service Catalog** items
Application Settings	**Admin > Data > Application Properties**	Lets you repair the following: ■ Default settings for **Application Settings**

Table 7-11 Settings that you can repair in the Process Manager portal *(continued)*

Settings	Location in the portal	Description
Hierarchy Data	**Admin > Data > Hierarchy Data Service**	Lets you repair the following: ■ Default values for **Hierarchy Data Service**
Calendars	**Calendar** page	Lets you repair the following: ■ Default settings for calendars ■ Deleted calendars
Data Mappings	**Admin > Process Automation > Incident Management > Service Dashboard > Manage Data Mapping**	Lets you repair the following: ■ Default values for **Data Mappings** ■ Deleted **Data Mappings**

Repairing Process Manager portal settings

During your use of ServiceDesk, you delete or change a portal setting and need to repair it. You can repair your ServiceDesk settings by restoring them back to their default state. You can rerun the ServiceDesk Installation and Configuration Wizard to repair your portal settings.

You can select which of the portal settings to repair, in the ServiceDesk Installation and Configuration Wizard, on the **Upgrade Options** page. For more information about the portal settings you can repair, see the following instruction:

See “About repairing Process Manager portal settings” on page 132.

To repair Process Manager portal settings

1. On the ServiceDesk server, in the location to which you downloaded the installation file, double-click the following shortcut:

   Symantec.ServiceDesk.Setup.msi

2. In the **Open File - Security Warning** dialog box, click **Run**.

3. On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove ServiceDesk**, click **Start Program**.

4. On the **Please Provide Windows Auth Credentials** page, under **Runtime Database Account Info**, type your run-time database credentials: the user name and password.

5. Click **Test Settings**.

   Do not leave this page until your settings are confirmed.

6 When you are finished click **Next**.

7 On the **Start ServiceDesk Installation Program** page, click **Install or Repair ServiceDesk** and then click **Next**.

8 On the ServiceDesk's **License Agreement** page, review the license agreement, and perform the following actions:

Check **I have read and agree to the license terms**.	Lets you accept the license terms and activate the **Next** option. Until you perform this action, the **Next** option is grayed out.
Click **Next**.	Lets you continue to the **Select ServiceDesk Modules to Install** page.

9 On the **Select ServiceDesk Modules to Install** page, click **Next**.

The ServiceDesk Installation and Configuration Wizard displays which modules are installed on your ServiceDesk server.

10 On the **Upgrade Options** page, select the portals settings that you want to repair and then click **Next**.

See “About repairing Process Manager portal settings” on page 132.

Warning: By checking a box, you overwrite any changes that you have made to those portal settings. However, you must overwrite your changes to repair the settings.

11 If necessary, on the **Set SMP Connection** page, provide or change the following information for the ServiceDesk to the Symantec Management Platform connection:

This connection lets the ServiceDesk server connect to the Symantec Management Platform to obtain licenses and to integrate with the Configuration Management Database.

SMP Address: (Port)**:**	Lets you type the address of the Symantec Management Platform so that the ServiceDesk server can connect to it. Lets you type the port to use for the protocol that you select. ■ The Symantec Management Platform default port is 80. ■ The Symantec Management Platform over SSL default port is 443. If you use multiple instances of the Symantec Management Platform, specify the Symantec Management Platform from which you intend to manage the ServiceDesk licenses.
Username **Password**	Lets you type the credentials that the ServiceDesk server can use to interact with the Symantec Management Platform. The credentials must be for a user who has administrative rights.
Use SSL (https://)	Lets you use secure (encrypted) connections from the ServiceDesk server back to the Symantec Management Platform. If you use SSL on the Symantec Management Platform, you need to check **Use SSL (https://)**.

12 Click **Test Connection** to test the connection.

If the connection fails, check to make sure that the Symantec Management Platform address, user name, password, port, and SSL selection are correct.

13 When you are finished, click **Next**.

14 If necessary, on the **Configure Mail Settings** page, provide or change the information for your outbound and your inbound mail settings.

15 If necessary, in the **Outbound Mail Settings** section, provide or change the outbound mail settings section for email communication to and from ServiceDesk.

SMTP Server Address: (Port)**:**	Lets you type the name of the mail server that ServiceDesk uses to send and receive emails. Use the following format: *<mail.domain_name.com>* Lets you specify the port to use for the protocol that you select. 1 The SMTP default port is 25. 2 The Secure SMTP (SSMTP) default port is 465.

Use SSL	Lets you use secure (encrypted) protocol to secure the email transmissions to and from ServiceDesk.
Send Mail From	Lets you type the email address from which ServiceDesk sends emails. For example: ■ *<No-reply@domain_name.com>* ■ *<Support@domain_name.com>* If you plan to respond to emails that are sent from ServiceDesk, Symantec recommends that you use a more specific address like this one. If you choose to monitor inbound email, use the same address that you use in the **Username** field under the **Inbound Mail Settings** section. That way, the responses are sent to the Inbox that ServiceDesk monitors.
Send Errors To	Lets you type the email address to which ServiceDesk errors are sent.

16 Click **Test** to test the outbound mail settings connection.

The ServiceDesk Installation and Configuration Wizard lets you precede with invalid outbound mail settings. Symantec recommends that you click Test to ensure that your settings are correct.

17 If necessary, in the **Inbound Mail Settings** section, provide or change the settings for the Inbox monitor tool. This tool lets you monitor a specific mailbox for the incidents that users submit to ServiceDesk by email.

Inbound Mail Protocol	Lets you select the protocol for the email transmissions to ServiceDesk. Select one of the following options: ■ **IMAP** ■ **POP** Symantec recommends that you use the POP protocol. Using IMAP might cause problems with some mail server programs, including Microsoft Exchange.

Inbound Mail Server

(Port)**:**

Lets you type the name of the mail server that the ServiceDesk Inbox monitoring tool monitors for incidents. Use the following format:

<mail.domain_name.com>

Lets you specify the port to use for the protocol that you select.

- The IMAP default port is 143.
- The IMAP4 over SSL (IMAPS) default port is 993.
- The POP3default port is 110.
- The Secure POP3 (SSL-POP) default port is 995.

Username

Password

Lets you type the address and password for the mailbox that the ServiceDesk Inbox monitoring tool monitors for the incidents that users submit by email.

Depending on your mail server , use one of the following formats:

- *<Support@domain_name.com>*
- *<Support>*

Also, use the same address in the **Username** field as you used in **Send Mail From** field under the **Outbound Mail Settings** section.

Use SSL

Lets you use secure (encrypted) protocol to secure the email transmissions to ServiceDesk.

Quarantine Folder (IMAP)

(IMAP protocol only) Lets you type the folder name where ServiceDesk places unprocessed emails when the IMAP protocol is used.

For example, *<UnprocessedInboundEmails>*

If an error occurs while ServiceDesk processes an inbound email, the email is removed from the monitored inbox and moved to the specified folder.

If you do not provide a name for the folder, ServiceDesk (SD.Email.Monitor Project) continues to process the error-prone email. Each time the email is processed, an error occurs, and email notifications are sent. This routine continues until either the message gets processed or it is manually deleted from the inbox.

18. Click **Test** to test the inbound mail settings.

    The ServiceDesk Installation and Configuration Wizard lets you precede with invalid inbound mail settings. Symantec recommends that you click **Test** to ensure that your settings are correct

19. When you are finished, click **Next**.

    Even if your settings are incorrect at this time, you can proceed with ServiceDesk module installation. You can change your outbound and your inbound mail settings in the Process Manager portal.

    On the **Master Settings** page, in the **Email Settings** section, you can edit the outbound email settings. On the **Application Properties** page and in the **ServiceDesk Settings** section, you can edit both the inbound and the outbound email monitoring settings.

20. If necessary, on the **Additional Options** page, change the following information:

Critical Error Handling section	Lets you provide the contact information that is used to display a message to the user for any error message that appears in ServiceDesk.
Critical Error Contact Name	Lets you type the name for the group or individual who provide your ServiceDesk support. For Example, a typical contact is the network administrator; however, you can specify any other individual or group.
Critical Error Contact Info	Lets you type the email address, telephone number, or other information for the group or individual who provides your ServiceDesk support.
Email Inbox Monitoring section	Lets you enable email inbox monitoring.
Enable Email Inbox Monitoring check box	

    You can modify the information after installation. In the Process Manager portal, on the **Application Properties** page, in the **ServiceDesk Setting** section, you can edit the information and enable or disable email inbox monitoring.

21. When you are finished, click **Next**.

22 On the **ServiceDesk Installation** page, click **Begin Installation**.

If you need to change any of your settings, click **Back** to return to the previous pages.

23 After the following message is displayed, click **Finish**:

Installation was successful.

Uninstalling ServiceDesk from the ServiceDesk server

You can uninstall ServiceDesk from the ServiceDesk server. For example, you might want to move ServiceDesk to a different ServiceDesk server.

This procedure uninstalls ServiceDesk only. It does not uninstall any of the Workflow Platform, which includes the Process Manager Portal, Workflow Designer, and the Process Manager database.

See "Uninstalling Workflow from the ServiceDesk server" on page 140.

You can still use Workflow after you have uninstalled ServiceDesk.

To uninstall ServiceDesk from the ServiceDesk server

1 On the ServiceDesk server, in the location to which you downloaded the installation file, double-click the following shortcut:

Symantec.ServiceDesk.Setup.msi

2 In the **Open File - Security Warning** dialog box, click **Run**.

3 On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove ServiceDesk**, click **Start Program**.

4 On the **Please Provide Windows Auth Credentials** page, under **Runtime Database Account Info**, type the user name and password.

5 Click **Test Settings**.

Do not leave this page until your settings are confirmed.

6 When you are finished, click **Next**.

7 On the **Start ServiceDesk Installation Program** page, click **Uninstall ServiceDesk** and then click **Next**.

8 On the **Uninstall ServiceDesk** page, click **Uninstall**.

To see the uninstall details, in the bottom left corner of the ServiceDesk Installation and Configuration Wizard, click **View Log**.

9 When uninstall is complete, click **Finish**.

Uninstalling Workflow from the ServiceDesk server

You can uninstall Workflow from the ServiceDesk server. For example, you moved ServiceDesk to a different ServiceDesk server. Now, you want to remove Workflow from the server.

See “Uninstalling ServiceDesk from the ServiceDesk server” on page 139.

Warning: If you uninstall Workflow before you uninstall ServiceDesk, you break ServiceDesk. Workflow must be installed to use ServiceDesk.

This procedure uninstalls the Process Manager portal and Workflow Designer only. It does not uninstall the Process Manager databases.

To uninstall Workflow from the ServiceDesk server

1. On the ServiceDesk server, in the location to which you downloaded the installation file, double-click the following shortcut:

   Symantec.ServiceDesk.Setup.msi

2. In the **Open File - Security Warning** dialog box, click **Run**.

3. On the **ServiceDesk Installation and Configuration** page, under **Install, Repair, or Remove Workflow Server and Portal**, click **Start Program**.

4. On the **Start Workflow Installation Program** page, click **Uninstall the Workflow Platform**.

   Warning: Do not click **Next** until you are prepared to uninstall Workflow. The uninstall process begins when you click **Next.**

5. To uninstall Workflow, click **Next**.

   To see the uninstall details, in the bottom left corner of the ServiceDesk Installation and Configuration Wizard, click **View Log**.

6. When uninstall is complete, click **Finish**.

Installing the Screen Capture Utility

This chapter includes the following topics:

- About installing the Screen Capture utility
- Downloading the Screen Capture Utility installation file

About installing the Screen Capture utility

ServiceDesk provides a Screen Capture utility that lets users capture images of their computer screens. For example, a user can capture an error message and attach it to an incident. The Screen Capture utility is available in different areas in the Process Manager portal.

Table 8-1 Methods for installing the Screen Capture utility

Method	When to use this method	Description
From a prompt in the Process Manager portal	■ To let end-users and ServiceDesk workers install the utility on their non-managed computers. ■ To let customers who are outside your organization install the utility.	When a user or ServiceDesk worker selects the option to capture a screen and the utility is not installed, they are prompted to install it.

Table 8-1 Methods for installing the Screen Capture utility *(continued)*

Method	When to use this method	Description
Directly from the installation file	■ To install the utility on any computer.	The **ServiceDesk Solution Console** page contains a link that lets you download the installation file for the Screen Capture utility. You can download the installation file to any computer and then run the installation. See "Downloading the Screen Capture Utility installation file" on page 142.

This instruction is an optional step in the following processes:

See "Installing ServiceDesk for the first time" on page 66.

See "Installing ServiceDesk in an environment with an existing instance of the Symantec Management Platform version 7.5 or 7.1 SP2" on page 67.

See "Migrating from ServiceDesk 7.1x" on page 75.

See "Migrating from ServiceDesk 7.0" on page 73.

See "Migrating from ServiceDesk 7.1 SP2 without upgrading your instance of the Symantec Management Platform 7.1 SP2" on page 77.

See "Migrating from Helpdesk Solution 6.x to ServiceDesk" on page 71.

Downloading the Screen Capture Utility installation file

In the Symantec Management Console, you can access a page that lets you download the Screen Capture Utility installation file. Access the Symantec Management Platform from any computer on which you plan to install the Screen Capture Utility. Download this file to the computer and then run the installation file. Users also can install it from the Process Manager portal.

See "About installing the Screen Capture utility" on page 141.

To download the Screen Capture Utility installation file

1 On the computer to which you want to download the installation file, open a browser and log on to the Symantec Management Console.

- Open Internet Explorer.
- Type **http://<*FDQN*>/altiris/console**.

- In the **Windows Security** dialog box, type your credentials and click **OK**.

2 In the **Symantec Management Console**, on the **Settings** menu, click **Settings > All Settings**.

3 In the left pane, expand **Settings > Service and Asset Management > ServiceDesk** and then click **ServiceDesk**.

4 On the **ServiceDesk Solution Console** page, under **Download ServiceDesk Installer**, click **Download Screen Capture Utility Installer**.

5 Save the Screen Capture Utility installation file to your computer.

Section 4

Configuring ServiceDesk

Chapter 9

Configuring ServiceDesk

This chapter includes the following topics:

About configuring ServiceDesk

The installation of the Workflow Platform and ServiceDesk modules includes an initial configuration of ServiceDesk and the Process Manager portal. The initial configuration lets you select the parts of ServiceDesk to install and configure communication settings.

See "Before you configure ServiceDesk" on page 147.

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs. First, you must add users and groups and set up their permissions. Also, ServiceDesk comes with a default set of business of hours. You need to configure the business hours and add holidays to meet your schedule.

Before you use the Problem Management and Knowledge Management processes, you may want to modify the email notifications and personalize the Process Manager portal.

Out-of-the-box, Change Management provides a default CAB and one preconfigured rule. The **OnChangeReceived** ruleset comes with a rule that routes all change requests to that default CAB. Before you put the Change Management process into production, you must perform certain tasks.

Examples of the tasks you must perform to configure the Change Management process are as follows:

- Create your Change Approval Boards.
- Create email templates.
- Configure your Change Management rulesets.

Out-of-the-box, Incident Management provides a default Service Queue, two preconfigured routing rules, and default Service Level Agreement levels, escalations, and milestones. The **OnIncidentReceived** ruleset has a preconfigured rule that routes all incidents to the default Service Queue. The **OnResolutionVerified** ruleset has a preconfigured rule that sends out the **Customer Satisfaction Survey** when a ticket is resolved. Before you put the Incident Management process into production, you must perform certain tasks.

Examples of the tasks you must perform to configure the Incident Management process are as follows:

- Configure your Service Level Agreement levels, escalations, and milestones.
- Create your service queues.
- Create email templates.
- Configure your Incident Management rulesets.

See "Configuring ServiceDesk" on page 147.

Before you configure ServiceDesk

Before you begin to configure ServiceDesk, you must use the ServiceDesk installer to install the Workflow framework and ServiceDesk modules on the ServiceDesk server.

The installation of the Workflow Platform and ServiceDesk modules includes an initial configuration of ServiceDesk and the Process Manager portal. The initial configuration lets you select the parts of ServiceDesk to install and configure communication settings.

See “Installing ServiceDesk 7.5” on page 65.

See “Migrating to ServiceDesk 7.5” on page 69.

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs.

See “Configuring ServiceDesk” on page 147.

Configuring ServiceDesk

Before you use ServiceDesk in your production environment, you must configure ServiceDesk to meet your needs. The configuration tasks are performed in the Process Manager portal and require administrator permissions.

See “About configuring ServiceDesk” on page 146.

You may want to perform some of these tasks again after your initial ServiceDesk configuration.

Before you begin to configure ServiceDesk, verify that it is installed and that you have performed the required setup steps.

See “Before you configure ServiceDesk” on page 147.

After you configure ServiceDesk, you may want to perform some additional configurations before you introduce ServiceDesk into your production environment.

See “Additional ServiceDesk configurations” on page 152.

If you migrated from a previous version of ServiceDesk or from Helpdesk Solution 6.x, you may want to migrate data to ServiceDesk 7.5.

See “About migrating data to ServiceDesk 7.5” on page 153.

Depending on your needs, you may want to perform some advanced customizations before you introduce ServiceDesk into your production environment.

See “Advanced ServiceDesk customizations” on page 154.

Table 9-1 ServiceDesk configuration tasks

Action	Description
Import users and groups from Active Directory, verify, and assign permissions.	If you use Active Directory authentication for ServiceDesk, you can set up Active Directory server connections and Active Directory sync profiles. Once you add the sync profiles, you can import the users and groups from Active Directory into ServiceDesk. See "Configuring Active Directory sync profiles" on page 254. Review the imported information to verify its accuracy, edit it if necessary, and assign permissions. See "Copying permissions between groups" on page 173. See "Adding or removing permissions for groups" on page 173.
Add users, groups, and organizational units, and assign permissions.	If you use native authentication for ServiceDesk, you must add the users in the Process Manager portal. ServiceDesk contains predefined groups and permissions, which you can use or modify. Assign the new users to the appropriate groups. See "Creating a new user" on page 175. See "Creating a group" on page 171. See "Creating an organizational unit" on page 174. See "Adding or removing permissions for groups" on page 173. See "Copying permissions between groups" on page 173.
Configure the Process Manager portal master settings.	The Process Manager portal master settings determine the behavior of ServiceDesk and the portal. You can use the default settings or you can edit them as necessary. Symantec recommends that you review and become familiar with the master settings before you edit them. See "About the Process Manager portal master settings" on page 250. See "Editing the Process Manager portal master settings" on page 250.
Customize the appearance of the Process Manager portal.	You can customize the Process Manager portal in the following ways: ■ Customize the general appearance by adding a company logo. You can perform this customization in the Process Manager portal, in the **Customization** section of the **Master Settings** page. See "Editing the Process Manager portal master settings" on page 250. ■ Customize individual portal pages for the entire organization or for users, groups, or organizational groups, or permission groups. Administrators have permission to customize portal pages and to grant customization permissions to other ServiceDesk users. See "About customizing the contents of Process Manager portal pages" on page 184.

Table 9-1 ServiceDesk configuration tasks *(continued)*

Action	Description
Configure your business hours and holidays.	Business hours are the hours during which your business is commonly conducted. ServiceDesk provides a set of default business hours. The default business hours are Monday thru Friday, 8:00 A.M. to 5:00 P.M. You can modify the default business hours or add your own business hours configurations. See "Configuring business hours" on page 161.
Configure Service Level Agreement (SLA) levels, escalations, and milestones.	A Service Level Agreement (SLA) is a contract between an organization and its service provider, which sets the expectations and requirements for service delivery. The SLA includes the allowable time frame for the service delivery. Incident Management provides default Service Level Agreement levels, escalations, and milestones. You can use the default settings or you can configure SLA levels, escalations, and milestones to meet your needs. See "Creating and Editing Service Level Agreements (SLAs)" on page 158.
Configure incident categories and the data hierarchy.	Categories are used to classify ServiceDesk incidents. ServiceDesk contains predefined incident categories, which you can use immediately or edit to meet your organization's requirements. If you migrated incidents or categories from Helpdesk Solution, those categories are added to the Process Manager portal for use in future incidents. Review the existing categories and edit or add to them if necessary. See "About Incident Management classifications and the data hierarchy" on page 177. See "Default categories for incidents and default classifications for problems" on page 297.
Verify or edit the incident types.	During incident submittal, support technicians can specify an incident type to identify the general nature of the incident. The incident type can be modified whenever an incident is worked. If an incident type has not been provided, the support technician must provide an incident type when an incident is resolved. ServiceDesk contains a set of predefined incident types that are ready to use. Review them to ensure that they meet your needs. If necessary, you can create or delete incident types. See "About incident types" on page 163. See "Creating and deleting incident types" on page 164.

Table 9-1 ServiceDesk configuration tasks *(continued)*

Action	Description
Verify or edit the default impact, urgency, and priority values.	During incident entry, the submitter specifies the incident's impact and urgency. Support technicians can also specify the priority. When a user submits an incident, the priority level is assigned based on the impact and the urgency that the user specified. See "About the incident priority" on page 155. ServiceDesk contains default values for the impact, urgency, and priority settings. You can change the available impact and urgency values and the priority that is assigned to the combination of the two values.
Create Incident Management service queues	The Incident Management process lets you route incidents to service queues. Before you can configure rules to route incidents, you must first create your service queues. These service queues are then available when you create your routing rules to route incoming incidents or to reassign an incident. Service queues consist of a group or multiple groups that you associate with it. You can change users and group without reconfiguring your routing rules. You can add or remove the users that are in the group that you associate with the service queue. You can add or remove the groups that are associated with the service queue. See "Creating incident service queues" on page 191.
Configure your Data Mapping Routing Tables	The Incident Management process lets you configure routing tables so that you can route incidents by specific classifications or by specific locations. Before you can configure rules to route incidents by specific classifications or locations, you must first configure the **Routing Tables**. These routing tables can then be used when you create your routing rules to route your incidents. See "About configuring Data Mapping Routing Tables" on page 163.
Create email templates for Incident Management.	Email notifications for Incident Management are handled through the Process Automation rules. Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. These templates are then available when you create your email notification rules and select the **Send Email** action. See "Creating email templates for Incident Management" on page 194.

Table 9-1 ServiceDesk configuration tasks *(continued)*

Action	Description
Configure the Incident Management Process Automation rules.	Rules determine which incidents are routed to which queues when new ServiceDesk incidents are submitted. Rules determine when email notifications are sent. Rules determine what happens when incident SLAs are late. This step requires time for testing and configuration. To set up automation rules properly, it's important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. See "Incident Management Process Automation rules components" on page 200.
Verify or edit the incident close codes.	When an incident is closed, the support technician must provide a close code to indicate the nature of the resolution. ServiceDesk contains a set of predefined close codes that are ready to use. Review them to ensure that they meet your needs. If necessary, you can delete or add to the default close codes. See "About incident close codes" on page 248. See "Adding and deleting incident close codes" on page 249.
Create change team groups for Change Management.	In the Change Management process, a change team is a group of people who can assess, plan, authorize, schedule, implement, and test a change request. The change team includes the change advisory board (CAB). The members of the CAB advise the change manager in the assessment, planning, and authorization of changes. During the initial approval phase of the Change Management process, the change manager selects the members of the change team. You can create predefined change team groups to facilitate the team selection. See "Configuring Change Management" on page 225.
Create email templates for Change Management.	Email notifications for Change Management are handled through the Process Automation rules. Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. These templates are then available when you create your email notification rules and select the **Send Email** action. See "Creating email templates for Change Management" on page 219.
Configure the Change Management Process Automation rules.	This step requires time for testing and configuration. To set up automation rules properly, it's important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. See "Configuring Change Management" on page 225.

Table 9-1 ServiceDesk configuration tasks *(continued)*

Action	Description
(Optional) Make the ServiceDesk documentation available to your users.	Each organization has specific requirements for providing documentation to their process workers and the users of the Process Manager portal. Therefore, the ServiceDesk documentation is not installed with ServiceDesk. Symantec recommends that you download these guides and make them available to your users as needed. See "Making the ServiceDesk documentation available to users" on page 236.
(Optional) Add a MIME type for remote control through RDP	When a process worker works a task that is associated with an equipment configuration item (CI), the worker can access the **Remote Control (Via RDP)** link. The link runs a tool, which generates and downloads an RDP file that contains the configuration item's IP address. The worker can use the RDP file to open a Remote Desktop Connection to the computer that the CI represents. This functionality requires that IIS (Internet Information Services) contains a MIME type for RDP. If you plan to use the remote control tool, you must add the new MIME type. In Internet Information Services Manager, you can edit the local computer's Properties and add a new MIME type. In the new MIME type, both the extension and MIME type are .rdp. After you add the new MIME type, you must restart IIS for the change to take effect.

