Symantec™ ServiceDesk 7.1 SP2 User Guide

Symantec™ ServiceDesk 7.1 SP2 User Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Section 1

Introducing ServiceDesk

Chapter 1

Introducing ServiceDesk

This chapter includes the following topics:

About ServiceDesk

Symantec ServiceDesk is an ITIL-compliant service management tool that lets you improve your IT infrastructure and provide a higher level of service. It incorporates Symantec Workflow technologies to manage service tickets, provide reports, and integrate with other Symantec products such as the Configuration Management Database (CMDB).

ServiceDesk requires a completed installation and implementation of a Symantec Management Platform 7.1 product. The ServiceDesk solution software is installed using the standard Symantec Management Platform mechanisms.

ServiceDesk includes all the primary ITIL Service Management processes. Processes in ServiceDesk include Incident Management, Problem Management, Change Management, and a Knowledge Management system. ServiceDesk also includes a Service Catalog.

After you install ServiceDesk, it is ready to use. However, you might choose to customize some aspects of ServiceDesk to meet your organization’s specific requirements. Because all ServiceDesk processes are based on workflows, you can customize the processes without making code-level changes.

For information about the kinds of modifications you can perform, see the *ServiceDesk Customization Guide* at the following URL:

http://www.symantec.com/docs/DOC2150

Table 1-1 Key features of ServiceDesk

Feature	Description
ITIL-based processes	All ServiceDesk processes are fully ITIL-based, which lets you implement a full ITIL solution.
Ready-to-use workflows and processes	ServiceDesk includes a set of high-quality, ITIL-based processes that have undergone extensive testing and development effort.
Easy customization	All ServiceDesk processes and forms are easy to customize using the Workflow Designer tool. See "About Workflow Designer" on page 40.
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 shown what is relevant for the particular point they are at in the process. The user is 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	You can define the normal business hours for your organization, which accounts for holidays and weekends. This business hours support allows for accurate Service Level Agreement reporting and accurate reporting of average response time and resolution time.
Email notifications	Email notifications are built into the ITIL processes. Email notifications keep users aware of changes to ticket status, and allow users to verify that an issue is fixed. In any process, email notifications can be used to notify the contacts that are associated with a ticket, assign tasks, and send alerts.
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. When a user has not responded to a Change Management approval task, an escalation may also be triggered.
Integration with other products	ServiceDesk can integrate with other products through the actions and URL calls that can trigger events in other systems. ServiceDesk Web services can also be used to display ServiceDesk processes and forms in third-party applications such as Microsoft SharePoint.

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

Feature	Description
Advanced reporting mechanisms	Advanced reporting mechanisms are included in ServiceDesk. Reports are easy to create and customize. In addition, report templates can be created to let groups and users customize and save their own reports. Reports can be defined and scheduled to run periodically, and 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 level.

Components of ServiceDesk

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

Table 1-2 Components of ServiceDesk

Component	Description
ServiceDesk solution software	The ServiceDesk solution software is installed on the Symantec Management Platform computer. This software provides the following functions: ■ Management of the ServiceDesk licensing The Symantec Installation Manager (SIM) installs the ServiceDesk solution software and applies the ServiceDesk licenses. ■ The installation file that is used to install the ServiceDesk application software on the ServiceDesk server computer. The ServiceDesk server computer is different from the Symantec Management Platform computer. ■ The ServiceDesk pages that appear in the Symantec Management Console. In the **Symantec Management Console**, you can access a page that lets you download the ServiceDesk installation file. ■ Integration between the ServiceDesk application software and the Configuration Management Database (CMDB). See "About ServiceDesk solution software" on page 43.

Table 1-2 Components of ServiceDesk *(continued)*

Component	Description
ServiceDesk application software	Incorporates all the Symantec Workflow technologies that manage service tickets, provide reporting capabilities, and integrate with other Symantec products. The ServiceDesk application software is installed on the ServiceDesk server computer. It cannot be installed on the same computer as Helpdesk Solution.
Workflow Designer	A tool that lets an administrator customize workflows to meet the needs of the organization. See "About Workflow Designer" on page 40. Workflow Designer is typically installed on a client computer. However, it can also be installed on the ServiceDesk server computer.
ServiceDesk portal	A Web-based interface that provides access to the ServiceDesk application software. The users of ServiceDesk access the portal from their Web browsers and use the portal to run the workflow processes. The ServiceDesk portal resides on the ServiceDesk server computer. The ServiceDesk portal is accessible from most Web browsers. See "About the ServiceDesk portal" on page 50.
Workflow Server software	The server-side software that includes the workflow extensions that are required to run the core workflow processes. These extensions must run on the server to which the workflows have been deployed, which is the ServiceDesk server computer. The ServiceDesk server is sometimes referred to as the Workflow server . See "About Workflow Server" on page 40.
Workflows	Definitions of the events or steps that a process can follow. The data that is provided for a specific process determines the path that the process takes through the workflow. ServiceDesk contains the core workflows that you can use immediately without customization. The core workflows let you manage service tickets and perform other service-related activities. The workflows and processes reside on the ServiceDesk server computer. See "About workflows, processes, tickets, and tasks" on page 33.
Process Manager (ServiceDesk) database	Stores the Process Manager details such as groups, users, and permissions. Other applications can use the Process Manager database. For example, it is included with Workflow Solution. When you install ServiceDesk, the Process Manager database is expanded to become the ServiceDesk database. However, it typically is referred to as the Process Manager database. The default name for the actual database is ProcessManager. It resides on the SQL Server computer.