Additional ServiceDesk configurations

After you configure ServiceDesk, you may want to perform some additional configurations before you introduce ServiceDesk into your production environment.

See "Configuring ServiceDesk" on page 147.

Table 9-2 Additional configuration tasks you can perform

Action	Description
Create incident templates.	In Incident Management, incident templates are special incident forms containing predefined, standard values for common issues. Using templates speeds the entry of incidents and helps to standardize and increase the accuracy of the incident information. Create incident templates for any issues that are reported frequently. You can edit and update them at any time. See "About incident templates" on page 212. See "Creating an incident template" on page 213.

Table 9-2 Additional configuration tasks you can perform *(continued)*

Action	Description
Create incident subtask templates.	In Incident Management, incident subtask templates are special incident forms containing predefined, standard values for common issues. Using subtask templates speeds the subtask assignment process and helps to standardize and increase the accuracy of the information. See "About subtask templates" on page 214. See "Creating subtask templates" on page 214.
Create change request templates.	In Change Management, change templates are special change forms containing predefined, standard values for common issues. Using templates speeds the entry of changes and helps to standardize and increase the accuracy of the change request information. See "About change templates" on page 227. See "Creating a new change template" on page 228.
Create and edit reports.	You can customize the ServiceDesk reports in the following ways: ■ You can copy a report and edit the copy to quickly create a new report. ■ You can use a wizard interface to create new reports, which eliminate the need to use SQL for report creation ■ You can add a report to any Process Manager portal page or dashboard, and you can define the size and placement of the report. ■ You can optimize your reports on the Process Manager portal pages to improve the performance of the Process Manager.

About migrating data to ServiceDesk 7.5

Depending on your needs, you may want to migrate data to ServiceDesk before you introduce ServiceDesk into your production environment.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See "Configuring ServiceDesk" on page 147.

If you migrated from a previous version of ServiceDesk or from Helpdesk Solution 6.x, you can migrate data to ServiceDesk 7.5.

Table 9-3 Data migration options

Option	Description
Migrate data from ServiceDesk 7.1 SP2.	You can leverage some data from ServiceDesk 7.1 SP2 in ServiceDesk 7.5. See "Migrating data from ServiceDesk 7.1 SP2" on page 285.
Migrate data from ServiceDesk 7.1 SP1.	You can leverage some data from ServiceDesk 7.1 SP1 in ServiceDesk 7.5. See "Migrating data from ServiceDesk 7.1 SP1" on page 286.
Migrate data from ServiceDesk 7.0 MR2.	You can leverage some data from ServiceDesk 7.0 MR 2 in ServiceDesk 7.5. See "Migrating data from ServiceDesk 7.0 MR2" on page 287.
Migrate data from Helpdesk Solution 6.x.	You can leverage some data from Helpdesk Solution 6.x in ServiceDesk 7.5. See "About migrating data from Helpdesk Solution 6.x" on page 288.

Advanced ServiceDesk customizations

Depending on your needs, you may want to perform some advanced customizations before you introduce ServiceDesk into your production environment.

See "Configuring ServiceDesk" on page 147.

The advanced customization tasks are configured in Workflow Designer. To view the projects that are available for advanced customization, you need to open Workflow Manager and then click **File > Open Project**.

For more information about using Workflow Designer to configure the workflow projects, see the Symantec™ Workflow 7.5 User Guide

For more information about the advanced customizations that you can perform in ServiceDesk, see Symantec Connect.

Table 9-4 Advanced customization tasks you can perform

Action	Description
Customize the appearance and content of forms.	In the Process Manager portal, a form is the screen or page that users and workers interact with during a process. ServiceDesk contains predefined forms for all its processes. These predefined forms are complete and ready to use immediately. However, you can customize any of the forms to meet your organization's established process requirements. See "About customizing forms" on page 185. Examples of common form customizations are as follows: ■ Setting permissions for forms. See "Setting permissions for a form" on page 188. ■ Editing the Customer Satisfaction Survey to change the frequency with which it is sent and the data that it collects. See "About the Customer Satisfaction Survey" on page 188. You can use Workflow Designer to customize the appearance and behavior of the forms in the Process Manager portal.
Customize email for ServiceDesk processes.	ServiceDesk can send email notifications when various Problem Management and Knowledge Management process events occur. It can also create incidents from inbound email. These email capabilities are predefined and ready to use. However, you can customize them as needed. See "Customizing the email actions for ServiceDesk processes" on page 231.
Verify the problem categories.	During the entry of a problem ticket, the process worker specifies a category to help classify the root cause of the problem. ServiceDesk contains default values for the problem category. You can add and edit the problem categories. You can make these changes by editing the `SD.ProblemManagement` project in Workflow Designer.

About the incident priority

Every incident that is submitted to the ServiceDesk is assigned a priority. This priority lets you determine how the incident is routed and when it is escalated. The prioritization of incidents helps you manage Service Level Agreements (SLA) and comply with the concepts of ITIL service management.

A user who submits an incident can specify the urgency and the impact. You can use these values to calculate the incident's priority and to create routing rules for its initial routing. This automatic calculation eliminates guesswork and prevents the user from assigning a high priority to every incident. The support technician who works the incident can change the urgency values and impact values as well as the calculated priority.

See “How the incident priority is calculated” on page 157.

A support technician who uses the advanced incident form can specify the urgency, impact, and priority. The priority is not calculated automatically because the support workers can assess an incident’s priority better than the users can.

ServiceDesk contains default values for the urgency, impact, and priority settings. The values that are available differ between the standard incident form and the advanced incident form. For the user’s benefit, the values that appear on the standard incident form are more descriptive.

See “Default priority, urgency, and impact values” on page 157.

Most ServiceDesk implementations either use the default priority, impact, and urgency values or make only minor changes.

To change these values and make them available in your Incident Management process, you need to modify different areas of the process as follows:

- In the Process Manager portal, you can edit these values on the **Application Properties** page.
  These are the values that you can choose from on the advanced incident form and on the "simple" incident form.

- In the Process Manager portal, you can change the impact, urgency, and priority values in the **Impact/Urgency Matrix** to match those on the **Application Properties** page.
  You can use the mappings in the **Impact/Urgency Matrix** to create routing rules to set the priority of your incidents. To use these mappings, select the **Set Priority** action and then in the next drop-down list select the **Using Impact/Urgency Matrix** option.
  You can edit this matrix from the **Data Mapping** page. Click **Admin > Process Automation**. Expand **Incident Management** and click **Service Dashboard**. Under **Actions: INCIDENT-MGMT**, click **Manage Data Mappings**.

- In Workflow Designer, you can edit the advanced feeder form to reconfigure the **Auto-calculate Priority** link on the advance incident form.
  Changing the values requires caution and a good understanding of the Symantec Workflow software. You can change the available impact and urgency values and the priority that is assigned to the combination of the two values. You make these changes by editing the advanced feeder form in Workflow Designer.
  For more information about forms customization and project modifications, see the Symantec™ Workflow 7.5 User Guide.

Default priority, urgency, and impact values

During incident entry, the submitter specifies the urgency and impact. When a user submits an incident, the priority is assigned based on the urgency and the impact that the user specified. The support technicians can change an assigned priority. Support technicians who create new incidents can specify the priority.

ServiceDesk contains default values for the priority, urgency, and impact settings.

See "About the incident priority" on page 155.

Table 9-5 Default priority, urgency, and impact values

Setting	Default values
Urgency	Represents an assessment of how much the issue affects the submitter or the primary contact. The end users and support technicians can select from the following values: - **Core Business Service** - **Support Service** - **Non-urgent Services**
Impact	Defines the extent of the issue by specifying how many people are affected. The users and support technicians can select from the following values: - **Department/LOB/Branch** (LOB means line of business) - **Small group or VIP** - **Single User**
Priority	Determines how the incident is routed and when it is escalated. This setting is available on the advanced incident form only. The default values are as follows: - **Low** - **Minor** - **Normal** - **High** - **Urgent** - **Emergency**

How the incident priority is calculated

When a user submits an incident, the incident is assigned a priority based on the impact and the urgency that the user specified. This automatic calculation can eliminate guesswork and prevents the user from assigning a high priority to every incident.

On the **Create a New Incident** page that the user sees, the option to specify the impact is named **Who is Affected?**.

See "About the incident priority" on page 155.

You can configure the values and the way that they combine to arrive at the priority.

Table 9-6 How the incident priority is calculated

Urgency	Impact	Calculated priority
Non-urgent Services	Single User	Low
Non-urgent Services	Small group or VIP	Normal
Non-urgent Services	Department/LOB/Branch	High
Support Service	Single User	Normal
Support Service	Small group or VIP	High
Support Service	Department/LOB/Branch	High
Core Business Service	Single User	High
Core Business Service	Small group or VIP	Urgent
Core Business Service	Department/LOB/Branch	Urgent

Creating and Editing Service Level Agreements (SLAs)

A Service Level Agreement (SLA) is a contract between an organization and its service provider. It sets the expectations and requirements for service delivery. The SLA can be between an external customer and your customer support team or between your organization's employees and your IT department. The corporate policy typically defines the overall SLA. The SLA formally defines the agreed-upon services, priorities, and responsibilities that are required to support the customers and users.

SLAs use a Business Hours Configuration to determine if an SLA is late or not. The predefined SLAs are configured to use the Default Business Hours. Before you create an SLA, you should configure your business hours.

See "Configuring business hours" on page 161.

Video: For more information about configuring business hours, creating SLAs, and rulesets for SLAs, see ServiceDesk Configuration: SLA Framework Overview on Symantec Connect.

When you create or edit SLA levels, you can configure the **Late Date**. SLA Configuration late date is made up of days and minutes. You can enter whole or fractional amounts into the **Days** field, in decimal format. You can also use a combination of days and minutes.

See "About configuring the Service Level Agreement (SLA) late date" on page 160.

To create or edit Service Level Agreements (SLAs)

1 In the **Process Manager**, click **Admin > Process Automation**.

2 On the **Available Services** page, expand **Incident Management** and click **Service Dashboard**.

3 Under **Actions: INCIDENT-MGMT**, click **Manage SLA Levels**.

4 On the **SLA Levels Configuration** page, under **SLA Levels**, perform one of the following actions:

Edit an existing SLA level	In the **SLA Levels** table, in the row for the SLA level that you want to edit, click the **Actions** symbol (orange lightning). Then click **Edit SLA Level**.
Add a new SLA level	In the lower right, click **Add SLA Level**.

5 In the **SLA Level Editor**, provide information for the following items:

Level	Provide a descriptive name to identify the SLA level.
Description	Provide a description of the purpose of the SLA level.
Milestone	Select the milestone for which the SLA level applies.
Escalation	Indicate whether or not the escalation is **Late** or **Warn**.
Late Date	Provide the amount of time that must pass for the SLA to be considered **Late** or **Warn**.
Use Business Hours	Indicate whether or not you want to associate business hours with this SLA level.
Business Hours	Select the **Business Hours Configuration** that you want to associate with this SLA level to determine when a service is considered **Late** or **Warn**.

6 Click **Save**.

About configuring the Service Level Agreement (SLA) late date

When you create or edit SLA levels, you can configure the **Late Date**. SLA Configuration late date is made up of days and minutes. You can enter whole or fractional amounts into the **Days** field, in decimal format. You can also use a combination of days and minutes.

See “Creating and Editing Service Level Agreements (SLAs)” on page 158.

ServiceDesk converts the total **Late Date** into minutes. It converts the days into minutes and then adds the total to the **Minute’s** field.

When configuring your SLA Level late dates you have the following options:

You can use your business hours to configure your late dates. (Check **Use Business Hours**.)	■ ServiceDesk calculates the late date into business minutes. It excludes the time that falls in holidays, weekends, off hours, and periods when the SLA is paused. ■ When you use the **Using Business Hours** option, one day equals the hours in a business day. For example, you use a work day from 9:00 A.M. to 5:00 P.M. The business day equals 8 hours or 480 minutes.
You can use a 24 hour day to configure your late dates. (Do not check **Use Business Hours**.)	■ ServiceDesk calculates the late date into minutes. It excludes time periods when the SLA is paused. ■ When you do not use the **Using Business Hours** option, one day equals 24 hours or 1,441 minutes.

Default SLA levels

A Service Level Agreement (SLA) defines the expectations and requirements for delivering a service, including the allowable time frame for the response and resolution.

A default SLA is built in to the Incident Management process. The SLA levels are configured according to the default business hours, which are set up for a nine hour day, 8:00 A.M. - 5:00 P.M. You can edit the default business hours and SLA levels to comply with your organization’s business hours and SLAs.

See “Configuring business hours” on page 161.

You manage your SLA levels from the **SLA Levels Configuration** page. To access the page, in the Process Manager portal, click **Admin > Process Automation**. Expand **Incident Management** and click **Service Dashboard**. Then, under **Actions: INCIDENT-MGMT** click **Manage SLA Levels**.

See "Creating and Editing Service Level Agreements (SLAs)" on page 158.

Table 9-7 Default SLA levels

SLA level	Description	Time frames
Initial Response	The initial response levels monitor how much time a worker is allowed to respond to an incident according to it priority. Responses include opening the ticket to set ownership, making comments, or resolving the incident.	The default SLA Levels for initial response are as follows: ■ Emergency: 60 minutes ■ High: 120 minutes ■ Normal: one business day ■ Low: two business days
Resolution	The resolution level monitors how much time a worker is allowed to resolve an incident according to its priority.	The default SLA Levels for resolution are as follows: ■ Emergency: one business day ■ High: two business days ■ Normal: five business days ■ Low: 10 business days

Configuring business hours

Business hours are the hours during which your business is conducted. Typical business hours can vary by location.

You can define multiple sets of business hours and holidays depending on your business locations and your SLA policy, such as the following:

- Default
  The default business hours are included with ServiceDesk. The hours are set from Monday through Friday, 8:00 A.M. to 5:00 P.M.
  You can edit the default business hours to meet your organizations requirements. You can define the beginning and ending business hours, holidays, and weekend days.
- Custom

You can create additional custom business hours. For example, if a specific department operates through the weekend while other departments operate during the business week. Or a retail industry might require special project-level business hours.

Video: For more information about configuring business hours, creating SLAs, and rulesets for SLAs, see ServiceDesk Configuration: SLA Framework Overview on Symantec Connect.

To configure business hours:

1 In the **Process Manager**, go to **Admin > Data > Business Hours**.

2 On the **Business Hours** page, do one of the following:

Modify the **Default Business Hours** configuration.	In the **Default Business Hours** row, click the **Action** symbol (orange lightning), and then click **Edit**.
Create a custom **Business Hours** configuration.	Click the **Add** symbol (green plus sign).

3 On the **Business Hours Configuration** page, provide information for the following items:

Name	Provide a descriptive name that indicates the purpose of the **Business Hours Configuration**. For example, U.S. East Sales Team Extended Business Hours.
Begin Business Hours	Provide the time of day when the business hours begin.
End Business Hours	Provide the time of day when the business hours end.
Holidays	■ In the **Date** field, enter the date of a holiday that is included in these Business Hours. ■ In the **Description** field, enter a description of the holiday and click **Add Holiday**. Note that holidays are excluded from the business hours. ■ Repeat this process for all of the holidays that apply to this **Business Hours Configuration**.
Weekends	Select any days which should be excluded from the **Business Hours Configuration**.

4 Click **Save**.

See “Creating and Editing Service Level Agreements (SLAs)” on page 158.

About configuring Data Mapping Routing Tables

The Incident Management process lets you configure data mapping routing tables so that you can route incidents by specific classifications or by specific locations. These tables reduce the number of routing rules that you need to create.

For example, you have several classifications that you want routed to specific service queues. You can configure the **Routing Table: Classification** to contain all the necessary classifications and which service queues to assign them. Then you can create one rule to route incidents by classification. In this rule, you can use the classification Routing Table to route the incidents with those specific classifications to the proper service queues.

You can configure these routing tables in the Process Manager portal. Click **Admin > Process Automation**, expand **Incident Management**, and click **Service Dashboard**. Under **Actions: INCIDENT MGMT**, click **Manage Data Mapping**.

Warning: The **Data Mapping Routing Tables'** editing process lets you delete data mapping records from the **Impact/Urgency Matrix**, **Routing Table: Classification**, and **Routing Table: Location** tables after they are used in your automation rules. Deleting a data mapping record that an automation rules relies on to execute, causes the rule to error out.

Video: For more information about configuring the Data Mapping Routing Tables, see ServiceDesk Configuration: Data Mapping and Routing Rules on Symantec Connect.

About incident types

You can use incident types to indicate the general nature of an incident. When support technicians use the advanced incident form to submit an incident, they can provide an incident type. An incident type is not required to submit an incident.

The incident type can be modified anytime an incident is worked. However, if an incident type has not been provided, the support technician must provide an incident type when the incident is resolved.

ServiceDesk contains a set of predefined incident types that are ready to use. If necessary, you can add to or delete the default incident types. You can edit the incident types in the Process Manager portal on the **Application Properties** page.

The incident type lets you select a type that best indicates the general nature of the incident.

The default incident types are as follows:

- **How To**
- **Break Fix**
- **Add or Install**
- **Change or Move**
- **Backup**
- **Authorize or Approve**
- **Delete or Remove**
- **Request**

See "Creating and deleting incident types" on page 164.

Creating and deleting incident types

ServiceDesk contains a set of predefined incident types that you can use to identify the general nature of an incident. If necessary, you can create your own incident types to use. You can also delete incident types.

See "About incident types" on page 163.

As a best practice, do not delete incident types after they are used in your incidents.

To create or delete incident types

1. In the Process Manager portal, click **Admin > Data > Application Properties**.
2. On the **Application Properties** page, under **Application Properties Profiles**, click **ServiceDeskSettings**.
3. At the far right of the **ServiceDeskSettings** title bar, click the **Actions** symbol (orange lightning), and then click **Edit Values**.
4. In the **Edit Profile Definition Instance** dialog box, scroll down to **Incident Type**, and under the list of incident types, click **Edit**.
5. In the dialog box that appears, take any of the following actions:

To create an incident type	In the field at the bottom of the dialog box, type the new incident type, and then click **Add**.
To delete an incident type	To the right of the incident type, Click the **Delete** symbol (a red X).

6 When you finish editing the incident types, click **Save**.

7 In the **Edit Profile Definition Instance** dialog box, click **Save**.

About the Service Catalog and service items

The Service Catalog is a Web part that appears on several Process Manager portal pages and that lets users select service items. A service item automates the routine actions that are performed in ServiceDesk. Service items are available for both process workers and users.

The service items are organized in categories, which appear in a tree view in the Service Catalog. You can control the use of the service items by setting permissions on a category or on individual items.

The Service Catalog contains many predefined service items, which can be used to initiate some of the ServiceDesk processes. For example, the default service items are used to submit an incident, submit a knowledge base request, and create a problem ticket.

Users who submit incidents can first search the Service Catalog for any self-service items that help them resolve the incident on their own. The self-service items can reduce incident submissions and reduce the amount time that support workers spend resolving incidents. During the incident submission process, users can search the Service Catalog for any items that can help them solve the issue on their own. A support technician can resolve an incident by suggesting a self-serve item.

See “About the Active Directory Self Service Catalog” on page 34.

Chapter 10

Managing security, users, roles, groups, and permissions

This chapter includes the following topics:

About ServiceDesk security and permissions

ServiceDesk manages access to the Process Manager portal through native authentication or Active Directory authentication.

See “About ServiceDesk authentication” on page 168.

ServiceDesk provides a high level of security within the Process Manager portal through the use of users, groups, organizational units, and permissions. The ServiceDesk permissions control all the views and possible actions in the Process Manager portal.

For example, permissions can grant or deny access to certain functions within ServiceDesk. Permissions can grant the ability to create users, and they can deny access to view and edit articles in the knowledge base.

The ServiceDesk permissions are hierarchical. The permission that is applied at the most specific level takes precedence. For example, a group is denied access to view a knowledge base article. However, a specific user within that group has permission to view the article. In this case, the user’s specific permission overrides the group setting, and the user is able to view the article.

Table 10-1 ServiceDesk permissions hierarchy

Permissions level	Description
User	Any user of the portal who can log on. Users can have permissions assigned to them. User can also inherit permissions from the groups and organizational units to which they belong.
Group	A collection of users. For example, the Support group might contain all your support technicians. The KB Editors group might contain all the people who can review and edit knowledge base articles. Users can be members of multiple groups. ServiceDesk permissions are almost always granted at the group level rather than at the user level. See “About group-level permissions” on page 168.
Permission	Permissions control the access to and use of the Process Manager portal. What users can view and what actions they can perform are based on permissions. For example, permissions may grant access to certain functions within ServiceDesk, such as the ability to create users. Or permissions may grant or deny access to view and edit articles in the knowledge base. Access to everything in ServiceDesk is controlled through permissions.
Organizational unit	A collection of users or groups. An organizational unit is generally a very large group. For example, an organizational unit may be a department, office, or division of an organization. The ServiceDesk organizational units do not correspond to the Active Directory organization units.

About group-level permissions

Groups are collections of ServiceDesk users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of ServiceDesk permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. ServiceDesk permissions are almost always granted at the group level rather than at the user level.

When you apply permissions to groups, you do not have to edit the permission settings for the individual users. The permissions changes that you make at the group level are updated for every user who is a member of that group.

You can use the default groups that are provided with ServiceDesk, create new groups, or import groups from Active Directory.

For more information, see the lists of default permissions in ServiceDesk in the Symantec™ ServiceDesk 7.5 User Guide.

See "Creating a group" on page 171.

About ServiceDesk authentication

The authentication method can be defined in the **Process Manager Active Directory Settings** section in the Process Manager portal on the **Master Settings** page. You can use native authentication or Active Directory (AD) authentication.

Table 10-2 Authentication methods for ServiceDesk users

Method	Description
Native authentication	With native authentication, users are authenticated against the Process Manager database. This authentication method requires that you create user accounts in ServiceDesk.

Table 10-2 Authentication methods for ServiceDesk users *(continued)*

Method	Description
Active Directory authentication	With Active Directory authentication, a mixed mode authentication is used. Active Directory users are authenticated against Active Directory. Any users who are not found in Active Directory are authenticated against the Process Manager database (native authentication). When Active Directory authentication is selected, the Active Directory users and groups are imported to ServiceDesk during synchronizations. The imported users and groups are stored in the Process Manager database. However, Active Directory passwords and other sensitive information are not stored in the Process Manager database. See "About Active Directory synchronization" on page 253. You can add additional Active Directory server connections or edit the settings for an existing server connection. You manage the Active Directory server connections in Workflow Explorer. See "Managing Active Directory server connections" on page 256. After you add an Active Directory server connection, you can add sync profiles. You can use the sync profiles to target the entire domain, organizational units and groups on the Active Directory server, and specific LDAP queries. These options are available on the **Active Directory Sync Profiles** page, which is accessed from the **Admin** menu. See "Managing Active Directory sync profiles" on page 270. See "Configuring Active Directory sync profiles" on page 254.

About adding users from Active Directory

When your organization uses Active Directory (AD) authentication, the Active Directory users and groups are imported to ServiceDesk during Active Directory synchronizations. The ServiceDesk users and groups are stored in the Process Manager database.

See "About ServiceDesk authentication" on page 168.

Table 10-3 How Active Directory users can be added to ServiceDesk

Method	Description
During the synchronization between ServiceDesk and Active Directory	You can schedule full or update ServiceDesk synchronizes with Active Directory to obtain new and updated users and groups from Active Directory. During synchronization, the user and the group data from Active Directory overwrites the user and the group data that is in ServiceDesk. See "About Active Directory synchronization" on page 253.

Table 10-3 How Active Directory users can be added to ServiceDesk *(continued)*

Method	Description
Manually	If a new user needs to access ServiceDesk between synchronization, you can add the user manually from Active Directory.
Automatically when a user logs on	This method is available only if the option **Auto Create Users on Initial Login** is selected for the Active Directory server. Users in Active Directory that have not been imported into ServiceDesk can be added to ServiceDesk when they log on to the Process Manager portal. When such a user enters their logon credentials, ServiceDesk checks the credentials against the Process Manager database. If the credentials are not there, ServiceDesk checks the credentials against Active Directory and adds the user to ServiceDesk. See "Adding Active Directory sync profiles" on page 272.

See "About adding groups from Active Directory" on page 170.

About adding groups from Active Directory

When your organization uses Active Directory (AD) authentication, the Active Directory users and groups are imported to ServiceDesk during sync profile synchronizations. When Active Directory users are imported to ServiceDesk, they retain their group associations from Active Directory. The ServiceDesk users and groups are stored in the Process Manager database.

See "About ServiceDesk authentication" on page 168.

Table 10-4 How Active Directory groups can be added to ServiceDesk

Method	Description
During manually run synchronizations	During the installation of the ServiceDesk application software, the users and groups from your Active Directory are imported to ServiceDesk. See "Methods for synchronizing Active Directory sync profiles" on page 280.

Table 10-4 How Active Directory groups can be added to ServiceDesk *(continued)*

Method	Description
During automatic synchronization between ServiceDesk and Active Directory	You can create sync schedules for when ServiceDesk synchronizes with Active Directory to obtain new and updated users and groups from Active Directory. During synchronization, the user and the group data from Active Directory overwrites the user and the group data that is in ServiceDesk. See "About Active Directory synchronization" on page 253.

When you import your groups from Active Directory, your Active Directory groups are added with only All Users permissions by default. You must assign additional permissions to those groups after they are imported.

See "Copying permissions between groups" on page 173.

See "About adding users from Active Directory" on page 169.

See "Managing Active Directory sync profiles" on page 270.

Creating a group

Groups are collections of ServiceDesk users. The use of groups lets you assign permissions more efficiently and helps simplify the ongoing administration of ServiceDesk permissions. Instead of assigning permissions to each user individually, you can specify the permissions for a group. The permissions for a group are valid for each user who is a member of that group. ServiceDesk permissions are almost always granted at the group level rather than at the user level.

See "About group-level permissions" on page 168.

An administrator or other user who has the appropriate permissions can create ServiceDesk groups. Groups can also be added by importing them from Active Directory.

See "About adding groups from Active Directory" on page 170.

You can copy permissions from another group and assign them to the new group. If you do not copy the permissions from another group, you must assign the permissions to the new group in a separate task.

See "Adding or removing permissions for groups" on page 173.

See "Copying permissions between groups" on page 173.

To create a group

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the **List Groups** page, at the upper right of the **All Groups** section, click the **Add Groups** symbol (white page with green plus sign).
3. In the **Add Group** dialog box, perform the following actions:
   - Type the name of the new group.
   - (Optional) Copy permissions from another group.
   - (Optional) Specify the group's home page.
   - (Optional) Specify the group's email address
4. Click **Save**.

Adding users to a group

When you add users to a ServiceDesk group, each user inherits the permissions that are defined for that group. An administrator or other user who has the appropriate permissions can add users to ServiceDesk groups.

See "About group-level permissions" on page 168.

See "Creating a group" on page 171.

To add users to a group

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the **List Groups** page, under **All Groups**, select the group to which you want to add users.
3. In the right pane, at the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Add User**.
4. In the **Add User** dialog box, take the following actions:
   - In **Add user to group**, type the user's email address or click **Pick** to search for a user.
   - (Optional) In **Relationship Type**, select the type of relationship.
     The relationship type is used if your organization customized ServiceDesk to assign tickets based on user relationships.
   - Click **Add** to add the user to the list at the top of the **Add User** dialog box.
5. When you finish adding users, in the **Add User** dialog box, click **Close**.

Adding or removing permissions for groups

In ServiceDesk, a group's permissions determine the permissions control the permissions that are granted to individual ServiceDesk users. When you assign permissions for a group, each user that is a member of that group is granted those permissions.

See "About group-level permissions" on page 168.

An administrator or other user who has the appropriate permissions can add or remove the permissions that are associated with a group.

To add or remove permissions from a group

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the **List Groups** page, under **All Groups**, select the group that you want to add or remove the permissions.
3. In the right pane, at the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Permissions**.
4. In the **Permissions For Group** dialog box, take any of the following actions:
   - Select the check box for each permission to assign to this group
   - Uncheck the checkbox for each permission to remove from this group.
   - Click **Select All** to add all available permissions to a group.
   - Click **Unselect All** to remove all permissions from a group.
5. Click **Save**.

Copying permissions between groups

You can copy all the ServiceDesk permissions from one group to another group.

Typically, you can import the permissions from another group when you create a new group in the Process Manager portal.

See "About adding groups from Active Directory" on page 170.

The ability to copy permissions between existing groups is useful when you import an Active Directory group. The imported groups are added with only All Users permissions by default and you must assign additional permissions yourself. Copying the permissions from another group eliminates the need to assign the permissions manually.

See "About group-level permissions" on page 168.

An administrator or other user who has the appropriate permissions can add or remove the permissions that are associated with a group.

To copy permissions between groups

1. In the Process Manager portal, click **Admin > Users > Accounts > List Groups**.
2. On the List Groups page, under **All Groups**, find the group for which you want to set permissions.
3. At the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Copy Permissions From**.
4. On the **Copy Permissions From Groups** page, in the **Group Name** field, specify the group from which to copy the permissions.

   You can type the name of the other group or click **Pick** to select a group from the **Group Picker** dialog box.
5. Click **Save**.

Creating an organizational unit

Organizational units are large groups of ServiceDesk users or groups. A typical organizational unit might be a department within a company.

An administrator or other user who has the appropriate permissions can create organizational units.

To create an organizational unit

1. In the Process Manager portal, click **Admin > Users > Accounts > List Organizations**.
2. On the **List Organizations** page, at the upper right corner of the page, click the **Add Root Organization** symbol (a white page with a green plus sign).
3. In the **Add Organization** dialog box, in the **Organization Name** field, type a descriptive name for the organization.

   You can use special characters in the name. Duplicate names are not allowed.
4. (Optional) In the **Description** field, type a description to further identify the organizational unit.
5. Click **Save**.

Creating a new user

An administrator or other user who has the appropriate permissions can create new ServiceDesk users.

Users can also be added to ServiceDesk through Active Directory.

See "About adding users from Active Directory" on page 169.

Every ServiceDesk user requires permissions to perform any actions in the Process Manager portal. By default, every new user is assigned to the All Users group, which provides general permissions. However, you must assign the user to one or more of the groups that provide the permissions that are appropriate for that user's role.

See "About group-level permissions" on page 168.

The easiest way to assign groups and permissions to a new user is by cloning them from another user during the user entry. If you do not clone the user information, you must assign the user to groups manually.

See "Adding users to a group" on page 172.

To create a new user

1. In the Process Manager portal, click **Admin > Users > Accounts > Manage Users**.
2. On the **Manage Users** page, at the right of the **All Users** title bar, click the **Add User** symbol (a person's head with a green plus sign).
3. In the **Add User** dialog box, on the **Main Information** tab, enter the information to identify the user.

4 (Optional) Add additional user information on the following tabs:

Clone User Lets you clone groups, permissions, or organizations for this user from an existing user.

Process Manager Settings Contains the options for setting the theme, home page, and time zone.

Email Settings Lets you add and delete additional email addresses and set the primary email address.

Phone Numbers Lets you add phone numbers, along with additional details about the phone numbers, for the user.

Messengers ID Lets you add multiple instant messenger IDs for the user, and designate one messenger ID as the primary contact.

Profiles Lets you add profile information for the user.

5 In the **Add User** dialog box, click **Save**.

Chapter 11

Managing categories and data hiearchy

This chapter includes the following topics:

About Incident Management classifications and the data hierarchy

The Incident Management process contains predefined incident classifications. You can use the default classifications immediately or create your own. Support technicians use the classifications to classify the incidents. The incident classifications help route the tickets to the appropriate service queue. The incident classifications also help sort incidents for reports.

If the parent classification is too broad, you can add levels of classifications to make the classification process more granular. You can define up to 10 levels of classifications in the hierarchy tree. The Incident Management hierarchy tree contains your incident classifications.

Set up your classification system to meet your needs without making it too complex. Add the categories that are vital to populating your reports. Provide only enough levels for the workers to accurately classify the incidents.

Too many classifications can make it difficult and time-consuming for workers to select the correct one. Mis-categorization can lead to inaccurate reporting. An overabundance of categories can make trend reporting less meaningful. The more categories that you have, the greater the number of routing rules you must create.

For more information see the following topics:

See “Adding an incident classification” on page 178.

See “Deleting an incident classification” on page 179.

See “Importing incident classifications” on page 180.

See “Exporting incident classifications” on page 180.

See “Migrating categories from Helpdesk Solution 6.x” on page 293.

Video: For more information about managing the classification hierarchy, see ServiceDesk Configuration: Manage Classification Hierarchy on Symantec Connect.

Adding an incident classification

ServiceDesk lets you add incident classifications to the Incident Management process. Your new classifications are available for any incidents that you create and to populate your reports. To add incident classifications, you use the **Add Hierarchy Items** option on the **Hierarchy Data Services** page.

Note: Best practices recommend that you add incident classifications before you set up your rulesets. Best practices recommend that you export and save the `Incident_Management.csv file` before you make any modifications to the Incident Management classification tree.

To add an incident classification

1 In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.

2 On the **Hierarchy Data Service** page, under **Hierarchy Tree**, select the parent classification in which you want the new incident classification to be located.

For example, if you want the classification to appear under **Handheld**, expand **Incident Management > Hardware** and click **Handheld**

3 Under the bottom right corner of the **Hierarchy: Incident Management** section, click **Add Hierarchy Items**.

4 In the **Add Hierarchy Items** dialog box, under **Add New Hierarchy Item (one per line)**, type the classifications that you want to add.

To add multiple items, press **Enter** after each item so that it appears on its own line.

5 When you are finished, click **Add Items**.

See "Exporting incident classifications" on page 180.

See "About Incident Management classifications and the data hierarchy" on page 177.

Deleting an incident classification

ServiceDesk lets you delete incident classifications from the Incident Management process. You can delete the classifications that are not valid or that are no longer useful. For example, you might decide to delete a predefined category that does not apply to your organization. If the classification that you delete contains any subclassifications, they are also deleted. Any incidents that belong to a deleted classifications remain unchanged.

Warning: Best practices recommend that you do not delete a classification after you set up your rulesets and begin using ServiceDesk. Rules that use the incident break. Any incidents that are still assigned to a deleted category do not appear in the reports and searches that are run. Best practices recommend that you export and save the `Incident_Management.csv file` before you make any modifications to the Incident Management classification tree.

To delete an incident classification

1 In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.

2 On the **Hierarchy Data Service** page, under **Hierarchy Tree**, select the parent classification from which you want to delete the classification

For example, if you want to delete a classification that appears under **Handheld**, expand **Incident Management > Hardware** and click **Handheld**.

3 In the **Hierarchy: Incident Management** section, to the right of the classification that you want to delete, click the **Delete** symbol (red X).

4 In the **Message from webpage** dialog box, click **OK**

See "Exporting incident classifications" on page 180.

See "About Incident Management classifications and the data hierarchy" on page 177.

Importing incident classifications

ServiceDesk lets you import incident classifications into the Incident Management process. You can import a `.csv file` that already contains the incident classifications and levels.

For example, you have more than one ServiceDesk server. You set up the incident classifications in the Process Manager portal on your first ServiceDesk server. You can export and save a copy of the `Incident_Management.csv file`. Then, you can import the `Incident_Management.csv file` and use it to populate the incident classifications in the Process Manager portal on your second ServiceDesk server.

Note: Best practices recommend that you import incident classifications before you set up your rulesets. Best practices recommend that you export and save the original `.csv file` before you import the new `.csv file`.

To import incident classifications

1. In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.
2. On the **Hierarchy Data Service** page, on the **Hierarchy Tree** title bar, click the **Actions** symbol (orange lightning) and then click **Import Category**.
3. In the **Import Category** dialog box, browse for and select the `.csv file` to import and then click **Import**.

See “Exporting incident classifications” on page 180.

See “About Incident Management classifications and the data hierarchy” on page 177.

Exporting incident classifications

ServiceDesk lets you export your incident classifications. You can export the `Incident_Management.csv file` from ServiceDesk that contains the incident classifications and levels.

Best practice recommends that you export a copy of the`Incident_Management.csv file` before you begin modifying or deleting your default Incident Management classifications, .

To export incident classifications

1. In the Process Manager portal, click **Admin > Data > Hierarchy Data Service**.
2. On the **Hierarchy Data Service** page, under the **Hierarchy Tree** section, click **Incident Management**.

3. On the right side of the **Hierarchy: Incident Management** title bar, click the **Action** symbol (orange lightning) and then click **Export Category**.
4. In the **File Download** dialog box, click **Save**.
5. In the **Save As** dialog box, select the location where you want to save the `Incident_Management.csv file` and then click **Save**.
6. In the **Download complete** dialog box, click **Close**.

See “Importing incident classifications” on page 180.

See “About Incident Management classifications and the data hierarchy” on page 177.

Chapter 12

Customizing the Process Manager portal

This chapter includes the following topics:

About the Process Manager portal

The Process Manager portal is a Web-based interface that provides access to the ServiceDesk software. Personnel who use ServiceDesk access the portal from their Web browsers and use it to run the ServiceDesk core processes and perform other ServiceDesk activities.

Examples of the tasks that users can perform in the Process Manager portal are as follows:

- Administrators can configure settings for the appearance, operation, and management of the portal.
- Users can create incidents and view knowledge sources such as the knowledge base.
- Process workers can work on incidents, create and work on tickets for other processes, contribute articles, and participate in discussions.

When you log on to Process Manager, the permissions that you are granted determine the elements of the portal that are available to you. If you cannot access a particular portal page or other feature, you probably do not have the appropriate permissions.

Table 12-1 Screen elements of the Process Manager portal

Element	Description
Process Manager portal	The browser window that appears when you open Process Manager. To access the Process Manager portal from the ServiceDesk server, double-click the **Process Manager** shortcut on the desktop. You can also access the Process Manager portal from the **Start** menu; expand **Symantec > Process Manager** and click **Process Manager**.
Site Actions drop-down list	A drop-down list that can appear at the top of the Process Manager portal window. It appears only when you have permission to edit the current Process Manager portal page.
Link	The clickable text that appears at the upper right and lower left of the Process Manager portal window. Examples of links are **Help**, **Account**, and **Logout**.
Tab bar	The horizontal row of tabs that appears near the top of the Process Manager portal window. The pages that appear on the tab bar are root pages.
Tab	A clickable segment of the tab bar. Clicking a tab opens a page or displays one or more menu commands.
Menu bar	The horizontal row of menu commands that appears beneath the tab bar. The contents of the menu bar depend on the tab that you click. Some tabs do not have a menu because they perform a single action. The pages that appear on the menu bar are subpages. Whenever you log on to the Process Manager portal, the portal opens to a specific page. Initially, your permissions determine which page opens. However, you can set a different page to open when you log on.
Menu command	A clickable segment of the menu bar. Clicking a menu command opens a page or displays one or more menu subcommands.
Page or portal page	The entire area that appears beneath the menu bar when you click a tab or a menu command. Most of the work in ServiceDesk is performed on a portal page or on a page that is accessed from a portal page. You can customize portal pages for the entire organization or for users, groups, permissions, or organizational units. Administrators have permission to customize portal pages and to grant customization permissions to other ServiceDesk users. See "About customizing the contents of Process Manager portal pages" on page 184.
Section or Web part	The segments that appear on a Process Manager portal page in the form of Web parts that let you perform actions or enter data. You can customize a portal page by adding, editing, or deleting one or more Web parts.

About customizing the contents of Process Manager portal pages

The Process Manager portal consists of pages, from which all ServiceDesk activities are performed. The portal pages can be customized to meet your specific requirements.

Examples of the customizations that can be made are as follows:

- An administrator configures a different **My Task List** page for each group.
- An individual adds a search capability to their own **Home** page.
- A support manager customizes their **Tickets** page and then shares it with the rest of the support group.
- An administrator customizes a **Process View** page for a specific type of worker. For example, a high-level support technician might need additional actions.

Administrators can perform all the customization actions and can grant customization permissions to other ServiceDesk users. Non-administrator users typically have fewer options for customizing portal pages.

Customizing portal pages consists of the following actions:

- Adding and deleting pages
- Specifying which pages can be customized
- Adding, editing, and deleting the Web parts that appear on a page
- Sharing pages with other users

You can also set a portal page to be the page that opens whenever you log on to the Process Manager portal.

Customizing forms

This chapter includes the following topics:

About customizing forms

In the Process Manager portal, a form is the screen or page that workers and users interact with during a process. The forms feed the process data into the database. For example, a change worker uses the **Request Change** form to submit a new change request. Users use the **Create New Incident** form to submit incidents.

ServiceDesk contains predefined forms for all its processes. These predefined forms are complete and ready to use immediately. However, you can customize any of the forms to meet your organization’s established process requirements.

For example, many organizations customize the Customer Satisfaction Survey form that is sent to the submitting user when an incident is resolved and confirmed. In the survey, the user rates how satisfied they are with the service that they received.

See “About the Customer Satisfaction Survey” on page 188.

The form customization can be performed at different levels and from different places.

Table 13-1 Levels of form customization

Level	Where to edit	What you can customize
The form itself	Workflow Designer For more information about customizing forms, see the Symantec™ Workflow 7.5 User Guide.	Examples of how you can customize a form are as follows: ■ Change the theme or the template style. You can select from a range of theme and template styles or you can create your own. You can also change the form size. ■ Change the text that appears on a form. ■ Change the images that appear on a form. ■ Rearrange the elements on the form. ■ Change error messages. The predefined forms contain the error messages that appear when a required field is not populated. You can edit these error messages. ■ Change the confirmation pages that are presented to users. Several process actions result in a confirmation message being sent to the user. For example, when a user submits an incident, a **Thank You** page appears; when a log on fails, an error page appears. You can change the contents of these pages. ■ Add data to a form. For example, you might add a field to the incident form so that the support technicians can assign the incident to a cost center. ■ Remove data from a form. **Warning:** Use caution when you remove data components from a form. Any of the output variables that those components designate become invalid after the removal, which breaks the process.

Table 13-1 Levels of form customization *(continued)*

Level	Where to edit	What you can customize
Aspects of the form's appearance and behavior in the Service Catalog	Process Manager portal, on the **Edit Form** page. See "Editing a form in the Process Manager portal" on page 187.	On the **Edit Form** page, you can edit the form information on the following tabs: ■ **Form Information** The name, description, and other information regarding the form's display in the Process Manager portal. ■ **WebPart Information** Lets you define the form as a Web part. ■ **User Information** Information about passing the user ID. ■ **Session Information** Information about passing a session ID. ■ **Permissions** Lets you determine who can access a process by setting permissions on the form that provides access to that process. See "Setting permissions for a form" on page 188. ■ **Profiles** Lets you assign a default form profile to the form.

Editing a form in the Process Manager portal

In the Process Manager portal, a form is the screen or page that workers and users interact with during a process. You can customize the aspects of a form's appearance and behavior in the Service Catalog.

See "About customizing forms" on page 185.

To edit a form in the Process Manager portal

1. In the Process Manager portal, click **Admin > Service Catalog Settings**.
2. Under **Browse Category**, select the form's category.
3. In the right pane, at the far right of the form's title bar, click the **Actions** symbol (orange lightning), and then click **Edit Form**.
4. On the **Edit Form** page, edit the information on one or more tabs as necessary.
5. Click **Save**.

Setting permissions for a form

A form is the screen or page that the users and workers interact with during a process. The ServiceDesk forms appear in the Service Catalog. You can determine who can access a process by setting permissions on the form that provides access to that process.

See “About customizing forms” on page 185.

To set permissions for a form

1. In the Process Manager portal, click **Admin > Service Catalog Settings**.
2. Under **Browse Category**, select the form’s category.
3. In the right pane, at the far right of the form’s title bar, click the **Actions** symbol (orange lightning), and then click **Edit Form**.
4. On the **Edit Form** page, click the **Permissions** tab and add or edit permissions as needed.
5. Click **Save**.

About the Customer Satisfaction Survey

After an incident is resolved, the submitting user receives a task to view its history, comments, and other information about its resolution. If the resolution is satisfactory, the user marks the incident as resolved. When the incident resolution is verified, the user can be asked to complete a Customer Satisfaction Survey to rate the service and the resolution. The Incident Management **OnResolutionVerified** ruleset comes with a preconfigured rule that can send out the Customer Satisfaction Survey when an incident is resolved.

You can customize the Customer Satisfaction Survey.

Examples of how you might change the Customer Satisfaction Survey are as follows:

- Change the frequency with which the survey is sent.
  By default, the **OnResolutionVerified** ruleset comes with a preconfigured rule that sends out the Customer Satisfaction Survey. Each time an incident is resolved, there is a 50% chance that the rule sends out the Customer Satisfaction Survey.
  You can change the frequency that the Customer Satisfaction Survey is sent out. Edit the condition in the preconfigured rule that sends out the survey.
  In the Process Manager portal, click **Admin > Process Automation**. Expand **Incident Management** and then click **Service Dashboard**. Expand **Ruleset: OnResolutionVerified** and select the Customer Survey rule. In the title bar, click the **Actions** symbol (orange lightning) and then click **Edit Rule**. On the

Edit Rule page, to the right of the condition, click the **Edit** symbol (note pad and green pencil).

- Change the data that the survey collects.
  You can change the text on the survey form. You can also change the survey questions and the possible responses so that you can track the information that is most important to your organization.
  You can change the appearance and fields of the Customer Satisfaction Survey by editing the `SD.CustomerSurvey` project in Workflow Designer.

For more information about customizing forms and editing the Customer Satisfaction Survey, see the Symantec™ Workflow 7.5 User Guide.

See “About customizing forms” on page 185.

Chapter 14

Configuring Incident Management

This chapter includes the following topics:

Creating incident service queues

The Incident Management process lets you route incidents to service queues. By default, ServiceDesk provides the **Default Incident Queue** service queue, and associates the Support group to it. Before you can configure your automation rules, Symantec recommends that you first create your incident service queues and associate your groups to the queues.

Video: For more information about creating and managing incident service queues, see ServiceDesk Configuration: Create and Manage Service Queues on Symantec Connect.

Service queues consist of a group or multiple groups that you associate with it. You can change users and group without reconfiguring your routing rules. You can add or remove the users that are in the group that you associate with the service queue. You can add or remove the groups that are associated with the service queue.

Note: Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents.

To create an incident service queue

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.
3. On the right side of the page, click **Manage Incident Service Queues**.
4. On the **Active Service Queues** page, click **New Queue**.
5. On the **Create/Edit Service Queue** page, in the **Service Queue Name** field, type the name of the service queue.

   Type a descriptive name of the service queue to make it easy to identify. The name is displayed in the list of service queues on the **Active Service Queues** page.
6. (Optional) Add the service queue location as follows:
   - To the right of the **Queue Location (Optional)** field, click the **Search** symbol (magnifying glass).
   - In the **Location Selection** dialog box, in the **Search Text** field, type your search criteria and click the **Search** symbol (magnifying glass).
   - Select the location and then click **Select Location**.
   - The location appears in the **Queue Location (Optional)** field.

7 In the **Queue Description** field, type a description of the service queue.

8 Add groups to the service queue as follows:

- Under **Security Group Membership**, in the **Search** field, type your group search criteria and click the **Search** symbol (magnifying glass).
- Select the group that you want to add and click **Add Selected**.
  To add additional groups to the service queue, repeat this step.
- The group appears in the **Groups Currently in Queue** field.
  To remove a group from this field, click the group.

9 When you are finished, click **Save Queue**.

10 On the **Active Service Queues** page, click **Close**.

See "Editing incident service queues" on page 192.

See "Deleting incident service queues" on page 193.

Editing incident service queues

You can edit your incident service queues. For example, you need to add another group to a service queue. Edit the service queue and add an additional group to the service queue.

Note: The group-to-service queue relationship is only used during ticket assignment. Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents. Individual ticket assignments can be reset when you reassign them to queue to which they are currently assigned. For example, you remove a group from a queue. To restrict the group's access to the existing tickets, reassign those tickets back to the queue.

Adding and removing groups from queues only affects future assignments and does not affect currently assigned incidents.

To edit an incident service queue

1 In the Process Manager portal, click **Submit Request**.

2 On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.

3 On the right side of the page, click **Manage Incident Service Queues**.

4 On the **Active Service Queues** page, locate the service queue that you want to edit.

5 To the right of the service queue, click the **Edit** link.

6 (Optional) In the **Service Queue Name** field, edit the name of the service queue.

7 (Optional) Change the service queue location as follows:

- To the right of the **Queue Location (Optional)** field, click the **Search** symbol (magnifying glass).
- In the **Location Selection** dialog box, in the **Search Text** field, type your search criteria and click the **Search** symbol (magnifying glass).
- Select the location and then click **Select Location**.
- The location appears in the **Queue Location (Optional)** field.

8 (Optional) In the **Queue Description** field, edit the description of the service queue.

9 (Optional) Remove groups from the service queue.

Under **Groups Currently in Queue** click the group that you want to remove.

10 (Optional) Add groups to the service queue as follows:

- Under **Security Group Membership**, in the **Search** field, type your group search criteria and click the **Search** symbol (magnifying glass).
- Select the group that you want to add and click **Add Selected**.
  To add additional groups to the service queue, repeat this step
- In the **Service Queue Management** dialog box, under **Service Queue Group Association**, click the **Add** symbol (green plus sign).
- The group appears in the **Groups Currently in Queue** field..

11 When you are finished, click **Save Queue**.

12 On the **Active Service Queues** page, click **Close**.

See “Creating incident service queues” on page 191.

See “Deleting incident service queues” on page 193.

Deleting incident service queues

You can delete incident service queues. Symantec recommends that you delete a service queue before you create your routing rules. Symantec also recommends that after you start routing incidents to a service queue, that you do not delete that service queue.

If you must delete a service queue after incidents are routed to it, make sure that the following conditions are met:

- Modify all the rules that route incidents to the queue and route them to another queue.

  Warning: If you delete a service queue before you modify the routing rules that route incidents to that queue, the routing rules error out.

- Remove the groups from the queue.

Note: Deleting a service queue does not affect the incidents that are currently assigned to the groups that are associated to the queue. Incidents previously routed to a queue remain assigned to that queue's groups, even if you delete the queue.

To delete an incident service queue

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.
3. On the right side of the page, click **Manage Incident Service Queues**.
4. On the **Active Service Queues** page locate the service queue that you want to delete.
5. Note that you should not complete the next step unless you are sure that you want to delete the routing rule.
6. To the right of the service queue, click the **Remove** link.
7. Click **Close**.

See “Editing incident service queues” on page 192.

See “Creating incident service queues” on page 191.

Creating email templates for Incident Management

Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. You can create email templates and associate them with actions. For example, a VIP submits an incident. A preconfigured email can be sent to a specific user or group notifying them of a VIP incident submittal. The email template can be preconfigured with subject line and message information.

Note: The **Send Email** process type action, on the Incident Management **Process View** page uses the Incident Management email templates. You may want to create email templates specifically for your technicians to use when working an incident ticket.

Video: For more information about creating email templates and creating rules to send emails, see ServiceDesk Configuration: Manage Email Templates in ServiceDesk on Symantec Connect.

To create an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: INCIDENT-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section, click **Add Email Template**.
5. In the **Add Email Template** dialog box, in the **Template Type** area, select one of the following template types:

Process Event	■ Lets you create an email template for process event rulesets. ■ The list of available fields in the **Available Fields** section corresponds specifically to process events. ■ These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset. For example, a process event email template can be delivered from the **OnIncidentReceived** ruleset.

Data Event	■ Lets you create an email template for a specific data event ruleset. ■ Lets you use the **Event** field to assign a data event category to the email template. ■ The list of available fields in the **Available Fields** section corresponds specifically to the type of data events that you select. ■ These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event. Note that the email template is only available for its corresponding data event ruleset. For example, you create a ruleset for *<OnDocumentAdded>* data event. You create a rule to deliver an email anytime a document is added to the incident ticket. When you create the email template for this rule, you must select **DocumentAdded** in the **Event** drop-down list.

6 (Optional) If you selected **Data Event**, in the **Event** drop-down list, select a data event.

For example, you want to create an email template so you can send an email out when a comment is added to an incident ticket. In the **Event** drop-down list, click **CommentAdded**.

7 In the **Name** field, type the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8 In the **From** field, type the name of the user or group sending the message.

9 (Optional) In the **Description** field, type the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

10 (Optional) In the **Subject** field, type the subject of the email.

11 (Optional) In the **Body** field, type the message.

If you want to let the end user's reply to the emails and have ServiceDesk capture those emails, you must add a reply code.

Use the following format:

{IID= *${WorkflowTrackingId}*}

${WorkflowTrackingId} is the variable that is added to the body of the email when you select **Workflow Tracking ID** in the **Available Fields** section.

12 (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
- Repeat this step until you are finished adding additional information.

13 When you are finished, click **Save**.

See “Editing email templates for Incident Management” on page 197.

See “Deleting email templates for Incident Management” on page 199.

Editing email templates for Incident Management

You can edit email templates if necessary. If you edit an email template before you use it in the **Send Email** action of a rule, you can edit all parts of the template. If you edit an email template after you use it in the **Send Email** action of a routing rule, do not edit the **Template Type**. **Template Type** makes the email template available only to rulesets that correspond to the event type that you select.

For example, process event email templates are only available to process event type rulesets. If you want to use that same email template for a different template type, you need to create a new email template. Then, you need to create a new rule to deliver it.

Note: Do not change the **Template Type** in an email template after you use it in a rule. Changing the **Template Type** appears to remove the selected email template from the **Send Email** action of the rule. Because the rule uses the ID number of the email template, the email is still sent, but it may not display the information as expected.

To edit an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: INCIDENT-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to edit. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Edit Email Template**.
5. (Optional) In the **Edit Email Template** dialog box, in the **Template Type** area, change the **Template Type** only if you have not created a rule that delivers the email template.

   Process Event

   - Lets you create an email template for process event rulesets.
   - The list of available fields in the **Available Fields** section corresponds specifically to process events.
   - These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset.

     For example, a process event email template can be delivered from the **OnIncidentReceived** ruleset.

   Data Event

   - Lets you create an email template for a specific data event ruleset.
   - Lets you use the **Event** field to assign a data event category to the email template.
   - The list of available fields in the **Available Fields** section corresponds specifically to the type of data events that you select.
   - These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event.

     Note that the email template is only available for its corresponding data event ruleset.

     For example, you create a ruleset for *<OnDocumentAdded>* data event. You create a rule to deliver an email anytime a document is added to the incident ticket. When you create the email template for this rule, you must select **DocumentAdded** in the **Event** drop-down list.

6 (Optional) If you changed the template type to **Data Event**, in the **Event** drop-down list, select a data event.

For example, you want to edit the email template so you can send an email out when a comment is added to an incident ticket. In the **Event** drop-down list, click **CommentAdded**.

7 (Optional) In the **Name** field, edit the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8 (Optional) In the **From** field, edit the name of the user or group sending the message.

9 (Optional) In the **Description** field, edit the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

10 (Optional) In the **Subject** field, edit the subject of the email.

11 (Optional) In the **Body** field, edit the message.

12 (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
- Repeat this step until you are finished adding additional information.

13 (Optional) Remove additional information from a specific area of the email.

14 When you are finished, click **Save**.

See “Creating email templates for Incident Management” on page 194.

See “Deleting email templates for Incident Management” on page 199.

Deleting email templates for Incident Management

You can delete email templates if necessary. If you want to delete an email template before creating a rule that delivers it, you can delete it without taking any other actions. To delete an email template after creating a rule that delivers it, you must first edit the rule to use a different email template. You can also delete the rule and then delete the email template.

To delete an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: INCIDENT-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to delete.
5. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Delete Email Template**.
6. In the **Message from webpage** dialog box, click **OK**

See “Creating email templates for Incident Management” on page 194.

See “Editing email templates for Incident Management” on page 197.

Incident Management Process Automation rules components

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process. You control the events that trigger a rule to run, the conditions for rule evaluation, and the action that occurs once the conditions are met.

The Process Automation rules contain three main components:

- **Rulesets**
  Rulesets function as triggers that initiate a rule to run. Rulesets can contain multiple rules. Rulesets are classified either process event types or data event types.
  Process Events let you determine what happens at specific points in the lifecycle of an incident.
  For example, **OnIncidentReceived** is a process event ruleset that lets you determine what happens at the incident creation point of the process.
  Data Events let you determine what happens if data changes at any point during the lifecycle of an incident.
  For example, **CommentAdded** is a data event ruleset that lets you take an action whenever a comment is added to an incident.
  By default, the **OnAnySlaMissed** and **OnAnySlaCompletedLate** rulesets are enabled. Only enable the data event type rulesets that you plan to use.
  See “Incident Management automation rules rulesets” on page 201.

- **Conditions**

  Conditions determine when an action should occur. You can add multiple conditions to a rule. You can configure them to meet all of the conditions or only some of the conditions. Conditions support the “Not” statement, with a **Not** checkbox.

  For example, you can add the **Affected User** condition to the rule that you create for the **OnIncidentReceived** ruleset. This condition lets you evaluate the new incident by who was affected.

  See “Incident Management automation rules conditions” on page 203.

- **Actions**

  Actions are the result of a rule when the conditions are met.

  For example, you can add the **Route Incoming Incident** action to the rule that you create for the **OnIncidentReceived** ruleset. This action lets you control which service queues receive which tickets when the conditions are met.

  See “Incident Management automation rules actions” on page 208.

See “Configuring new automation rules for Incident Management” on page 210.

Incident Management automation rules rulesets

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.

See “Incident Management Process Automation rules components” on page 200.

See “Configuring new automation rules for Incident Management” on page 210.

Rulesets function as triggers that initiate a rule to run. Rulesets are classified as either process event or data event types.

Table 14-1 Incident Management rulesets

Ruleset	Description	Event type
OnIncidentReceived	Runs when an incident is created.	Process Event
OnOwnershipChanged	Runs when the ownership of a ticket is assigned or changed to a specific person.	Process Event
OnResolutionVerified	Runs when the affected contact verifies the resolution of an incident.	Process Event
OnTicketAssigned	Runs when an incident is assigned to a Service Queue.	Process Event

Table 14-1 Incident Management rulesets *(continued)*

Ruleset	Description	Event type
OnTicketClosed	Runs when an incident is finally closed .	Process Event
OnIncidentEdited	Runs when a technician edits the details of a ticket.	Process Event
OnTicketPlacedOnHold	Runs when an incident is put on hold.	Process Event
OnTicketRemovedFromHold	Runs when an incident is removed from hold.	Process Event
OnTicketReopened	Runs when a closed incident is reopened.	Process Event
OnTicketResolved	Runs when an incident is resolved.	Process Event
OnVerificationTimeout	Runs if the primary contact does not verify the incident within the verification window.	Process Event
OnAnySlaCompletedLate	Runs when an SLA is complete late: Initial Response or Resolution.	Data Event
OnAnySlaMissed	Runs if an SLA is reached before action is completed: Initial Response or Resolution.	Data Event
ContactAdded	Runs if a contact is added to an incident. The ruleset is not enabled by default.	Data Event
DocumentAdded	Runs if a document is added to an incident. For example, you add an asset to an incident. The ruleset is not enabled by default.	Data Event
ProcessReferenceCreated	Runs when a process reference is added to an incident. The ruleset is not enabled by default.	Data Event
TaskAssignmentCreated	Runs when a subtask is assigned on an incident. The ruleset is not enabled by default.	Data Event

Table 14-1 Incident Management rulesets *(continued)*

Ruleset	Description	Event type
TaskCompleted	Runs when a subtask on a ticket is completed. The ruleset is not enabled by default.	Data Event

Incident Management automation rules conditions

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.

See "Incident Management Process Automation rules components" on page 200.

See "Configuring new automation rules for Incident Management" on page 210.

Conditions determine when an action should occur. You can add multiple conditions to a rule.

Table 14-2 Ruleset conditions

Condition	Description	Condition availability
Affected Assets	Options: ■ If any assets are attached to an incident ■ If specific assets are attached to an incident	All rulesets
Affected Business Service	If a specific service is attached to an incident	All rulesets
Affected Departments	Options: ■ If an affected department is set ■ If a specific department is set	All rulesets
Affected Location	Options: ■ If an affected location is set ■ If a specific location is set	All rulesets

Table 14-2 Ruleset conditions *(continued)*

Condition	Description	Condition availability
Affected User	Options: ■ If the affected user is also the submitter ■ If the affected user is in a specific group ■ If the affected user is a VIP ■ If the affected user is a specific user	All rulesets
Any	Runs the rule on all incidents	All rulesets
Classification	Options: ■ Runs the rule on all incidents ■ If an Incident has been classified If a specific classification is set ■ If a specific subclassification is set	All rulesets
Contacts	Options: ■ If a contact exists ■ If a contact on the incident is part of a specific group ■ If a contact on the incident is a specific contact	All rulesets
Impact	Options: ■ If an impact is set ■ If a specific impact is set	All rulesets
Incident Description	Options: ■ If the descriptions contains text ■ If the description starts with text	All rulesets
Incident Title	Options: ■ If the title contains text ■ If the title starts with text	All rulesets
Priority	Options: ■ If a priority is set ■ If a specific priority is set	All rulesets

Table 14-2 Ruleset conditions *(continued)*

Condition	Description	Condition availability
Process Name	Options: - If the process name contains text - If the process name starts with text - If the process name is a specific text	All rulesets
Random	Random pass based on a target % between 0 and 100	All rulesets
Request Channel	Options: - Incident is created from the service catalog - Incident is created from the Technician Page - Incident is created from an Email - Incident is created from a Custom entry point	All rulesets
SLA Exists	Options: - SLA Exist for Milestone: Initial Response or Resolution. - A specific SLA exist	All rulesets
SLA Status (by Escalation)	Options: - If it is completed late for a specific milestone - If late for a specific milestone - If it is satisfied for a specific milestone - If working for a specific milestone	All rulesets
SLA Status (by Level)	Options: - If it is completed late for a specific SLA level - If late for a specific SLA level - If it is paused for a specific SLA level - If it is satisfied for a specific SLA level - If working for a specific SLA level	All rulesets

Table 14-2 Ruleset conditions *(continued)*

Condition	Description	Condition availability
Urgency	Options: - If an urgency is set - If a specific urgency is set	All rulesets
SLA Type	Is set to a specific type	**OnAnySlaCompletedLate** **OnAnySlaMissed**
Comment	Options: - Added comment contains text - Added comment starts with text - Added comment is specific text	**CommentAdded**
Commenter	Is a specific user	**CommentAdded**
Contact	Options: - Added contact is primary contact - Added contact is VIP - Added contact is specific user	**ContactAdded**
Contact Location	Options: - Added contact location contains text - Added contact location starts with text - Added contact location is specific text	**ContactAdded**
Attachment Name	Options: - Added document name contains text - Added document name starts with text - Added document name is specific text	**DocumentAdded**
Attachment Size	Options: - Added document is larger than KB - Added document is smaller than KB	**DocumentAdded**

Table 14-2 Ruleset conditions *(continued)*

Condition	Description	Condition availability
Process Reference Type	Added process reference is a specific type	**ProcessReferenceCreated**
Process Reference URL	Options: ■ Added process reference URL contains text ■ Added process reference URL starts with text ■ Added process reference URL is specific text	**ProcessReferenceCreated**
Child Process Name	Options: ■ Added child process name contains text ■ Added child process name starts with text ■ Added child process name is specific text	**ProcessRelationshipCreated**
Child Process ServiceID	Options: ■ Added child process Service ID contains text ■ Added child process Service ID starts with text ■ Added child process Service ID is specific text	**ProcessRelationshipCreated**
Process Relationship Name	Options: ■ Added process relationship name contains text ■ Added process relationship name starts with text ■ Added process relationship name is specific text	**ProcessRelationshipCreated**
Task Assignee	Options: ■ New task assignee contains text ■ New task assignee starts with text ■ New task assignee is specific text	**TaskAssignmentChanged**

Table 14-2 Ruleset conditions *(continued)*

Condition	Description	Condition availability
Task Name	Options: ■ New task name contains text ■ New task name starts with text ■ New task name is specific text	**TaskAssignmentChanged** **TaskCreated** **TaskCompleted**
Task Priority	Options: ■ New task priority contains text ■ New task priority starts with text ■ New task priority is specific text	**TaskAssignmentChanged** **TaskCreated** **TaskCompleted**

Incident Management automation rules actions

The Incident Management Process Automation rules consist of rulesets, conditions, and actions. These components let you control your Incident Management process.

See "Incident Management Process Automation rules components" on page 200.

See "Configuring new automation rules for Incident Management" on page 210.

Actions are the result of a rule when the conditions are met. You can add multiple actions to a rule.

Table 14-3

Action	Description	Action availability
Add Contact	Adds a contact to the incident and defines contact information. Options: ■ Define Contact Type. ■ Define Is Primary. ■ Define User.	All rulesets
Do Nothing	Take no action	All rulesets

Table 14-3 *(continued)*

Action	Description	Action availability
Grant Ticket Access	Sets the permissions for the ticket Options: ■ Set Can Administrate ■ Set Can Edit ■ Set Can View Grants access to ticket Options: ■ To User ■ To Group	All rulesets
Modify SLA	Options: ■ Complete for Milestone ■ Delete for Milestone ■ Reset for Milestone ■ Resume for Milestone.	All rulesets
Pause SLA	By Milestone	All rulesets
Remove Ticket Access	Options: ■ From Everyone ■ From Specific User ■ From Specific Group	All rulesets
Send Email	Send Email Options: ■ To Affected User ■ To Submitter ■ To all Assignees ■ To Owner ■ To Resolver ■ To Specific Group ■ To Specific User	All rulesets Data event email templates are only available to the specific events to which they are tied.
Send Incident To Workflow	Defines URL of Workflow, evokes workflow, and passes session ID for incident	All rulesets

Table 14-3 *(continued)*

Action	Description	Action availability
Set SLA	Sets SLA for an incident and define Options: ■ Replace existing SLA. ■ SLA calculation start time (Submit Date / Now)	All rulesets
Route Incoming Ticket	Assign ticket to Service Queue Options: ■ To Specific Service Queue ■ Based on Category Table ■ Based on Location Table	Process event type rulesets
Set Impact	Set Impact for Incident	Process event type rulesets
Set Location	Set incident location Options: ■ To Affected User's Location ■ To Specific Location	Process event type rulesets
Set Owner	Assign Owner for an incident to a specific user	Process event type rulesets
Set Priority	Set Priority for Incident	Process event type rulesets
Reassign Current Incident Task	Reassign incident to a specific queue	Data event type rulesets

Configuring new automation rules for Incident Management

You can configure rulesets for the Incident Management process. The set of rulesets is known as the automation library.

Video: For more information about configuring new automation rules for Incident Management, see the following on videos Symantec Connect:

- ServiceDesk: Rulesets Overview
- ServiceDesk Configuration: Data Mapping and Routing Rules
- ServiceDesk: SLA Framework Overview

- ServiceDesk Configuration: Manage Email Templates

See “Incident Management Process Automation rules components” on page 200.

See “About Incident Management” on page 30.

To configure a new automation rule for Incident Management

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Service Dashboard: INCIDENT-MGMT** section, locate the ruleset to which you want to add a rule.
4. To the right of the ruleset, click the **Actions** symbol (orange lightning) and then click **Add Rule**.

   See “Incident Management automation rules rulesets” on page 201.
5. In the **Add Rule** dialog box, in the **How groups are evaluated** area, select one of the following options:
   - **All groups must be met to satisfy**
   - **Any group satisfies**
6. Click **Add Group**.
7. Click **Add Condition**.
8. In the **How conditions in this group are evaluated** area, select one of the following options:
   - **All conditions must be met to satisfy**
   - **Any condition satisfies**
9. In the **Add Condition** drop-down list, select a condition for the rule.

   See “Incident Management automation rules conditions” on page 203.
10. Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the condition.
11. (Optional) Check **Not** to set a condition that inverts the selected condition so that the rule only executes if the condition is false.

    The **Not** operator applies only to the condition, not to the entire rule.
12. Click the **Plus** symbol (blue plus sign) to add the condition.
13. (Optional) Click the Plus symbol (blue plus sign) to add another condition. Repeat Steps 9 - 13.
14. Click **Add Action.**

15. In the **Actions** drop-down list, select an action to execute if the condition is met.

    See “Incident Management automation rules actions” on page 208.

16. Select an option from each drop-down list that appears or type the information in the specified field to narrow the parameters of the action.
17. Click the Plus symbol (blue plus sign) to add the action.
18. (Optional) Click the Plus symbol (blue plus sign) to add another action. Repeat Steps 15 - 18.
19. In the Disposition (on successful actions) area, select one of the following options:
    - **Continue**
    - **Stop**
20. (Optional) Click **Advanced** and select which of the following actions you want to include in the ruleset:

Run next rule if condition fails to evaluate	If an error occurs during the evaluation of an incident's conditions, the ruleset continues to execute (if not checked, the ruleset does not execute).
Run next rule if action fails to execute	If an error occurs while the condition executes, the ruleset attempts to continue executing.

21. Click **Save.**

About incident templates

Incident templates are special incident forms containing predefined, standard values for common issues. Using templates speeds the entry of incidents and helps to standardize and increase the accuracy of the incident information.

For example, users frequently call support to restart a server, reset a password, or clear a printer jam. You can create an incident template that contains the appropriate category, type, title and description, and a reference to a related knowledge base article. The next time a user calls with that problem, the support technician can use the template to help create an incident with the correct values.

Before you create an incident template, be sure of its purpose. Incident templates are meant to handle Incident Management issue only, such as to report break or fix issues. Create Service Catalog processes for other types of requests that occur frequently. For example, you might create a Service Catalog process that requests software or equipment or that requests HR to process a new hire.

Incident templates are available only for the advanced incident form that the support technicians use. The templates are created and used within the advanced incident form. A template can be associated with a specific user or it can be shared globally. Incident templates can be edited and updated at any time based upon the changes that occur within your environment.

See “About the Service Catalog and service items” on page 165.

See “Creating an incident template” on page 213.

Creating an incident template

You can use the advanced form to create an incident template. You can create an incident template while creating an incident. The next time you create an incident for a similar issue, you can use this template to fill in some of the information automatically. You can also open the advanced form and create an incident template whenever one is needed.

See “About incident templates” on page 212.

To create an incident template

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Requests** page, under **Service Catalog**, click **IT Services**.
3. On the right side of the page, click **Submit Incident (Advanced)**.
4. On the **Create Incident** page, enter only the information that needs to appear in the template.
5. Click **Save As Template**.
6. On the **Incident Template** page, provide information to identify and describe this template.
7. Check **User Only Template** if the template is only for your use. Uncheck **User Only Template** if the template is for all users to use.

8 (Optional) Click **View Attachments Details** to view lists of all the items that are attached to the template. Click **View Basic Details** to view the general information and additional classifications information.

9 Click **Save Template**

10 On the **Create Incident** page, you can continue to create an incident or cancel it.

Note that canceling the incident does not affect the template that you created.

About subtask templates

Subtask templates increase the speeds of the subtask assignment process. They standardize subtask information and increase the accuracy .When you create a subtask, you can use a template to quickly fill in some of the subtask information.

For example, a common subtask in your environment requires a specific worker or group to check a user’s Active Directory permissions. You can create a template that contains the title, description, and priority. The next time that subtask is required for a specific incident, you can use the relevant template to help create the subtask.

See “Creating subtask templates” on page 214.

Creating subtask templates

You can use subtask to break up the actions that are needed to resolve an incident. Then, you can assign those subtasks to other personnel. For the subtasks that are repeatable, you can create subtask templates. After you create a subtask template, you can use the template to create identical subtasks. The template fills in the information automatically for the new subtask.

To create a subtask template

1 In the Process Manager portal, click **Submit Request**.

2 On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.

3 On the right side of the page, click **Manage Incident Subtask Templates**.

4 On the **Manage Subtask Templates** page, click **Add Template**.

5 Under **Subtask Template’s Details**, in the **Template Name** field, type a descriptive name for the email template.

Type a name that makes the subtask easy to identify a list of subtask templates.

6 Click **Add Task**.

7 On the **Create Subtask** page, in the **Task Title** field, type the title of the subtask

8 In the **Task Priority** drop-down list, select the priority for the subtask.

9 Assign the incident to a user as follows:

- To the right of the **Assign to user** field click the **Search** symbol (magnifying glass).
- In the **User Selection** dialog box, in the **Search Text** field, type the first name, last name, or part of an email address. Then, click the **Search** symbol (magnifying glass).
- Select the user and then click **Select User**.

10 In the **Task Details** field, type instructions for completing the subtask.

11 When you are finished, click **Save Subtask**.

12 Click **Save Template**.

The subtask template is displayed in the **Manage Subtask Templates** dialog box, in the **Subtask Template's Details** section.

13 On the **Manage Subtask Templates** page, click **Finished Managing Templates**.

See "About subtask templates" on page 214.

See "Deleting subtask templates" on page 216.

See "Editing subtask templates" on page 215.

On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**

Editing subtask templates

After you create your subtask template, you may need to edit it. For example, you may need to assign the subtask to a different user or add additional information to the task details.

To edit a subtask template

1 In the Process Manager portal, click **Submit Request**.

2 On the **Submit Request** page, in the **Service Catalog** section, click **Administrative Services**.

3 On the right side of the page, click **Manage Incident Subtask Templates**.

4 On the **Manage Subtask Templates** page, locate the subtask template that you want to edit.

5 To the right of the subtask template, click the **Edit** link.

6 Under **Subtask Template's Details**, perform any of the following actions:

Change the descriptive name for the email template.	In the **Template Name** field, type a name that makes the subtask easy to identify a list of subtask templates.
Remove a task from the subtask template.	To the right of the task that you want to remove, click the **Remove** link.
Edit a task in the subtask template.	■ To the right of the task that you want to edit, click the **Edit** link. ■ On the **Create Subtask** page, modify the **Subtask Details** information as needed. ■ Click **Save Subtask**.
Add a task to the subtask template.	■ Click the **Add Task**. ■ On the **Create Subtask** page, provide the required **Subtask Details** information. ■ Click **Save Subtask**.

7 Click **Save Template**.

8 Click **Finished Managing Templates**.

See "Creating subtask templates" on page 214.

See "Deleting subtask templates" on page 216.

Deleting subtask templates

After you create your subtask templates, you may need to delete an obsolete subtask template.

To delete a subtask template

1 In the Process Manager portal, click **Submit Request**.

2 On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**.

3 On the right side of the page, click **Manage Incident Subtask Templates**.

4 On the **Manage Subtask Templates** page, locate the subtask that you want to delete.

5 To the right of the subtask template, click the **Remove** link.

6 On the **Manage Subtask Templates** page, click **Finished Managing Templates**.

See “Creating subtask templates” on page 214.

See “Editing subtask templates” on page 215.

Chapter 15

Configuring Change Management

This chapter includes the following topics:

About the Change Management process

The Change Management process ensures that standardized methods and procedures are used to handle all changes efficiently and promptly. The process minimizes the effect of any related incidents upon service. Using Change Management improves the reliability and responsiveness of IT services and processes, leading to a higher turnaround of changes. It also reduces rework and the duplication of effort. Standard or common change requests can be expedited. The use of automation rules enables customization without having to edit the workflow directly. The process includes the ability to define and use templates for quickly completing a change plan.

See “About Change Management” on page 32.

The Change Management process is initiated when someone requests a change.

The change manager who provides the initial approval of a change request also selects the change type. The change type determines the number of steps that the change implementation requires. It also determines the number of workers who must be involved in each step.

When a task is assigned to multiple workers, all the assignees must complete the task for the change request to advance to the next stage. The change manager can complete tasks on behalf of the task assignees by checking the **Work Tasks Assigned To Others** check box on the change request’s **Process View** page. This option helps move the process forward if a task assignee is unavailable, on vacation, or otherwise unable to work the task.

The Change management process consists of the following states:

- Received
- Planned
- Reviewed
- Closed

During the planning phase, the change manager can select one of two variations to tailor the process to the request: Standard or Emergency.

A standard plan change is commonly requested and performed, meaning that procedures, risk and cost are well-understood and CAB approval is not necessary. Essentially, the Planned state is skipped. For example, once a computer has become obsolete, it experiences a standard change of repurposing or disposal. A standard change is usually scheduled for a later time to coincide with maintenance windows or a release. Typically, an organization has a one-to-one mapping between standard plans and plan templates. This one-to-one mapping is so that if the Standard type is selected, the change manager can find the matching template, and load the plan details.

An emergency change cannot be scheduled for later. If it is designated as an emergency, then it should be implemented immediately following approval by the E-CAB. Like the Standard plan type, the plan details are not required before submission to the CAB.

Creating email templates for Change Management

Before you can configure rules to send out email notifications, you must first create your email templates for those notifications. You can create email templates and associate them with actions. For example, if a change management request requires the approval of a director-level individual, a preconfigured email can be sent to that individual. The email template can be preconfigured with subject line and message information.

Note: The **Send Email** process type action, on the Change Management **Process View** page uses the Change Management email templates. You may want to create email templates specifically for your change analyst, approvers, and others to use when working a change request ticket.

To create an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Service** page, expand **Change Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: CHANGE-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section, click **Add Email Template**.
5. In the **Add Email Template** dialog box, in the **Template Type** area, select one of the following template types:

Process Event	■ Lets you create an email template for process event rulesets. ■ The list of available fields in the **Available Fields** section corresponds specifically to process events. ■ These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset. For example, a process event email template can be delivered from the **OnChangeReceived** ruleset.

Data Event	■ Lets you create an email template for a specific data event ruleset. ■ Lets you use the **Event** field to assign a data event category to the email template. ■ The list of available fields in the **Available Fields** section corresponds specifically to the type of data events that you select. ■ These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event. Note that the email template is only available for its corresponding data event ruleset. For example, you create a ruleset for *<OnDocumentAdded>* data event. You create a rule to deliver an email anytime a document is added to the change request ticket. When you create the email template for this rule, you must select **DocumentAdded** in the **Event** drop-down list.

6 (Optional) If you selected **Data Event**, in the **Event** drop-down list, select a data event.

For example, you want to create an email template so you can send an email out when a comment is added to a change ticket. In the **Event** drop-down list, click **CommentAdded**.

7 In the **Name** field, type the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8 (Optional) In the **Description** field, type the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

9 In the **From** field, type the name of the user or group sending the message.

10 (Optional) In the **Subject** field, type the subject of the email.

11 (Optional) In the **Body** field, type the message.

If you want to let the end user's reply to the emails and have ServiceDesk capture those emails, you must add a reply code.

Use the following format:

{IID= *${WorkflowTrackingId}*}

${WorkflowTrackingId} is the variable that is added to the body of the email when you select **Workflow Tracking ID** in the **Available Fields** section.

12 (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
- Repeat this step until you are finished adding additional information.

13 When you are finished, click **Save**.

See “Editing email templates for Change Management” on page 222.

See “Deleting email templates for Change Management” on page 224.

Editing email templates for Change Management

You can edit email templates if necessary. If you edit an email template before you use it in the **Send Email** action of a rule, you can edit all parts of the template. If you edit an email template after you use it in the **Send Email** action of a rule, do not edit the **Template Type**. **Template Type** makes the email template available only to rulesets that correspond to the event type that you select.

For example, process event email templates are only available to process event type rulesets. If you want to use that same email template for a different template type, you need to create a new email template. Then, you need to create a new rule to deliver it.

Note: Do not change the **Template Type** in an email template after you use it in a rule. Changing the **Template Type** appears to remove the selected email template from the **Send Email** action of the rule. Because the rule uses the ID number of the email template, the email is still sent, but it may not display the information as expected.

To edit an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Change Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: CHANGE-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to edit. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Edit Email Template**.
5. (Optional) In the **Edit Email Template** dialog box, **Template Type** area change the **Template Type** only if you have not created a rule that delivers the email template.

Process Event

- Lets you create an email template for process event rulesets.
- The list of available fields in the **Available Fields** section corresponds specifically to process events.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for a process event ruleset.

  For example, a process event email template can be delivered from the **OnChangeReceived** ruleset.

Data Event

- Lets you create an email template for a specific data event ruleset.
- Lets you use the **Event** field to assign a data event category to the email template.
- The list of available fields in the **Available Fields** section corresponds specifically to the type of data events that you select.
- These email templates appear in the list of available email templates when you create a rule to deliver an email for that specific data event.

  Note that the email template is only available for its corresponding data event ruleset.

  For example, you create a ruleset for *<OnDocumentAdded>* data event. You create a rule to deliver an email anytime a document is added to the change request ticket. When you create the email template for this rule, you must select **DocumentAdded** in the **Event** drop-down list.

6 (Optional) If you changed the template type to **Data Event**, in the **Event** drop-down list, select a data event.

For example, you want to edit the email template so you can send an email out when a comment is added to a change ticket. In the **Event** drop-down list, click **CommentAdded**.

7 (Optional) In the **Name** field, edit the name for the email template.

This name displays on the **Notification Templates** page, in the **Email Templates** section.

8 (Optional) In the **Description** field, edit the description of the email template.

This description displays on the **Notification Templates** page in the **Email Templates** section.

9 (Optional) In the **From** field, edit the name of the user or group sending the message.

10 (Optional) In the **Subject** field, edit the subject of the email.

11 (Optional) In the **Body** field, edit the message.

12 (Optional) Add additional information to a specific area of the email.

- In the **Add To** area, select the field (**From**, **Subject**, or **Body**) to which you want to add the additional information.
- Then, in the **Available Fields** section, select the fields that you want to add.
- Repeat this step until you are finished adding additional information.

13 (Optional) Remove additional information from a specific area of the email.

14 Click **Save**.

See "Creating email templates for Change Management" on page 219.

See "Deleting email templates for Change Management" on page 224.

Deleting email templates for Change Management

You can delete email templates if necessary. If you need to delete an email template before creating a rule that delivers it, you can delete it without taking any other actions. To delete an email template after you create a rule that delivers it, you need to edit the rule and select a different email template. You can also delete the rule and then delete the email template.

To delete an email template

1. In the Process Manager portal, click **Admin > Process Automation**.
2. On the **Available Services** page, expand **Incident Management** and then click **Service Dashboard**.
3. On the **Automation Rules** page, in the **Actions: CHANGE-MGMT** section, click **Manage Email Templates**.
4. On the **Notification Templates** page, in the **Email Templates** section locate the email template that you want to delete.
5. To the right of the email template, click the **Action** symbol (orange lightning) and then click **Delete Email Template**
6. In the **Message from webpage** dialog box, click **OK**.

See "Creating email templates for Change Management" on page 219.

See "Editing email templates for Change Management" on page 222.

Configuring Change Management

To configure change management you define the change manager group. Next you configure access to the Service Catalog items and to the change request process view. Then you set up email templates. Finally, you configure automation rules.

Note: The process skips CAB approval for Standard changes; however, the OnCabApproval ruleset executes in this case. If this action is not desirable, you can add a ruleset the top of your ruleset that aborts execution if the change type is Standard.

Table 15-1 Process for configuring Change Management

Step	Action	Description
Step 1	Define your Change manager group or groups	Your organization may have several different groups responsible for managing incoming change requests. Which group manages the incoming change may depend on the category, location, or other attributes of the request. You must create these groups in the portal and add people to them as needed.

Table 15-1 Process for configuring Change Management *(continued)*

Step	Action	Description
Step 2	Configure Access to the Service Catalog Items	ServiceDesk Installation adds three service catalog items: Request Change, Manage CABs, and Manage Change Templates. By default, the Request Change item is accessible to anyone in the All Users group. However, this form is contained in the ServiceDesk category, which is not accessible to all users. If this access level is not desirable, you should change it in **Admin > Service Catalog Settings**. Select to edit categories or forms and then add permissions as desired. Manage CABs and Manage Change Templates are only accessible to Administrators by default. You may want to grant access to these items to your change manager group or groups.
Step 3	Configure Access to the Change Request Process View	The process view page for Change Management is very robust. The page contains a full description of the request. It also contains the current implementation plan, history of the ticket, current assignments, etc. You can grant access to other users or groups to the full view in the **Admin > Portal > Manage Pages** screen. The page is located under the Process View Pages category and is called **SD Change View**. Select **Edit Page**, and then open the **Permissions** tab.
Step 4	Set up Email Templates	In Change Management, you have complete control over who receives notifications and what those notifications look like. You have control over when the notifications are sent, without ever needing to open the process in the Workflow Designer. You can customize the templates by determining what your notification rules should be and what the notifications should contain. For example, you may want to notify the requestor as soon as the system receives the ticket. You may want to notify the requestor after the ticket has been approved at each level. Email templates for this process can be configured in **Admin > Automation Rules**. See “Creating email templates for Change Management” on page 219.

Table 15-1 Process for configuring Change Management *(continued)*

Step	Action	Description
Step 5	Configure Automation Rules	This step requires time for testing and configuration. To set up automation rules properly, it's important to understand the underlying process. The actions available in the rule builder give you the ability to change information about the ticket while the ticket executes. For example, when a ticket is received, you might check if the requestor is a VIP and automatically set the ticket owner and send email. Typically, the first ruleset you want to configure is the **OnChangeReceived** ruleset. This ruleset is enacted upon the receipt of a change request.

About change templates

After you create a change request, you can use a template to fill in the following change request information:

- **Risk Assessment Score**
- **Cost of Implementing**
- **Cost of Not Implementing**
- **Implementation Plan**
- **Testing Plan**
- **Backout Plan**

Using change templates speeds up the entry of change request information and helps to standardize and increase the accuracy of the change request information. For example, a template can help you create a change request for the occasional change of a user's security configuration. By using a template, you can be sure that the correct steps are followed.

Change templates are useful when you have standardized plans for rolling out periodic maintenance changes. For example, you can use a template to provide the change request information for deploying hot fixes from Microsoft every two months. Once you create a change template, it is available from within a change request ticket's **Process View** page.

You can create a change template as follows:

- On the **Submit Request** portal page
  Click **Administrative Services** and then click **Manage Change Templates**.
- On a change request ticket's **Process View** page
  Under **Process Actions**, click **Manage Templates**.

See "Creating a new change template" on page 228.

Creating a new change template

You can create your own change templates. Using change templates speeds up the entry of change request information and helps to standardize and increase the accuracy of the change request information. For example, a template can help you create a change request for the occasional change of a user's security configuration. By using a template, you can be sure that the correct steps are followed.

To create a new change template

1 To open the **Manage Change Plan Templates** dialog box use one of the following options:

Option 1:

- In the Process Manager portal, click **Submit Request**.
- On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**.
- On the right side of the page, click **Manage Change Templates**.

Option 2:

- In the Process Manager portal, click **My Task List**.
- Under **Task Viewer**, under **Project Name**, expand **SD.ChangeManagement**.
- In the list of tasks, find and open the change request ticket.
- On the change request ticket's **Process View** page under **Process Actions**, click **Manage Templates**.

2 On the **Manage Change Plan Templates** page, click **New Template**.

3 In the **Template Name** field, type the name of the template.

4 (Optional) Provide the following information:

- **Template Description**
- **Risk Assessment Score**
- **Cost of Implementing**
- **Cost of Not Implementing**

- **Implementation Plan**
- **Testing Plan**
- **Backout Plan**

5 Click **Save Template**.

See “About change templates” on page 227.

See “Editing a change template” on page 229.

Editing a change template

You can edit your change templates. For example, you may need to add additional steps to the testing plan section or increase the cost of implementing the change.

To edit a change template

1 To open the **Manage Change Plan Templates** dialog box use one of the following options:

Option 1:	■ In the Process Manager portal, click **Submit Request**. ■ On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**. ■ On the right side of the page, click **Manage Change Templates**.
Option 2:	■ In the Process Manager portal, click **My Task List**. ■ Under **Task Viewer**, under **Project Name**, expand **SD.ChangeManagement**. ■ In the list of tasks, find and open the change request ticket. ■ On the change request ticket's **Process View** page under **Process Actions**, click **Manage Templates**.

2 On the **Manage Change Plan Templates** page to the right of the template that you want to edit, click **Edit**.

3 (Optional) In the **Template Name** field, edit the name of the template.

4 (Optional) Edit the following information:

- **Template Description**
- **Risk Assessment Score**
- **Cost of Implementing**
- **Cost of Not Implementing**

- **Implementation Plan**
- **Testing Plan**
- **Backout Plan**

5 Click **Save Template**.

See “Creating a new change template” on page 228.

See “Deleting a change template” on page 230.

Deleting a change template

You can delete your change templates. For example, you may want to delete an obsolete change template.

To edit a change template

1 To open the **Manage Change Plan Templates** dialog box use one of the following options:

Option 1:	■ In the Process Manager portal, click **Submit Request**. ■ On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**. ■ On the right side of the page, click **Manage Change Templates**.
Option 2:	■ In the Process Manager portal, click **My Task List**. ■ Under **Task Viewer**, under **Project Name**, expand **SD.ChangeManagement**. ■ In the list of tasks, find and open the change request ticket. ■ On the change request ticket's **Process View** page under **Process Actions**, click **Manage Templates**.

2 On the **Manage Change Plan Templates** page to the right of the template that you want to delete, click **Delete**.

Warning: When you click **Delete**, your change template is permanently deleted.

See “Creating a new change template” on page 228.

See “Editing a change template” on page 229.

Customizing the email in ServiceDesk

This chapter includes the following topics:

Customizing the email actions for ServiceDesk processes

ServiceDesk can perform the following automatic email actions:

- Send email notifications at various stages of the Problem Management and Knowledge Management processes, based on one or more events that occur within these processes.
- Accept new incidents or updates to current incidents through inbound email.

These email capabilities are predefined and ready to use. However, you can customize them as needed.

All the actions that are listed in **Process for customizing the email action for ServiceDesk processes** table are optional and can be performed in any order.

Table 16-1 Process for customizing the email actions for ServiceDesk processes

Action	Description
Customize the automatic email notifications.	The Problem Management and Knowledge Management processes can trigger several types of email notifications. You can customize the email notifications by editing the project for the appropriate process in Workflow Designer. See "About automatic email notifications" on page 232. For more information about editing the process projects, see the Symantec™ Workflow 7.5 User Guide.
Edit the automatic email contents.	The contents of the automatic email messages are predefined for each type of notification. You can customize any of these messages or add new ones. See "About the contents of email notifications" on page 233.
Customize the email monitoring.	ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification. You can customize the email monitoring as follows: ■ The mailbox and other email settings are configured during the installation of the ServiceDesk application software. If necessary, you can change some of these settings on the portal **Master Settings** page. ■ You can use the monitoring process as it is defined or you can customize it. For example, you can monitor multiple mailboxes, define the email contents to be processed, and change the assignee for the new incidents. See "About configuring the email monitoring" on page 234.

About automatic email notifications

ServiceDesk can send email notifications at various stages of a process, based on one or more events that occur within the process. The type of event determines the contents and the recipients of the email notifications.

ServiceDesk contains default notifications for the following core processes:

- Problem Management
- Knowledge Management

The default notifications are ready to use. However, you can customize the email notifications by editing the appropriate project in Workflow Designer. For example, you can change the event that triggers a notification or create a notification for a new event.

For more information about editing the email notifications, see the Symantec™ Workflow 7.5 User Guide.

You can also change the default contents of the automatic email notifications.

See "About the contents of email notifications" on page 233.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the Process Manager portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted.

Email notifications for Incident Management and Change Management are handled through the Automation Rules. For these processes, you must create email templates and then create rules for sending them.

See "Creating email templates for Incident Management" on page 194.

See "Configuring new automation rules for Incident Management" on page 210.

See "Creating email templates for Change Management" on page 219.

About the contents of email notifications

ServiceDesk can send email notifications at various stages of the Problem Management and Knowledge Management processes. Email notifications can be sent based on one or more events that occur within these processes.

See "About automatic email notifications" on page 232.

The contents of the email messages are predefined and ready to use. However, you can customize any of these messages. You can also edit the triggers of the emails or add notifications to additional processes.

ServiceDesk obtains the contents of the email messages from several sources.

Table 16-2 Sources for the contents of the email messages

Source	Description
The **Send Email** component or adjacent text component within the Problem Management process	▪ The Problem Management process executes the **Send Email** component to generate the email messages within the process itself. ▪ The message text may be composed within the **Send Email** component or within adjacent text component. ▪ You can customize the default email messages by editing the message text within the Problem Management process in Workflow Designer
The **Send Email** component or adjacent text component within the knowledge base submission process	▪ The knowledge base submission process executes the **Send Email** component to generate the email messages within the process itself. ▪ The message text may be composed within the **Send Email** component or within adjacent text components. ▪ You can customize the default email messages by editing the message text within the knowledge base submission process in Workflow Designer.

For more information about configuring the content for email or editing processes and Projects, see the Symantec™ Workflow 7.5 User Guide.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the Process Manager portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted.

About configuring the email monitoring

ServiceDesk can accept new incidents or updates to current incidents through inbound email. ServiceDesk monitors the appropriate inbox for all new, unread emails and processes them by creating incidents or routing them to the support team for classification. This email process relies on an automatically-generated reply code to link the email correspondence to an incident. The support workers do not have to check an Inbox because the email correspondence is added to the incident's history.

By default, the email monitoring process can also add the contents of the email responses to a process ticket. The recipient of the email can send a reply that contains the requested information. The monitoring process reads the reply code that is associated with the email. The process adds the email contents to the appropriate process history and creates a task for the process worker.

The mailbox and other email settings are configured during the installation of the ServiceDesk application software. If necessary, you can change these settings on the **Application Properties** page, under the **Service Desk Settings** link. The **Application Properties** page is available from the **Admin** menu.

See "Commands on the Admin menu" on page 243.

The default monitoring process is ready to use. However, you can customize it in several ways to meet your organization's requirements.

Table 16-3 Suggestions for customizing the email monitoring

Customization	Method
Examples of how you might customize the email monitoring process are as follows: ■ Configure the process to monitor multiple mailboxes. ■ Add or change the words or phrases in the subject line that trigger the creation of an incident. ■ Create an incident rule that defines the words or phrases in the message body that can populate values in the incident. ■ Use a notification rule to automatically create an email if additional information is needed from the original sender.	Edit the SD.Email.Monitor project in Workflow Designer.
Create templates for the users who submit incident through email so ServiceDesk can capture or evaluate specific information. Many organizations perform this customization.	You can create an email template in your email client, and then set up incident rules in the SD.Email.Monitor project to evaluate the template content. For example, if you include a Location field in the email template, the incoming email messages can be routed to the correct location.

For more information about configuring email and customizing projects, see the Symantec™ Workflow 7.5 User Guide.

Chapter 17

Distributing the ServiceDesk documentation

This chapter includes the following topics:

- Making the ServiceDesk documentation available to users
- Configuring the Help link for ServiceDesk documentation
- Linking to the ServiceDesk documentation from a Links Web part
- Displaying the ServiceDesk documentation in a File Browser Web part
- Adding the ServiceDesk documentation to Document Management

Making the ServiceDesk documentation available to users

Each organization has specific requirements for providing documentation to their process workers and the users of the Process Manager portal. Therefore, the ServiceDesk documentation is not installed with ServiceDesk. We recommend that you download these guides and make them available to your users as needed.

To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The updated documentation files are not installed with the software updates. When you plan how to distribute the documentation to your ServiceDesk users, consider the ease of updating the documents in the future.

Table 17-1 Process for making the ServiceDesk documentation available to users

Step	Action	Description
Step 1	Download the documentation to a shared network drive or other location.	Download any of the following documents: ■ Symantec™ ServiceDesk 7.5 Implementation Guide This guide is for the administrator who installs and configures ServiceDesk. ■ Symantec™ ServiceDesk 7.5 User Guide This guide is for the process workers. The ServiceDesk release notes and other documentation resources contain the links to the location for downloading the documentation files. See "Where to get more information" on page 21.
Step 2	Make the documentation available to the users.	You can provide access to the documentation files in whatever way you decide is best. Some of the options that are available in ServiceDesk are as follows: ■ Edit the **Help** link that appears at the lower left of the Process Manager portal window. Set the link to target the location of the documentation files. The default target for the **Help** link is the ServiceDesk **Product Support** page on the Symantec Website. See "Configuring the Help link for ServiceDesk documentation" on page 238. ■ Add the documentation files to a document management category and add a category browser Web part to access them. See "Adding the ServiceDesk documentation to Document Management" on page 241. ■ Add a file browser Web part that enables browsing to the documents. See "Displaying the ServiceDesk documentation in a File Browser Web part" on page 240. ■ Add the **Links** Web part that provides links to the documents. See "Linking to the ServiceDesk documentation from a Links Web part" on page 238. We do not recommend that you deliver copies of the documentation to individual users. The more copies of the documentation that you distribute, the harder it becomes to update all of them.
Step 3	Tell the users how to access the documentation.	Use the method that is best for your organization. One option is to create a Bulletin Board message that users can view in the Process Manager portal.

Configuring the Help link for ServiceDesk documentation

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by configuring the **Help** link that appears in the Process Manager portal to link to the location of the documentation files.

The default target for the **Help** link is the ServiceDesk **Product Support** page on the Symantec Website. Other options are available for providing access to the documentation from within the Process Manager portal.

See "Making the ServiceDesk documentation available to users" on page 236.

Caution: To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The documentation files are not installed with the software updates.

To configure the Help link for ServiceDesk documentation

1. In the Process Manager portal, click **Admin > Portal > Master Settings**.
2. On the **Master Settings** page, expand the **Process Manager Settings** section.
3. In **Help Link Url**, type the fully qualified path to the location of the documentation files in the following format:

   http://www.< ***domain*** **>.com/<** ***folder*** **>**
4. Click **Save**.

Linking to the ServiceDesk documentation from a Links Web part

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding a **Links** Web part in the Process Manager portal to display links to the location of the documentation files.

You can set permissions on the portal page to which you add the Web part. The permissions settings ensure that only the appropriate users can access the documentation.

Other options are available for providing access to the documentation from within the Process Manager portal.

See "Making the ServiceDesk documentation available to users" on page 236.

Caution: To avoid the distribution of outdated documentation, you must update the documentation files when updates are available. The documentation files are not installed with the software updates.

Table 17-2 Process for linking to the ServiceDesk documentation from a **Links** Web part

Step	Action	Description
Step 1	Ensure that the documentation files are in the correct folder.	If you downloaded the documentation files to a location that is not accessible to all the users, move the files to an appropriate shared location.
Step 2	Add a **Links** Web part to a portal page that the target users can access.	The portal page that you select should be accessible to the target users only. For example, add a link to the *ServiceDesk Implementation Guide* on a portal page that only the administrators can access. The **Links** option is in the **Catalog Zone** pop-up under the **UI** section.
Step 3	Edit the Web part to specify the target URL.	In the **Editor Zone** pop-up, under **Property Grid**, in **URL**, you must specify the fully-qualified path or URL where the documentation is located.
Step 4	Make additional edits to the Web part.	In the **Editor Zone** pop-up, we recommend that you select the following options: ■ **Show open in new window control** This option is in the **Links Editor** section. ■ **Title** The text that you type here appears in the Web part title bar. For example, you might type **ServiceDesk Documentation**. This option is in the **Appearance** section. You can edit other attributes of the Web part as needed.

Displaying the ServiceDesk documentation in a File Browser Web part

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding a **File Browser** Web part in the Process Manager portal to display the folder that contains the documentation files.

The **File Browser** Web part displays a folder tree that starts with a parent folder that you specify. The users can navigate to the child folder that contains the documentation.

You can set permissions on the portal page to which you add the Web part. The permissions settings ensure that only the appropriate users can access the documentation. You can also set permissions on the documentation folder.

Other options are available for providing access to the documentation from within the Process Manager portal.

See “Making the ServiceDesk documentation available to users” on page 236.

Caution: To avoid the distribution of outdated documentation, you must update the documentation files in the Document Management system when updates are available. The documentation files are not installed with the application updates.

Table 17-3 Process for displaying the ServiceDesk documentation in a **Browser** Web part

Step	Action	Description
Step 1	Ensure that the documentation files are in a folder that the target users can access.	If you downloaded the documentation files to a location that is not accessible to all the users, move the files to an appropriate shared location. Be sure to place the documentation files in their own folder, under a parent folder that contains no other subfolders. The **File Browser** Web part displays all the subfolders of the parent folder.
Step 2	Add a **File Browser** Web part to a portal page that the target users can access.	The portal page that you select should be accessible to the target users only. For example, add a link to the *ServiceDesk Implementation Guide* on a portal page that only the administrators can access. The **FileBrowser** option is in the **Catalog Zone** pop-up under the **UI** section.

Table 17-3 Process for displaying the ServiceDesk documentation in a **Browser** Web part *(continued)*

Step	Action	Description
Step 3	Edit the Web part to specify the target folder.	In the **Editor Zone**, under **Property Grid**, in **Folder**, you must specify the parent folder of the folder that contains the documentation files. Be sure to include the full path to the parent folder. The **File Browser** Web part cannot display any files in the parent folder. Therefore, do not specify the documentation folder as the parent.
Step 4	(Optional) Make other edits as needed.	You can edit other attributes of the Web part as needed. For example, you might change the title of the Web part to Browse ServiceDesk Documentation. The **Title** option is in the **Editor Zone** pop-up under the **Appearance** section.

Adding the ServiceDesk documentation to Document Management

If you choose to make the ServiceDesk documentation available to your users, you can download it to a shared network drive or other location. After the download, you must provide a means for the users to access the documentation. You can do so by adding the documentation files to a document category and providing access to those files from a category browser Web part.

You can set permissions on the category or on the document files so that only the appropriate users can access the documentation.

Other options are available for providing access to the documentation from within the Process Manager portal.

See “Making the ServiceDesk documentation available to users” on page 236.

Caution: To avoid the distribution of outdated documentation, you must update the documentation files in the Document Management system when updates are available. The documentation files are not installed with the Server software updates.

Table 17-4 Process for adding the ServiceDesk documentation to Document Management

Step	Action	Description
Step 1	(Optional) Create a new documents category.	You can dedicate an entire category to the documentation. For example, you might name the category ServiceDesk Documentation. Alternatively, you can add the documentation files to an existing category.
Step 2	(Optional) Set permissions on the category.	You can set permissions at the category level if all the documents in that category are intended for the same users. Alternatively, you can set permissions on the individual documents.
Step 3	Add one or more documentation files to the category.	Add the documentation files from their download location.
Step 4	(Optional) Set permissions on the documents.	If the category contains multiple documents for different types of users, you can set permissions on the individual documents. For example, you can set permissions on the *ServiceDesk Implementation Guide* so that only administrators can view it. We recommend that you do not allow anyone to edit the documentation files.
Step 5	Add a category browser Web part to a portal page that the target users can access.	The category browser Web part displays the document categories and lets the user select the category and view the documents in that category. The **CategoryBrowserWebPart** option is in the **Catalog Zone** pop-up under the **Documents** section.
Step 6	(Optional) Edit the Web part.	You can edit the Web part as needed. For example, you might change the title of the Web part to ServiceDesk Documentation. The **Title** option is in the **Editor Zone** pop-up under the **Appearance** section.

Chapter 18

Performing administrative tasks

This chapter includes the following topics:

Commands on the Admin menu

The **Admin** menu provides access to all the administrative functions that are available in ServiceDesk. Only an administrator or other user who has the appropriate permissions can access this menu.

The **Admin** menu consists of all the options that are available on the **Admin** page in the Process Manager portal.

Table 18-1 Commands on the **Admin** menu

Command	Subcommand	Description
Data	**Application Properties**	Lets you add, edit, and delete application properties. Typically, you define application properties as part of the installation configuration process, but you can also work with them from the Admin area. Application properties are a type of profile. Instead of hard-coding the values that you use in workflow components, you can define application properties to represent those values. You can use the properties in multiple workflow components. See "About application properties" on page 248.
Data	**Lists/Profiles**	Lets you add, edit, and delete profile definitions. Profiles let you categorize data by adding customizable fields, which you can use for further sorting of data. For example, you can set up profile values of "hardware" and "OS" for incidents. When users enter incidents in ServiceDesk, they can specify the hardware type and operating systems that are involved in the incident. When technicians analyze the data from multiple incidents, they can see patterns emerge. These patterns may reveal that they have serious problems with a certain hardware and OS combination, which needs further investigation.
Data	**Document Type**	Lets you add, edit, and delete document types. The document type defines the file format of a document that is imported to the Document Management system. The users who import documents can specify the document type. However, users can import files of types other than those that are defined.
Data	**Document Category Type**	Lets you add, edit, and delete document category types. The document category type provides an additional means of grouping and organizing the document categories. You can sort the category display on the **Documents** page by document category type instead of alphabetically.
Data	**Hierarchy Data Service**	Lets you add, edit, and delete incident categories and hierarchy items. ServiceDesk uses categories to classify incidents. You can use additional levels of classification items to further identify the incidents. The main categories and the additional classification items are referred to as the data hierarchy. See "About Incident Management classifications and the data hierarchy" on page 177.

Table 18-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Data	**User Relationship Type**	Lets you add, edit, and delete user relationship types. User relationship types define the relationships that users can have to other users and to groups. User relationship types can reflect that one user is the manager of another, or that a user is a member of a group. You can base incident assignment on relationships. For example, an incident is assigned to the support group. If the incident is not resolved after two days, it is assigned to the most senior person in that group. The assignment process only needs to know of the relationship to use for assignment, not the specific users. Therefore, if the most senior support worker changes, the assignments follows automatically.
Data	**Profile Reference Type**	Lets you add or edit a profile reference type. This option is available only if Workflow Solution is installed. You might want to call support for assistance if you plan to change or add profile reference types. Profiles let you define data. When you set up a profile, you set up the pieces of data that you want to see in different ServiceDesk items. ServiceDesk items include articles, schedules, or documents. For example, if you work with mortgage applications, you might want to know the property address, assessed value, and other information on the properties. Setting up profile reference types lets you define the property-specific data that you want to see.
Data	**Process Type Actions**	Lets you add, edit, and delete **Process Type Actions** on the **Process View** pages for Incident and Change Management. **Process Type Actions** are the links that let you perform other processes from the incident and the change request tickets' **Process View** page.
Data	**Business Hours**	Lets you add, edit, and delete business hours configurations. You can set up your business hours and holidays based on your business locations and SLA policy. You can use these business hours and holidays to set up routing rules so that incidents are routed to specific service queues during business hours. You can also set up routing rules so that incidents are routed to specific queues during non-business hours, weekends, and holidays.

Table 18-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Portal	**Master Settings**	Lets you configure the master settings for the Process Manager portal, which determine the behavior of the ServiceDesk application software and portal. See "About the Process Manager portal master settings" on page 250.
Portal	**Manage Pages**	Lets you manage all the pages in the Process Manager portal. You can import, edit, delete, export, and move pages up and down the menu list. You can also add root pages and subpages, and make a root page a subpage. The Process Manager portal is a Web-based interface that provides access to the ServiceDesk application software. Most of the work in ServiceDesk is performed in a portal page or in a page that is accessed from a portal page. See "About the Process Manager portal" on page 182.
Portal	**Plugin Upload**	Lets you upload plugins, web parts, resources, or pages. For example, you can create a workflow project that you can upload as a plugin. You can create a workflow for the Document Management process, which requires users to go through several steps before a document is approved. You can load that workflow project into the Process Manager portal as a plugin.
Portal	**Web Parts Catalog**	Lets you add new Web parts to the catalog, and edit and delete existing Web parts.
Service Catalog Settings	Not applicable	Lets you manage the Service Catalog items. You can set the permissions on which ServiceDesk users, groups, and organizational units have access to the specific forms. You can also edit, rename, create, and delete Service Catalog items and categories, and modify Service Catalog item attributes such as the form size.

Table 18-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Users	**Accounts**	Lets you manage the various ServiceDesk user, group, permission, and organization accounts. This command has the following subcommands: ▪ Manage Users Lets you add, edit, and delete users. You can also manage groups, organizations, and permissions for users, merge users, and set user relationships. In addition, you can set the Users password, enable or disable the user, add credit cards, transactions, and key value pairs for the user. ▪ List Permissions Lets you add, edit, and delete permissions and view the users and groups that are assigned a certain permission. ▪ List Groups Lets you add, edit, and delete groups, add users to groups, add permissions to groups, and remove users from groups. ▪ List Organizations Lets you add, edit, and delete organizations, add users and permissions to organizations, and remove users from organizations.
Users	**AD Users**	Lets you view the current list of users in Active Directory and select users to update.
Users	**Manage Delegations**	Lets you add and delete delegations for users.
Active Directory	**Sync Profiles**	Lets you add and manage the Active Directory sync profiles that you can create in ServiceDesk. See "Managing Active Directory sync profiles" on page 270.
Active Directory	**Sync Profile Schedule**	Lets you configure schedules for automatically synchronizing your profiles with Active Directory. Lets you configure schedules for full syncs and for update syncs. For example, you can schedule a full sync to occur weekly and an update sync to occur daily.
Reports	**Report Schedule List**	Lets you configure the schedules that automatically execute and email reports.
Manage KB Synonyms	Not applicable	Lets you add, edit, and delete knowledge base synonyms

Table 18-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Process Automation	Not applicable	Lets you configure automation rules for any workflow-based application, which includes service automation library. Automation rules let the administrator configure the Incident Management and the Change Management processes.

About application properties

ServiceDesk contains a set of default application properties named **ServiceDeskSettings**, which the components in Workflow Designer and Workflow Solution can use. The application properties are also referred to as profile properties in the Workflow products.

A best practice in the Workflow products is to reference the application properties instead of hard-coding values. If you need to change certain values, change them on the **Application Properties** page in ServiceDesk.

For example, instead of hard-coding the group “Support” in a component, you can use the application property for that group instead, as follows:

[ProfileProperties]service_desk_settings_group_support

When changes are made to the application property, the changes are automatically reflected in Workflow. Some of the values that you might change are the priority, impact, urgency, or URLs for processes.

For example, you can link to a page in your organization’s intranet from multiple ServiceDesk processes by defining an application property for the page’s URL. When you add that property to ServiceDesk forms, the intranet link appears on the pages that result from those forms.

The **Application Properties** page is available on the **Admin** menu.

See “Commands on the Admin menu” on page 243.

About incident close codes

When an incident is closed, the support technician must provide a close code to indicate the nature of the resolution.

ServiceDesk contains a set of predefined close codes that are ready to use. If necessary, you can delete or add to the default close codes. You can edit the incident close codes in the Process Manage portal on the Applications Properties page.

Close codes let you select a code that indicates the nature of the resolution.

The default close codes are as follows:

- **Advice Given**
- **Change Required**
- **Completed Success**
- **Monitoring Required**
- **No Fault Found**
- **Other**
- **Review Documentation**
- **Training Required**
- **Other**

See “Adding and deleting incident close codes” on page 249.

Adding and deleting incident close codes

ServiceDesk contains a set of predefined close codes that are used when an incident is resolved. If necessary, you can delete or add to the default close codes.

See “About incident close codes” on page 248.

Deleting a close code does not affect any process tickets that contain that close code. The tickets retain the close code, which is visible as usual when you view the tickets. Any reports that refer to a deleted close code still work.

To add or delete incident close codes

1. In the Process Manager portal, click **Admin > Data > Application Properties**.
2. On the **Applications Properties** page, under **Application Properties Profiles**, click **ServiceDeskSettings**.
3. At the far right of the **ServiceDeskSettings** title bar, click the **Actions** symbol (orange lightning), and then click **Edit Values**.
4. In the **Edit Profile Definition Instance** dialog box, scroll down to **CloseCodes**, and under the list of close codes, click **Edit**.

5 In the dialog box that appears, take any of the following actions:

To add a close code	In the box at the bottom of the dialog box, type the new close code, and then click **Add**.
To delete a close code	Click the **Delete** symbol (a red X) to the right of the close code.

6 When you finish editing the close codes, click **Save**.

7 In the **Edit Profile Definition Instance** dialog box, click **Save**.

About the Process Manager portal master settings

The Process Manager portal master settings determine the behavior of the ServiceDesk application software and portal.

The Process Manager portal master settings are established during the installation of the ServiceDesk application software. You can use the default settings or you can edit them as necessary. We recommend that you review the settings to familiarize yourself with them and then customize them for your organization.

See “Editing the Process Manager portal master settings” on page 250.

Examples of the types of settings that you might change are as follows:

- Settings under the **Account Management** section
  Password Expire Months, **Register Fail e-mail address**, and **Security Question 1**
- Settings under the **Workflow Settings** section
  Workflow Task Due Date and **Workflow Task Late Date**

Do not change the settings for URLs or disable check boxes without fully understanding the ramifications. Few organizations need to change that type of information.

The portal master settings are arranged in sections. Expand each section to see the settings that appear there.

Editing the Process Manager portal master settings

The Process Manager portal master settings determine the behavior of the ServiceDesk application software and portal.

Although default master settings are established during the installation of the ServiceDesk application software, you can edit them to customize them for your organization.

See “About the Process Manager portal master settings” on page 250.

Do not change the settings for URLs or disable check boxes without fully understanding the ramifications. Few organizations need to change that type of information.

To edit the Process Manager portal master settings

1. In the Process Manager portal, click **Admin > Portal > Master Settings**.
2. On the **Process Manager Settings** page, expand the section that contains the settings that you want to edit.
3. Change the settings as necessary.
4. Continue to expand and edit additional sections as needed.
5. When you finish reviewing and editing the settings, at the lower right of the page, click **Save**.

Creating user relationship types

You can customize ServiceDesk so that process tickets can be assigned based on relationships. For example, if an incident is not completed in time, it can escalate from the original worker to that worker’s supervisor. The relationships can be between users, groups, permissions, or organizational units.

To create a user relationship type

1. In the Process Manager portal, click **Admin > Data > User Relationship Type**.
2. Click the **Add Relationship Type** symbol (green plus sign).
3. In the **Add Relationship Type** dialog box, type the name for the relationship.
4. In the **Relates To** drop-down list, select the type of relationship.

   The relationship can relate to users, groups, permissions, or organizational units.
5. Click **Save**.

Chapter 19

Managing the Active Directory connections

This chapter includes the following topics:

- Deleting an Active Directory sync profile
- Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes
- Methods for synchronizing Active Directory sync profiles
- Running a full Active Directory sync profile synchronization manually
- Running update Active Directory sync profile synchronization manually
- Synchronizing all Active Directory sync profiles manually
- Checking the status of an Active Directory sync profile synchronization

About Active Directory synchronization

You can choose to use Active Directory authentication as its authentication method for ServiceDesk.. You can synchronize ServiceDesk with Active Directory. This synchronization lets you add and update Active Directory users, organizational units, and groups in the Process Manager database. During synchronization, data from Active Directory updates data that are in the Process Manager database. The Process Manager database does not store sensitive information such as passwords.

You add Active Directory synchronization profiles, after you connect ServiceDesk to an Active Directory server. These synchronization profiles let you import the entire Active Directory domain or specific organizational units and groups. These units and groups are not the same as the organizational groups that ServiceDesk uses to categorize users.

The communication between ServiceDesk and Active Directory occurs by means of LDAP queries against the Active Directory database. ServiceDesk provides several ways to initiate the synchronization

The Active Directory synchronization performs the following actions:

- Imports and updates the Active Directory users in ServiceDesk
- Imports and updates the Active Directory organizational units and groups in ServiceDesk

When you use Active Directory authentication, you still can create user accounts and organizational units in ServiceDesk. For example, you might create an account for a short-term contractor who you do not want to add to Active Directory

After you install ServiceDesk, you can set up your Active Directory server connections, synchronization schedules, and sync profiles. ServiceDesk can then synchronize with Active Directory to obtain new and updated users and groups.

Active Directory synchronization affects the changes and deletions of ServiceDesk user accounts as follows:

- When you delete a user from Active Directory, the user is not deleted from ServiceDesk. The user is only disabled in ServiceDesk.
- Any changes that you make to a user in ServiceDesk are overwritten during the next synchronization.

If you edit user information or delete a user in Active Directory instead, the information is updated in ServiceDesk during the next synchronization. This rule applies to the users group, manager, and organizational unit information.

See “About ServiceDesk authentication” on page 168.

See “Methods for synchronizing Active Directory sync profiles” on page 280.

See “About adding users from Active Directory” on page 169.

See “About adding groups from Active Directory” on page 170.

See “Creating a new user” on page 175.

See “Creating an organizational unit” on page 174.

See “Configuring Active Directory sync profiles” on page 254.

Configuring Active Directory sync profiles

If your organization chooses to use Active Directory authentication as its authentication method for ServiceDesk, you can configure Active Directory sync profiles. You can use these sync profiles to target an entire Active Directory domain, organizational units and groups, or specific LDAP queries.

After you configure your Active Directory sync profiles, ServiceDesk can synchronize these sync profiles with Active Directory. During synchronization, ServiceDesk can obtain new and updated users and organizational units and groups.

After you configure your Active Directory sync profiles, you can add, edit, or delete your Active Directory server connections, sync profile schedules, and sync profiles. You can manage your Active Directory server connections in Workflow Explorer. You can manage your Active Directory sync profile schedules and sync profiles in ServiceDesk.

See “About Active Directory synchronization” on page 253.

See “Methods for synchronizing Active Directory sync profiles” on page 280.

See “Managing Active Directory server connections” on page 256.

See “Managing Active Directory sync profile schedules” on page 265.

See "Managing Active Directory sync profiles" on page 270.

Table 19-1 Process for configuring an Active Directory sync profile

Step	Action	Description
Step 1	Add Active Directory server connections.	In Workflow Explorer, you can connect ServiceDesk with your Active Directory servers. See "Adding Active Directory server connections" on page 257.
Step 2	Select **Active Directory Authentication** as the authentication type.	In ServiceDesk, you can select Active Directory as your authentication method. See "Selecting Active Directory as the authentication method" on page 262. Note that after you select Active Directory as your authentication method, you do not need to do it again. Active Directory is now your authentication method.
Step 3	Add automatic sync profile schedules.	In ServiceDesk, you can add automatic Active Directory sync profile schedules. See "Adding Active Directory sync profile schedules" on page 266. When adding your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations: ■ Update synchronization ■ Full synchronization
Step 4	Add Active Directory sync profiles.	In ServiceDesk, you can add sync profiles for your Active Directory server connections. See "Adding Active Directory sync profiles" on page 272.
Step 5	(Optional) Test an Active Directory server connection.	In ServiceDesk, you can test each ServiceDesk to Active Directory server connection. See "Testing an Active Directory server connection" on page 263.

Table 19-1 Process for configuring an Active Directory sync profile *(continued)*

Step	Action	Description
Step 6	(Optional) Manually perform a full synchronization for an Active Directory sync profile.	In ServiceDesk, you can manually run full synchronization for the Active Directory sync profiles that you specify. See "Running a full Active Directory sync profile synchronization manually" on page 281.
Step 7	(Optional) Manually perform a full Active Directory synchronization for all Active Directory sync profiles.	In ServiceDesk, you can manually perform full synchronization for all your Active Directory sync profiles. See "Synchronizing all Active Directory sync profiles manually" on page 283.
Step 8	(Optional) Check the status of an Active Directory sync profile synchronization.	In ServiceDesk, you can view information about the users and organizational units and groups that are synchronized. You can also view the status of the Active Directory sync profile synchronization. See "Checking the status of an Active Directory sync profile synchronization" on page 284.
Step 9	Assign permissions to your imported groups.	By default, the imported groups are added to the All Users group. Therefore your imported groups have All User permissions. You must assign your Active Directory groups additional permissions. See "Copying permissions between groups" on page 173.

Managing Active Directory server connections

In Workflow Explorer, you can add one or more Active Directory server connections. After you add your Active Directory server connections, you may need to edit the settings of an Active Directory server connection. You may also need to delete an Active Directory server connection. In Workflow Explorer, you can manage your Active Directory server connections.

After you add your Active Directory server connections, you can then add sync profile schedules and sync profiles for them. You can use these sync profile schedules to schedule update and full synchronizations with Active Directory. You can use these sync profiles to import data from Active Directory to the Process Manager database. You can import the entire domain, organizational units and groups on the Active Directory server, or for specific LDAP queries. In ServiceDesk, you can manage these sync profile schedules and sync profiles.

See "Managing Active Directory sync profile schedules" on page 265.

See "Managing Active Directory sync profiles" on page 270.

Table 19-2 Process for managing Active Directory server connections

Step	Action	Description
Step 1	Add Active Directory server connections.	In Workflow Explorer, you can connect ServiceDesk with your Active Directory servers. See "Adding Active Directory server connections" on page 257.
Step 2	(Optional) Edit the settings of an Active Directory server connection.	In Workflow Explorer, you can edit the settings of an Active Directory server connection. See "Editing the settings of an Active Directory server connection" on page 260.
Step 3	(Optional) Delete an Active Directory connection.	In Workflow Explorer, you can delete an Active Directory server connection. See "Deleting an Active Directory server connection" on page 262.
Step 4	(Optional) Test an Active Directory server connection.	In ServiceDesk, you can test the Active Directory server connection. See "Testing an Active Directory server connection" on page 263. Note that you can only test an Active Directory server connection after you add a sync profile for that server connection.

Adding Active Directory server connections

If your organization uses Active Directory authentication as its authentication method for ServiceDesk, you may need to add one or more Active Directory server connections. In Workflow Explorer, you can add Active Directory server connections at any time. For example, you might need to connect to an Active Directory server in a new location.

See “Configuring Active Directory sync profiles” on page 254.

See “Managing Active Directory server connections” on page 256.

Before you add an Active Directory server connection, you need to collect the following information:

- NETBIOS domain name of the Active Directory server
- Credentials for Active Directory
  The user name and password of an account that can connect to the Active Directory and retrieve user information
- Domain controller host name or IP address

To add Active Directory server connections

1. On the ServiceDesk server on the Windows **Start** menu, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the **Symantec Workflow Explorer** page in the toolbar at the top of the page, click **Credentials**.
3. In the left pane, click **Active Directory**.
4. In the right pane, click **Add New**.

5 In the **New AD Connection Profile** dialog box, type the following information for your Active Directory connection:.

Domain Controller

Lets you type the IP address or host name of your domain controller.

Domain

Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows:

<MyDom>

Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network. If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work.

The format for the fully qualified domain name is as follows:

<MyDomain.com>

Username

Password

Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information.

You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory.

For security purposes, you must retype the password every time you add or edit an Active Directory server connection.

Default Timeout

Lets you specify the parameters for the default timeout.

Note that 20000 is the default setting.

Name

Is Default check box

Lets you specify a name for the Active Directory connection profile.

Lets you choose whether to use the Active Directory connection profile as the default profile.

6 When you are finished, click **OK**.

7 Repeat the steps in this procedure to add additional server connections.

8 (Optional) If you have not selected Active Directory as your authentication method, then you need to select **Active Directory Authentication** as your authentication method.

See “Selecting Active Directory as the authentication method” on page 262.

To Test your Active Directory server connection

1 In the right pane, select the Active Directory server connection that you want to test.

2 Click **Test**.

3 (Optional) If the test fails, recheck your Active Directory setting by doing the following:

- In the right pane, select the Active Directory server connection that failed.
- Click **Edit**.
- In the **Edit AD connection settings** dialog box, edit the settings as needed and then click **OK**.
- Test the Active Directory server connection. See Step 1.

4 In the **AD connection succeeded** dialog box, click **OK**.

Editing the settings of an Active Directory server connection

After you add your Active Directory server connections, you may need to edit the settings of an Active Directory server connection. In Workflow Explorer, you can edit any of the Active Directory servers to ServiceDesk connections. For example, if you need to change the user name and password for an Active Directory server connection, you can change it.

If you need to convert native users to Active Directory users, you can do so in **Process Manager Active Directory Settings**. These settings appear in the Process Manager portal on the **Master Settings** page.

See “Managing Active Directory server connections” on page 256.

To edit the settings of an Active Directory server connection

1 On the ServiceDesk server on the Windows **Start** menu, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.

2 On the Symantec Workflow Explorer page in the toolbar at the top of the page, click **Credentials**.

3 In the left pane, click **Active Directory**.

4 In the right pane, select the Active Directory server connection profile that you want to edit.

5 In the right pane, click **Edit**.

6 In the **Edit AD connection settings** dialog box, edit the following settings as needed:

Domain Controller

Lets you type the IP address or host name of your domain controller.

Domain

Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows:

<MyDom

Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network. If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work.

The format for the fully qualified domain name is as follows:

<MyDomain.com >

Username

Password

Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information.

You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory.

For security purposes, you must retype the password every time you add or edit an Active Directory server connection.

Default Timeout

Lets you specify the parameters for the default timeout.

Note that 20000 is the default setting.

Name

Is Default check box

Lets you specify a name for the Active Directory connection profile.

Lets you choose whether to use the Active Directory connection profile as the default profile.

7 When you are finished, click **OK**.

8 Close Workflow Explorer.

9 (Optional) After you edit the settings of an Active Directory server connection, you may want to test the server connection.

See “Testing an Active Directory server connection” on page 263.

Deleting an Active Directory server connection

After you add your Active Directory server connections, you may need to delete an Active Directory server connection. For example, you may need to replace your current Active Directory server computer. In Workflow Explorer, you can delete an Active Directory server connection.

Note: You cannot delete an Active Directory server connection that any of your Active Directory sync profiles currently use to import data. Before you can delete that Active Directory server connection, you must perform one of the following actions: Delete all the sync profiles for that Active Directory server connection, or switch all the sync profiles to another server connection.

See “Managing Active Directory sync profiles” on page 270.

To Delete an Active Directory server connection

1. On the ServiceDesk server on the Windows **Start** menu, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the Symantec Workflow Explorer page in the toolbar at the top of the page, click **Credentials**.
3. In the left pane, click **Active Directory**.
4. In the right pane, select the Active Directory server connection profile that you want to delete.
5. In the right pane, click **Delete**.
6. In the confirmation message dialog box, click **OK**.

See “Managing Active Directory server connections” on page 256.

Selecting Active Directory as the authentication method

If you want to use Active Directory as your authentication method for ServiceDesk, you must first add an Active Directory server connection. Then, you can select Active Directory as your authentication method in the Process Manager portal on the **Master Settings** page.

Note: You do not need to reselect Active Directory as your authentication method to add additional Active Directory server connections or sync profiles.

After you select Active Directory as your authentication method, you can add Active Directory sync profiles for your Active Directory server connections.

See “Configuring Active Directory sync profiles” on page 254.

See “Adding Active Directory server connections” on page 257.

To select Active Directory as the authentication method

1. In the Process Manager portal, click **Admin > Portal > Master Settings**.
2. On the **Master Settings** page, expand the **Process Manager Active Directory Settings** section.
3. In **Process Manager Active Directory Settings** section, check **Active Directory Authentication**.
4. (Optional) In the **Process Manager Active Directory Settings** section, select any of the other options that are appropriate for your environment. You can also type information for the Active Directory users that you do not want to import to ServiceDesk.
5. Scroll down to the bottom of the **Master Settings** page and click **Save**.

Testing an Active Directory server connection

After you configure your Active Directory sync profiles, you can test any of your Active Directory server connections. For example, you may want to test the server connection before you run a manual synchronization or after an automatic synchronization fails. In ServiceDesk, you can test the connection on the **Active Directory Sync Profiles** page.

Note: If the connection test fails, report it to the administrator who manages your Active Directory servers.

See “Configuring Active Directory sync profiles” on page 254.

See “Managing Active Directory server connections” on page 256.

See “Managing Active Directory sync profiles” on page 270.

To test an Active Directory server connection

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Test AD Server**.
3. After you view the message that reports the success or failure of the connection, you can close the message dialog box.

New AD Connections Profile and Edit AD connection settings dialog boxes

If your organization chooses to use Active Directory authentication as its authentication method for ServiceDesk, you need to add Active Directory server connections. You may also need to edit the settings for an Active Directory connection. During the addition or the edit of a server connection, you open the **New AD Connection Profile** or the **Edit AD connection settings** dialog box. These dialog boxes let you add information for an Active Directory server connection or edit an existing one.

See "Adding Active Directory server connections" on page 257.

See "Editing the settings of an Active Directory server connection" on page 260.

Table 19-3 Options on the **New AD Connection Profile** and **Edit AD connection settings** dialog boxes

Option	Description
Domain Controller	Lets you type the IP address or host name of your domain controller.
Domain	Lets you type the NETBIOS domain name of your Active Directory. The correct format is as follows: *<MyDom>* Do not use the fully qualified domain name unless it is necessary. For example, your organization might not allow NETBIOS in your network. If you use the fully qualified domain name, the option to create a ServiceDesk user account automatically does not work. The format for the fully qualified domain name is as follows: *<MyDomain.com>*

Table 19-3 Options on the **New AD Connection Profile** and **Edit AD connection settings** dialog boxes *(continued)*

Option	Description
Username **Password**	Lets you specify the credentials of the account that can connect to the Active Directory and retrieve user and group information. You can specify any user in your domain whose privileges are high enough to retrieve users and groups from Active Directory. For security purposes, you must retype the password every time you add or edit an Active Directory server connection.
Default Timeout	Lets you specify the parameters for the default timeout. **Note:** *20000* is the default setting for **Default Timeout**.
Name **Is Default** check box	Lets you specify a name for the Active Directory connection profile. Lets you choose whether to use the Active Directory connection profile as the default profile.

Managing Active Directory sync profile schedules

In ServiceDesk, you can add Active Directory sync profile schedules. These schedules let you schedule automatic update and full synchronizations between your sync profiles and the Active Directory servers to which they are connected. After you add your Active Directory sync profile schedules, you may need to edit a sync profile schedule. You may also need to delete a sync profile schedule. In ServiceDesk, you can manage your Active Directory sync profile schedules.

See “Managing Active Directory sync profiles” on page 270.

Table 19-4 Process for managing Active Directory sync profile schedules

Step	Action	Description
Step 1	Add automatic synchronization schedules.	In ServiceDesk, you can add automatic Active Directory sync profile schedules. See "Adding Active Directory sync profile schedules" on page 266. When adding or editing your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations : ■ Update synchronization ■ Full synchronization
Step 2	(Optional) Edit automatic synchronization schedules.	In ServiceDesk, you can edit an automatic Active Directory sync profile schedule. See "Editing an Active Directory sync profile schedule" on page 268.
Step 3	(Optional) Delete an automatic synchronization schedule.	In ServiceDesk, you can delete an automatic Active Directory sync profile schedule. See "Deleting an Active Directory sync profile schedule" on page 269.

Adding Active Directory sync profile schedules

In ServiceDesk, you can add Active Directory sync profile schedules so that they are available when adding your Active Directory sync profiles.

For example, you add an Active Directory server connection. You know the organizational units and groups that you want your Active Directory sync profiles to import from Active Directory to the Process Manager database. Now, you need to add Active Directory sync profile schedules. After you add these schedules, you can use them to schedule update and full synchronization when adding these Active Directory sync profiles.

Note: Name your Active Directory sync profile schedules so that you can easily associate them with the sync profiles to which you want to assign them. If you ever need to edit the synchronization schedules for any of your Active Directory sync profiles, you must do so on the **Active Directory Sync Profile Schedule** page. You cannot edit the schedule while editing an Active Directory sync profile; you can only select a different schedule or add a new one.

After you add your Active Directory sync profile schedules, they appear in the drop-down lists for the **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile** fields. These fields appear in the **Add Schedule for Active Directory Server** dialog box. This dialog box appears during the addition of an Active Directory sync profile.

The **Schedule For Update Sync Profile** field lets you schedule an automatic synchronization that only updates the changes that have been made to Active Directory since the last synchronization. The **Schedule For Full Sync Profile** field lets you schedule an automatic synchronization that updates the entire Active Directory domain or entire organizational units or groups.

See “Configuring Active Directory sync profiles” on page 254.

See “Managing Active Directory sync profiles” on page 270.

See “Managing Active Directory sync profile schedules” on page 265.

See “Methods for synchronizing Active Directory sync profiles” on page 280.

To add Active Directory sync profile schedules

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profile Schedule**.
2. On the **Sync Profile Schedule** page, at the far right of the title bar, click the **Add Sync Profile Schedule** symbol (green plus sign).
3. In the **Sync Profile Schedule** dialog box, enter the following information:

Name	Lets you name your synchronization schedule.

Select type of schedule	Lets you select when you want the synchronization to occur. The following options let you make additional choices for when the synchronization occurs: ■ **Weekly** Lets you select which day or days of the week you want the synchronization to occur. ■ **Monthly** Lets you specify which day of the month you want the synchronization to occur. ■ **One time only** Lets you select the date that you want the one time synchronization to occur.
Start time	Lets you select what time you want the synchronization to start.

4 When you are finished, click **Save**.

Editing an Active Directory sync profile schedule

After you add your Active Directory sync profile schedules, you can edit any synchronization schedule. In ServiceDesk, you can edit an Active Directory sync profile schedule. For example, after you add an Active Directory sync profile schedule, you discover that it interferes with a maintenance schedule. Now, you need to change the start time of a full synchronization or the time that you want the synchronization to occur.

Note: The changes that you make to an Active Directory sync profile schedule affect any of the sync profiles to which you added that schedule.

After you edit an Active Directory sync profile schedule, the edited schedule appears in the drop-down lists for the **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile** fields. These fields appear in the **Edit Schedule for Active Directory Server** dialog box. This dialog box appears during the edit of an Active Directory sync profile.

The **Schedule For Update Sync Profile** field lets you schedule an automatic synchronization that only updates the changes that have been made to Active Directory since the last synchronization. The **Schedule For Full Sync Profile** field lets you schedule an automatic synchronization that updates the entire Active Directory domain or entire organizational units or groups.

See “Managing Active Directory sync profile schedules” on page 265.

See “Managing Active Directory sync profiles” on page 270.

To edit an Active Directory sync profile schedule

1 In the Process Manager portal, click **Admin > Active Directory > Sync Profile Schedule**.

2 On the **Sync Profile Schedule** page, at the far right of the specific sync profile schedule name, click the **Actions** symbol (orange lightning), and click **Edit AD Sync Profile Schedule**.

3 In the **Edit Active Directory Sync Profile Schedule** dialog box, edit any of the following information:

Name	Lets you name your synchronization schedule.
Select type of schedule	Lets you select when you want the synchronization to occur. The following options let you make additional choices for when the synchronization occurs: ■ **Weekly** Lets you select which day or days of the week you want the synchronization to occur ■ **Monthly** Lets you specify which day of the month you want the synchronization to occur. ■ **One time only** Lets you select the date that you want the one time synchronization to occur.
Start time	Lets you select what time you want the synchronization to start.

4 When you are finished, click **Save**.

Deleting an Active Directory sync profile schedule

After you add your Active Directory sync profile schedules, you can delete update or full synchronization schedules. For example, you may need to delete an obsolete schedule.

After you delete your Active Directory sync profile schedule, it no longer appears in the drop-down lists for the **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile** fields. These fields appear in the **Add Schedule for Active**

Directory Server or **Edit Schedule for Active Directory Server** dialog boxes. These dialog boxes appear during the addition or edit of an Active Directory sync profile.

Note: You cannot delete a sync profile schedule that any of your Active Directory sync profiles currently use. You must edit the sync profiles that use that schedule and select a different update or full synchronization schedule for them to use.

See "Editing an Active Directory sync profile schedule" on page 268.

To delete an Active Directory sync profile schedule

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profile Schedule**.
2. On the **Sync Profile Schedule** page, at the far right of the specific sync profile schedule name, click the **Actions** symbol (orange lightning), and click **Delete Schedule**.
3. In the confirmation message dialog box, click **OK**.

See "Managing Active Directory sync profile schedules" on page 265.

See "Managing Active Directory sync profiles" on page 270.

Managing Active Directory sync profiles

After you add your Active Directory server connections and select Active Directory as your authentication method, you can then add sync profiles for the connections. You can also edit and delete Active Directory sync profiles. In ServiceDesk, you can manage your Active Directory sync profiles.

You can use these Active Directory sync profiles to import data from Active Directory to the Process Manager database. You can target the entire domain, organizational units and groups on the Active Directory server, or specific LDAP queries. You manage these sync profiles in the Process Manager portal.

Before you begin adding your Active Directory sync profiles, you can add synchronization schedules for the sync profiles. After you add or edit an Active Directory sync profile, you may want to run a full synchronization manually before the next scheduled, automatic synchronization

See "Managing Active Directory server connections" on page 256.

See "Managing Active Directory sync profile schedules" on page 265.

See "Methods for synchronizing Active Directory sync profiles" on page 280.

Table 19-5 Process for managing Active Directory sync profiles

Step	Action	Description
Step 1	Add automatic synchronization schedules.	In ServiceDesk, you can add automatic Active Directory sync profile schedules. See "Adding Active Directory sync profile schedules" on page 266. When adding or editing your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations. ■ Update synchronization ■ Full synchronization
Step 2	Add Active Directory sync profiles.	In ServiceDesk, you can add sync profiles for your Active Directory server connections. See "Adding Active Directory sync profiles" on page 272.
Step 3	(Optional) Edit automatic synchronization schedules.	In ServiceDesk, you can edit an automatic Active Directory sync profiles schedule. See "Editing an Active Directory sync profile schedule" on page 268.
Step 4	(Optional) Delete an automatic synchronization schedule.	In ServiceDesk, you can delete an automatic Active Directory sync profiles schedule. See "Deleting an Active Directory sync profile schedule" on page 269.
Step 5	(Optional) Edit an Active Directory sync profile.	In ServiceDesk, you can edit an Active Directory sync profile. See "Editing an Active Directory sync profile" on page 275.
Step 6	(Optional) Delete an Active Directory sync profile.	In ServiceDesk, you can delete an Active Directory sync profile. See "Deleting an Active Directory sync profile" on page 278.
Step 7	(Optional) Manually perform a full synchronization for an Active Directory sync profile.	In ServiceDesk, you can manually perform full synchronizations for the Active Directory sync profile that you specify. See "Running a full Active Directory sync profile synchronization manually" on page 281.

Table 19-5 Process for managing Active Directory sync profiles *(continued)*

Step	Action	Description
Step 8	(Optional) Manually perform update synchronization for an Active Directory sync profile.	In ServiceDesk, you can manually perform update synchronizations for the Active Directory sync profile that you specify. See "Running update Active Directory sync profile synchronization manually" on page 282.
Step 9	(Optional) Manually perform a full synchronization for all Active Directory sync profiles.	In ServiceDesk, you can manually perform full synchronizations for all your Active Directory sync profiles. See "Synchronizing all Active Directory sync profiles manually" on page 283.
Step 10	(Optional) Check the status of an Active Directory sync profile synchronization.	In ServiceDesk, you can view information about the users and groups that are synchronized and the status of the Active Directory sync profile's synchronization. See "Checking the status of an Active Directory sync profile synchronization" on page 284.
Step 11	(Optional) Test an Active Directory server connection.	In ServiceDesk, you can test each Active Directory server connection. For example, the synchronization of an Active Directory sync profile fails. You may want to test the Active Directory server connection. See "Testing an Active Directory server connection" on page 263.

Adding Active Directory sync profiles

If your organization uses Active Directory authentication as its authentication method for ServiceDesk, you may need to add Active Directory sync profiles. These sync profiles let you import data from Active Directory to the Process Manager database. After you add your Active Directory server connections, you can add sync profiles for those connections. In ServiceDesk, you can add Active Directory sync profiles at any time.

You can add Active Directory sync profiles to target the entire domain, organizational units and groups on the Active Directory server, or specific LDAP queries. For example, you add a new organizational unit to Active Directory. You can add a sync profile for it in the Process Manager portal.

See "Configuring Active Directory sync profiles" on page 254.

See "Managing Active Directory sync profiles" on page 270.

See "Methods for synchronizing Active Directory sync profiles" on page 280.

To add Active Directory sync profiles

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, at the far right of the **Active Directory Sync Profiles** title bar, click the **Actions** symbol (orange lightning), and click **Add AD Sync Profile**.

3 In the **Add Active Directory Sync Profile** dialog box, type or select the following information:

AD Sync Profile Name Lets you specify a name for the sync profile.

Select Connection Lets you choose which Active Directory server connection you want the sync profile to target.

AD Server Email Domain Lets you specify an email address for the users that you obtain from Active Directory. Use the following format:

<domain.com>

ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.

Auto Create User On Initial Login Lets you have a ServiceDesk user account created automatically when a new user logs on.

A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.

AD Users Default Groups Lets you select the group to which users are added when their accounts are created automatically.

The **All Users** group is the most typical selection.

This option is available when you check **Auto Create User on Initial Login**.

4 When you are finished, click **Next**.

Note that if you do not enter the critical information or a connection cannot be made, a warning is displayed and you cannot proceed.

5 Under **Synchronization Option**, select one of the following options:

Entire Domain	Connects ServiceDesk with your entire Active Directory.
Organization units	Connects ServiceDesk with one or more Active Directory organizational units, which you select from the tree view that appears in this dialog box. The tree view displays the organization units that are defined in the specified Active Directory.
Groups	Connects the ServiceDesk with one or more Active Directory groups, which you select from the tree view that appears in this dialog box. The tree view displays the groups that are defined in the specified Active Directory.
Specify LDAP Queries	Connects ServiceDesk to a specific LDAP Query.

6 When you are finished, click **Next**.

7 In the **Add Active Directory Field Mapping** dialog box, select which fields in Active Directory you want to map to which fields in Process Manager and click **Next**.

Note that normally you do not need to change any field mapping settings. Symantec recommends that you do not change any mappings to key fields, such as Primary Email ID (Email address), first names, and last names.

8 In the **Add Schedule for Active Directory Server** dialog box, select a schedule in the drop-down lists for **Schedule For Full Sync Profile** and **Schedule For Update Sync Profile**.

Note that if the proper schedules do not appear in the drop-down lists for **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile,** you must add schedules.

To add a schedule, click **Add Schedule**, add your schedules, and click **Save**. Repeat the process if you need to add another schedule. When you are done, the added schedules appear in the drop-down lists.

See “Adding Active Directory sync profile schedules” on page 266.

9 When you are finished, click **Finish**.

Editing an Active Directory sync profile

After you add your Active Directory sync profiles, you can edit the settings for any sync profile. In ServiceDesk, you can change the sync profile settings to target a different organizational unit or group on the Active Directory server. You can map a different Active Directory field to a Process Manager field.

See “Managing Active Directory sync profiles” on page 270.

To edit an Active Directory sync profile

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Edit AD Sync Profile**.
3. In the **Edit Active Directory Sync Profiles** dialog box, you can edit the following information:

AD Sync Profile Name

Lets you specify a name for the sync profile.

Select Connection

Lets you choose which Active Directory server connection you want the sync profile to target.

AD Server Email Domain

Lets you specify an email address for the users that you obtain from Active Directory. Use the following format:

<domain.com >

ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.

Auto Create User On Initial Login

Lets you have a ServiceDesk user account created automatically when a new user logs on.

A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.

AD Users Default Groups

Lets you select the group to which users are added when their accounts are created automatically.

The **All Users** group is the most typical selection.

This option is available when you check **Auto Create User on Initial Login**.

4. When you are finished, click **Next**.

   Note that if you do not enter the critical information or a connection cannot be made, a warning is displayed and you cannot proceed.

5. In the **Edit Active Directory Sync Profile** dialog box under **Synchronization Option**, you can select a different target for the synchronization. If the target of your synchronizations has changed, select one the following options:

   Entire Domain Synchronizes ServiceDesk with your entire Active Directory.

   Organization units Synchronizes ServiceDesk with one or more Active Directory organizational units, which you select from the tree view that appears in this dialog box. The tree view displays the organization units that are defined in the specified Active Directory.

   Groups Synchronizes ServiceDesk with one or more Active Directory groups, which you select from the tree view that appears in this dialog box. The tree view displays the groups that are defined in the specified Active Directory.

   Specify LDAP Queries Synchronizes ServiceDesk to a specific LDAP Query.

6. When you are finished, click **Next**.

7. In the **Edit Active Directory Field Mapping** dialog box, you can edit which fields in Active Directory you want to map to which fields in Process Manager.

   Note that normally you do not need to change any field mapping settings. Symantec recommends that you do not change key fields mapping, such as Primary Email Id (Email address), first names, and last names.

8 When you are finished, select one of the following options:

Save	If you do not want to edit the sync profile schedules, click **Save**. The dialog box closes, your changes are saved, and you are finished.
Next	If you want to edit the sync profile schedules, click **Next**. Go to step 9. Note that editing a sync profile schedule means selecting or adding a different schedule. If you want to edit the sync profile schedule, you must edit it from the **Active Directory Sync Profiles Schedule** page. See “Editing an Active Directory sync profile schedule” on page 268.

9 In the **Edit Schedule for Active Directory Server** dialog box, you can select a different schedule in the drop-down lists for **Schedule For Full Sync Profile** and **Schedule For Update Sync Profile**.

Note that if the proper schedule does not appear in the drop-down lists for **Schedule For Full Sync Profile** or **Schedule For Update Sync Profile**, you must add a schedule.

To add schedule, click **Add Schedule**, add your schedules, and click **Save**. When you are done, the added schedule appears in the drop-down lists.

See “Adding Active Directory sync profile schedules” on page 266.

10 When you are finished, click **Finish**.

Deleting an Active Directory sync profile

After you add your Active Directory sync profiles, you can delete any of the Active Directory sync profiles that you no longer need. For example, you may need to delete an obsolete sync profile.

To delete an Active Directory sync profile

1 In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.

2 On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profile**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Delete AD Sync Profile**.

3 In the confirmation message dialog box, click **OK**.

See “Managing Active Directory sync profiles” on page 270.

Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes

If your organization uses Active Directory authentication for its authentication method for ServiceDesk, you need to add Active Directory sync profiles. You may also need to edit an Active Directory sync profile. During the addition or edit of your Active Directory sync profiles, you open the **Add AD Sync Profile** or the **Edit AD Sync Profile** dialog box. These dialog boxes let you add information for a new Active Directory sync profile or edit an existing one.

See “Adding Active Directory sync profiles” on page 272.

See “Editing an Active Directory sync profile” on page 275.

Table 19-6 Options on the **Add Active Directory Sync Profiles** dialog box and **Edit Active Directory Sync Profiles** dialog boxes

Option	Description
AD Sync Profile Name	Lets you specify a name for the sync profile.
Select Connection	Lets you choose which Active Directory server connection you want the sync profile to target.
AD Server Email Domain	Lets you specify an email address for the users that you obtain from Active Directory. Use the following format: domain.com ServiceDesk requires that all users have an email address, but Active Directory does not. This domain is appended to the user name of any user who does not have an email address.
Auto Create User On Initial Login	Lets you have a ServiceDesk user account created automatically when a new user logs on. A new user who logs on to ServiceDesk is authenticated against the Process Manager database. If the user does not have an account there, and this check box is checked, the user is authenticated against Active Directory. If the user has an Active Directory account, a mirror account is created in the Process Manager database.

Table 19-6 Options on the **Add Active Directory Sync Profiles** dialog box and **Edit Active Directory Sync Profiles** dialog boxes *(continued)*

Option	Description
AD Users Default Groups	Lets you select the group to which users are added when their accounts are created automatically. The **All Users** group is the most typical selection. This option is available when the following check box is checked: **Auto Create User on Initial Login**.

Methods for synchronizing Active Directory sync profiles

When your organization uses Active Directory authentication as its authentication method for ServiceDesk, ServiceDesk can synchronize with Active Directory. The synchronization lets you add and update Active Directory users and groups in the Process Manager database. You can add automatic synchronization schedules to your Active Directory sync profiles. You can also manually run Active Directory sync profile synchronizations.

When ServiceDesk synchronizes with Active Directory, you can view information about the users and groups that are synchronized and the status of the synchronization.

See “About Active Directory synchronization” on page 253.

See “Configuring Active Directory sync profiles” on page 254.

See “Managing Active Directory sync profiles” on page 270.

See “Checking the status of an Active Directory sync profile synchronization” on page 284.

Table 19-7 Methods for synchronizing Active Directory sync profiles

Method	Description
Run automatic update and full synchronizations.	In ServiceDesk, you can add automatic Active Directory sync profile schedules. See "Adding Active Directory sync profile schedules" on page 266. When adding your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations: ■ Update synchronization ■ Full synchronization See "Adding Active Directory sync profiles" on page 272.
Manually run a full synchronization.	In ServiceDesk, you can manually run a full Active Directory sync profile synchronization at any time. This process lets you run a full synchronization on the specified Active Directory sync profile. See "Running a full Active Directory sync profile synchronization manually" on page 281.
Manually run update synchronization.	In ServiceDesk, you can manually run update Active Directory sync profile synchronization at any time. This process lets you synchronize an Active Directory sync profile with only the changes that have been made to it since the last synchronization. See "Running update Active Directory sync profile synchronization manually" on page 282.
Manually synchronize all the Active Directory sync profiles.	In ServiceDesk, you can manually run a full synchronization of all your Active Directory sync profiles at any time. This process lets you synchronize all your sync profiles for each Active Directory server connection. See "Synchronizing all Active Directory sync profiles manually" on page 283.

Running a full Active Directory sync profile synchronization manually

In ServiceDesk, you can manually synchronize an Active Directory sync profile with Active Directory at any time between the automatic synchronization intervals. For example, when you add a new Active Directory sync profile, you can manually synchronize it immediately instead of waiting for the next automatic synchronization.

This process runs a full synchronization as follows:

- If the Active Directory sync profile includes the entire Active Directory server domain, the entire domain is synchronized.

- If the Active Directory sync profile includes only specific Active Directory organizational units or groups, the entire contents of those units and groups are synchronized.

See "About Active Directory synchronization" on page 253.

See "Configuring Active Directory sync profiles" on page 254.

See "Managing Active Directory sync profiles" on page 270.

See "Methods for synchronizing Active Directory sync profiles" on page 280.

Warning: Any users that are connected to Process Manager might be disconnected during the synchronization.

You can check the status of the synchronization during the process or after the process finishes.

See "Checking the status of an Active Directory sync profile synchronization" on page 284.

To run a full Active Directory sync profile synchronization manually

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Run Reset Sync Profile**.
3. When the dialog box that announces the start of the synchronization appears, you can close it.

Running update Active Directory sync profile synchronization manually

In ServiceDesk, you can manually run update synchronization of an Active Directory sync profile with Active Directory at any time between automatic synchronization intervals. With this synchronization process, you synchronize only the changes that were made to Active Directory since the last synchronization.

For example, after you add or remove users in Active Directory, you want to apply those changes to Active Directory sync profile immediately. You can check the status of the synchronization during the process or after the process finishes.

See "About Active Directory synchronization" on page 253.

See "Managing Active Directory sync profiles" on page 270.

See “Methods for synchronizing Active Directory sync profiles” on page 280.

See “Checking the status of an Active Directory sync profile synchronization” on page 284.

To run update Active Directory sync profile synchronization manually

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Run Update Sync Profile**.
3. When the dialog box that announces the start of the synchronization appears, you can close it.

Synchronizing all Active Directory sync profiles manually

In ServiceDesk, you can manually synchronize all your Active Directory sync profiles with all Active Directory servers to which ServiceDesk is connected. For example, you might need to recover after a power loss. This synchronization method includes the synchronization of all the Active Directory sync profiles for each Active Directory server connection.

See “About Active Directory synchronization” on page 253.

See “Configuring Active Directory sync profiles” on page 254.

See “Managing Active Directory sync profiles” on page 270.

See “Methods for synchronizing Active Directory sync profiles” on page 280.

To synchronize all Active Directory sync profiles

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, at the far right of the **Active Directory Sync Profiles** title bar, click the **Actions** symbol (orange lightning), and click **Run AD Sync Profile**.
3. When the dialog box that announces the start of the synchronization appears, you can close it.

Checking the status of an Active Directory sync profile synchronization

When ServiceDesk synchronizes with Active Directory, you can view information about the users and groups that are synchronized and the status of the synchronization. For example, if your Active Directory is large, you might periodically check the status as the synchronization runs. If a synchronization is not running, the status check shows information for the last synchronization that occurred. For example, you can verify that an overnight synchronization completed successfully. You can check the status of an Active Directory synchronization in the Process Manager portal from the **Active Directory Sync Profiles** page.

See "Configuring Active Directory sync profiles" on page 254.

See "Managing Active Directory sync profiles" on page 270.

See "Methods for synchronizing Active Directory sync profiles" on page 280.

To check the status of an Active Directory sync profile synchronization

1. In the Process Manager portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, under **Active Directory Sync Profiles**, at the far right of the specific sync profile name, click the **Actions** symbol (orange lightning), and click **Check Sync Status**.
3. The **Sync Process Status** dialog box opens and displays status of the sync profile synchronization.
4. If you check the status of a synchronization during the synchronization, you can click **Refresh** to update the display.
5. When you are finished viewing the status information, click **Close**.

Migrating data from ServiceDesk 7.1 SP2, 7.1 SP1, and 7.0 MR2

This appendix includes the following topics:

Migrating data from ServiceDesk 7.1 SP2

You can leverage some data from ServiceDesk 7.1 SP2 in ServiceDesk 7.5.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See "Configuring ServiceDesk" on page 147.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets

- Close Problem Management tickets
- Closed knowledge base submission tickets
- End User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 tickets to ServiceDesk 7.5.

See "About migrating data to ServiceDesk 7.5" on page 153.

Migrating data from ServiceDesk 7.1 SP1

You can leverage some data from ServiceDesk 7.1 SP1 in ServiceDesk 7.5.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See "Configuring ServiceDesk" on page 147.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets
- Close Problem Management tickets
- Closed knowledge base submission tickets
- End User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 tickets to ServiceDesk 7.5.

See "About migrating data to ServiceDesk 7.5" on page 153.

Migrating data from ServiceDesk 7.0 MR2

You can leverage some data from ServiceDesk 7.0 MR2 in ServiceDesk 7.5.

Note: Before you migrate data to ServiceDesk 7.5, make sure to import or add your users and groups. Reports cannot match closed tickets to process workers if they have not been created in ServiceDesk.

See "Configuring ServiceDesk" on page 147.

You cannot migrate the following data:

- Open process data
- Active process data

You can migrate the following ticket types:

- Closed Incident Management tickets
- Closed Change Management tickets
- Close Problem Management tickets
- Closed knowledge base submission tickets
- End User Surveys
- User-defined processes

You can access this historical ticket data from ServiceDesk 7.5 for reporting purposes.

For instructions on how to migrate this data and to access to the migration scripts, see the article Migrate existing closed ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 tickets to ServiceDesk 7.5.

See "About migrating data to ServiceDesk 7.5" on page 153.

Appendix B

Migrating data from Altiris® Helpdesk Solution™ 6.x

This appendix includes the following topics:

About migrating data from Helpdesk Solution 6.x

You can leverage specific data from Helpdesk Solution 6.x in ServiceDesk. You can migrate your categories and knowledge base contents. You can link your Helpdesk Solution incidents to corresponding incident tasks in ServiceDesk. You can then work these incidents in ServiceDesk. You use the Helpdesk Solution migration links in the Service Catalog to migrate Helpdesk Solution data to ServiceDesk. When migrating data from Helpdesk Solution to ServiceDesk, you must keep both environments operational.

Note: Symantec ServiceDesk replaces the functionality of Helpdesk Solution 6.x and earlier. ServiceDesk does not upgrade or install over Helpdesk Solution. ServiceDesk is installed on a different server and uses different databases.

You use the Helpdesk Solution migration links in the Service Catalog to migrate Helpdesk Solution data to ServiceDesk. When migrating data from Helpdesk Solution to ServiceDesk, you must keep both environments operational.

Not all data is supported for migration. The following table includes the data items that can be migrated and links to instructions on how to migrate each item.

Table B-1 The Helpdesk Solution 6.x data that ServiceDesk can use

Data	Description
Helpdesk Solution incidents	Incidents cannot be directly migrated to the ServiceDesk server. However, each Helpdesk Solution incident can be linked to a new, corresponding incident task in ServiceDesk. You can see and work those incidents in the ServiceDesk portal, but their data always remains on the Helpdesk Solution server. Best practice is to stop entering new incidents into Helpdesk Solution after the ServiceDesk system is operational and the incident migration is performed. See "Migrating incidents from Helpdesk Solution 6.x" on page 289.
Helpdesk Solution categories	The categories are migrated from Helpdesk Solution to ServiceDesk. See "Migrating categories from Helpdesk Solution 6.x" on page 293.
Helpdesk Solution knowledge base contents	The knowledge base (KB) articles are migrated from Helpdesk Solution to ServiceDesk. See "Migrating knowledge base (KB) content from Helpdesk Solution 6.x" on page 294.

See "About migrating data to ServiceDesk 7.5" on page 153.

Migrating incidents from Helpdesk Solution 6.x

You can migrate the incidents from Helpdesk Solution 6.x so that you can use them in ServiceDesk. You migrate Helpdesk Solution incidents in the Process Manager portal.

The Incident Migration wizard lets you select the incidents to migrate and determine when to close the migrated incidents. The migration continues for some time after you finish the wizard, depending on how many incidents you migrate.

See "How Helpdesk Solution 6.x incident data corresponds to ServiceDesk incidents" on page 291.

See "About working Helpdesk Solution 6.x incidents in ServiceDesk" on page 292.

Warning: In most cases, this migration should not be run more than once.

At the end of this procedure, you can remove the **Migrate Helpdesk 6 Incidents** link from the Service Catalog to prevent running the migration again.

Best practice is to stop entering new incidents into Helpdesk Solution after the ServiceDesk system is operational and the incident migration is performed.

To migrate incidents from Helpdesk Solution

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**.
3. Under **New Requests**, click **Migrate Helpdesk 6 Incidents**.
4. In the **Incident Migration** wizard, on the **Welcome** page, type the Symantec Management Platform address and the credentials for the Helpdesk Solution installation whose data you want to migrate.
5. When you are finished, click **Next**.
6. On the **Choose Incident Types** page, select the incidents by their status that you want to migrate to ServiceDesk.

   Note that you do not need to migrate closed incidents.
7. Click **Next**.
8. On the **Fetching Incidents List** page, the Incident Migration Wizard looks up all the requested incidents from Helpdesk Solution.
9. On the **Confirmation** page, review the incident statuses that you selected, and then complete the following options:

Until which "close" status(es) would you like to monitor the migrated incidents?	Select the Helpdesk Solution incident statuses that should trigger the closure of the migrated incidents in ServiceDesk. For example, you select **Escalated to Vendor**. When a support technician sets a Helpdesk Solution incident to that status, the corresponding ServiceDesk incident is closed.
Email address	Type an email address for ServiceDesk to send an email to when the migration is complete.

10. When you are finished, click **Submit**.

11 On the **Finished** page, select one of the following options:

Remove Link From Service Catalog

Removes the link for incident migration from the Service Catalog.

Symantec recommends that you remove the link after you perform this task once.

Leave Link In Service Catalog

Leaves the link in the Service Catalog.

You should leave the link only if there is an issue with the first migration attempt.

12 When the wizard finishes, click **Close**.

How Helpdesk Solution 6.x incident data corresponds to ServiceDesk incidents

When you migrate incidents from Helpdesk Solution 6.x to ServiceDesk, the incidents are not moved or copied to the ServiceDesk server. Instead, each migrated Helpdesk Solution incident is linked to a new, corresponding incident task in ServiceDesk. The new ServiceDesk incidents are assigned to the Migrated Incidents category and they obtain their header data from the original Helpdesk Solution incidents.

See "About migrating data from Helpdesk Solution 6.x" on page 288.

See "Migrating incidents from Helpdesk Solution 6.x" on page 289.

Table B-2 Helpdesk Solution incident data and corresponding ServiceDesk incident data

Data in Helpdesk Solution 6.x	Data in ServiceDesk
Assigned to	Contacts
Category	Added to the task header
Comments	History, user comment
Date Created	Open date
Description	Incident Description
Equipment	Related Items
Incident contact (submitter)	Primary contact
Last Comment	History

Table B-2 Helpdesk Solution incident data and corresponding ServiceDesk incident data *(continued)*

Data in Helpdesk Solution 6.x	Data in ServiceDesk
Last Date change	History
Location	Related Items
Priority	Priority
Resolution	History, user comment
Status	Status
Title	Incident Title
Title ID	Incident Title
Ticket number	Added to the task Name (title) and Description

About working Helpdesk Solution 6.x incidents in ServiceDesk

ServiceDesk can use incident data from an installation of Helpdesk Solution 6.x.

See “About migrating data from Helpdesk Solution 6.x” on page 288.

During the migration, for each Helpdesk Solution incident, a task that has the same priority is created in ServiceDesk. The data from the Helpdesk Solution incidents sets the status, title, priority, and description of the new ServiceDesk tasks. The new tasks are assigned to the Migrated Incidents category so that they are easily distinguished from ServiceDesk incidents.

See “How Helpdesk Solution 6.x incident data corresponds to ServiceDesk incidents” on page 291.

The support technician works a migrated incident by opening its task in ServiceDesk. When the incident reaches a specific status, the copy of the incident in ServiceDesk is closed. The statuses that trigger the closure are selected during the incident migration process.

Warning: The Helpdesk Solution incidents remain on the Helpdesk Solution server and they are linked to the ServiceDesk incidents throughout their life cycle. Therefore, do not delete or shut down the Helpdesk Solution server immediately. Monitor the Migrated Incidents category in ServiceDesk and when all its incidents are closed, then it is safe to shut down Helpdesk Solution.

Migrating categories from Helpdesk Solution 6.x

You can migrate the categories from Helpdesk Solution 6.x so that you can use them in ServiceDesk. You can migrate the categories in the Process Manager portal.

Category migration can be run multiple times.

To migrate categories from Helpdesk Solution

1. In the Process Manager portal, click **Submit Request**.
2. On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**.
3. Under **New Requests**, click **Helpdesk 6 Category Migration Wizard**.
4. In the **Migrate Categories** wizard, on the **Welcome** page, type the Symantec Management Platform address and the credentials for the Helpdesk Solution whose data you want to migrate.
5. When you are finished, click **Next**.
6. On the **Choose Categories** page, select the categories to migrate, and then click **Migrate**.
7. When the migration finishes, click **Close**.

See “About migrating data from Helpdesk Solution 6.x” on page 288.

About migration of knowledge base (KB) content from Helpdesk Solution 6.x

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.

See “Migrating knowledge base (KB) content from Helpdesk Solution 6.x” on page 294.

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. If you run the migration wizard in the background, you can check the **Configuration Logging Utility** for 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 on the **Migration Review** page. 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.
- Try to migrate smaller subsets of those articles to help identify a problematic article.

Also, in the migration wizard, on the **Migration Review** page, you should select **Monitored Migration**. The selection 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.

After migration, you can delete the copied directory, unless failures occurred. If you want to rerun the migrator for the failed content, do not delete the copied directory. 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.

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.

Migrating knowledge base (KB) content from Helpdesk Solution 6.x

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.

See "About migration of knowledge base (KB) content from Helpdesk Solution 6.x" on page 293.

Be advised that the migration process takes a long time to complete.

To migrate knowledge base (KB) content from Helpdesk Solution 6.5

1. Copy the directory that houses the KB files to the ServiceDesk server.

   This requirement is due to .NET restrictions at the command-line level.

2. The directory structure for the KB content to copy must follow this format:

   <drive>`:\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.

3. Grant the Network Service account access to the directory.

4. In the Process Manager portal, click **Submit Request**.

5. On the **Submit Request** page, under **Service Catalog**, click **Administrative Services**.

6. Under **New Requests**, click **Migrate KB Articles from Helpdesk 6.5**.

7. In the KB Migration Wizard, on the **Welcome** page, click **Continue**.

8. On the **Source Selection** page, type the location of the KB Libraries that you previously copied to your ServiceDesk server and then click **Next**.

   Use the following format:

   <drive>`:\Libraries\another directory\Articles`

9. On the **Library Selection** page, select the libraries to migrate and then click **Add Libraries to Migration List**.

10. On the **Topic Selection** page, select the KB topics to migrate and then click **Add Topics to Migration List**.

11. On the **Migration Review** page, type an email address for ServiceDesk to send an email to when the migration is complete.

12. When you are finished, select one of the following options:

Background Migration **(Recommended)**	■ Lets the migration of the knowledge base content occur in the background. Symantec recommends that you use this migration method. ■ When you click Background Migration, the KB Migration Wizard closes. ■ You receive status updates from the migration process by email

Monitored Migration **(Used for Trouble Shooting)**	■ Lets you monitor the migration in real-time status. ■ This method requires that the browser remain open. If you close the browser, before the migration is finished, the migration process is stopped. You must restart the migration process from the beginning. ■ Because this method provides more detail, Symantec recommends that you use this method only if a migration fails.

13 (Optional) If you chose to monitor the migration, on the **Migrating** page, the **Incident Migration Wizard** migrates the topics that you selected from Helpdesk Solution 6.5.

14 (Optional) If you chose to monitor the migration, on the **Confirmation** page, review the details of the migration. When you are finished, close the migration wizard.

Default categories in ServiceDesk

This appendix includes the following topics:

- Default categories for incidents and default classifications for problems

Default categories for incidents and default classifications for problems

ServiceDesk uses categories to classify incidents and route them to the appropriate incident technician or group queue. The person that creates the incident can select a category for that incident. The category also helps sort incidents for reports. ServiceDesk also uses classifications to classify problems. During the initial problem analysis, the problem analyst can select a classification for the problem.

ServiceDesk contains predefined incident categories and problem classifications, which can be used immediately or edited to meet your organization's requirements.

Table C-1 Default categories for incidents and default classifications for problems

Main category or classification	Category or classification level 2	Category or classification level 3
Hardware	**Desktop**	■ **Backup** ■ **Disk** ■ **Memory** ■ **Network** ■ **Office** ■ **PC Personality**

Table C-1 Default categories for incidents and default classifications for problems *(continued)*

Main category or classification	Category or classification level 2	Category or classification level 3
Hardware	**Drive**	N/A
Hardware	**Handheld**	■ **Can't Sync** ■ **Other**
Hardware	**Keyboard**	N/A
Hardware	**Monitor**	N/A
Hardware	**Mouse**	N/A
Hardware	**Notebook**	■ **Backup** ■ **Disk** ■ **Docking Station** ■ **Employee** ■ **Fax** ■ **Machine Discovery** ■ **Memory** ■ **Modem** ■ **Network** ■ **NIC** ■ **Other**
Hardware	**Phone**	■ **No Dial Tone** ■ **Other** ■ **Reset Voice Mail Pin** ■ **Voice Mail Not Working**
Hardware	**Printer**	■ **Jammed** ■ **Other** ■ **Out of Toner**
Hardware	**Server**	■ **CPU or Blade** ■ **Disk** ■ **Memory** ■ **Other**

Table C-1 Default categories for incidents and default classifications for problems *(continued)*

Main category or classification	Category or classification level 2	Category or classification level 3
How To	■ **Access Email** ■ **Access the Web** ■ **Install Printer Drivers** ■ **Other** ■ **Recover Deleted Files** ■ **Use Handheld** ■ **View Email Attachment**	N/A
Internet	■ **Can't Browse Web Site** ■ **Other**	N/A
Microsoft Office	N/A	N/A
Network	■ **Can't Access Some Resources** ■ **No Connection** ■ **Other**	N/A
Service	**Email**	■ **Can't Send Email** ■ **Email Won't Run** ■ **Not Receiving Email** ■ **Other**
Software	■ **Deployment Failure** ■ **Migration Failure** ■ **Operating System** ■ **Other** ■ **Sw Delivery Failure**	N/A

Index