Table 1-2 Components of ServiceDesk *(continued)*

Component	Description
Replication database	Replicates certain data from the Process Manager database. You can either copy or move the original data to the replication database or to a file. Use the database replication for archiving or for improving performance of the Process Manager database. The default name for the actual database is ProcessManagerReplication. It typically resides on the same SQL Server computer as the Process Manager database. See "About replicating the Process Manager database" on page 379.
Analysis database	Stores the configuration details and contains the built-in tools that facilitate the use of the data in the Process Manager database for reporting. The default name for the actual database is ProcessManagerAnalysis. It resides on the SQL Server computer.

What's new in this version

Table 1-3 List of new features in ServiceDesk 7.1

Feature	Description
Support for Windows Server 2008.	Windows Server 2008 and 2008 R2 are now supported.
Support for SQL Server 2008.	SQL Server 2008 and SQL Server 2008 R2 are now supported.
New on-demand report for the Administrator for checking active licenses.	The new report can be found by clicking **Reports > Default > Licensing Information.**
The Administrator can install an upgraded process as a separate project.	The upgraded project can later be compared to a previous version using the **Comparison Tool**. For more information, see *Workflow Solution Users's Guide*.
Documentation for setting up distributed environment for scaling.	For more information, see *ServiceDesk Customization Guide*.
New routing and notification rules for events within the incident management process.	The Administrator can configure routing and notification rules for specific events within the incident management process.

Table 1-3 List of new features in ServiceDesk 7.1 *(continued)*

Feature	Description
New event-specific rule sets.	The Administrator is able to select one of the events for which to configure a rule set. Default rule sets are provided.
New **Automation Rules** interface.	The Administrator can configure a sequenced set of rules to execute at specific events in the incident management process. A rule is comprised of a composite condition and an action. For example, some of the conditions available are: ■ Impact. ■ Location. ■ Priority. ■ Affected user.
Incident Analyst is now able to reassign an incident during reclassification of that incident.	The **Reclassify** form is modified to force the user to move past the reclassify screen explicitly, either by saving, or skipping the reclassification. Next the User is taken to a page that assures them their data has been saved with an option to either close the form or reassign it.
Incident Analyst receives a confirmation screen after new incident template has been created.	A confirmation screen is added at the end of the template process that displays the items that were included in the template.
Incident Worker is now able close incidents without sending out a survey.	Incident Worker is able to close and resolve a group of related incidents using the **Quick Close** process without survey being sent.
Managers now have the ability to reassign pending tasks.	
The User can now view related incidents for any **Configuration Item**.	The User can right-click on a **Configuration Item** in their SMP to view related incidents. A link can be selected which takes them directly to the process view page for that incident.
Multiple new service requests are available.	The following new service request processes are available: ■ A service catalog item that allows users to request a password reset. ■ A service catalog item that allows users to request access to a shared folder.

Table 1-3 List of new features in ServiceDesk 7.1 *(continued)*

Feature	Description
The default process view page has been modified to include a **Quick Service** links section.	The default process view page, **Quick Service** links section contains two new ServiceDesk processes: **Reset Password** and **Request Access to Network Share.**
The Technician can move incident from resolved to close without the user having to complete the survey.	
The incident now automatically moves from resolved state to close state.	The incident moves from the resolved state to the closed state when the user survey task times out. The default timeout has been shortened and can now be changed.
The Analyst can create a knowledge base article from an incident regardless of its status.	
The Technician has the ability to change the primary contact on an incident.	
Better visibility for submitter and affected user on the process view page of an incident.	The process view page of an incident has been modified to make the submitter and affected user more visible on the screen. In addition the Technician can add and delete contacts.
New Web part for the Technician for viewing incident assignment.	The Technician can view incident assignment in a separate Web part from within the **Incident Process View** page. The page is located directly beneath the primary contact Web part.

The updates include the enhancements, changes, or deprecations in the features that existed in ServiceDesk 7.0 MR2.

Where to get more information

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

Table 1-4 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.
Implementation Guide	Information about how to install, configure, and implement this product.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. 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 when the page is active. ■ 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 Symantec products.

Table 1-5 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Understanding ServiceDesk concepts

This chapter includes the following topics:

About workflows, processes, tickets, and tasks

ServiceDesk and Workflow Designer let you work with, create, and edit workflows, processes, tickets, and tasks. These items are related to the workflow processing in ServiceDesk.

See "About ServiceDesk" on page 23.

Table 2-1 Descriptions of workflows, processes, tickets, and tasks

Item	Description
Workflow	Consists of the defined steps that a process can follow. A workflow is the design of the possible process events. For example, a workflow can be a purchase order approval or rejection, or a way to manage incidents. Workflows are created in Workflow Designer. You can use Workflow Designer to customize the default workflows and publish them to the production environment. See "About Workflow Designer" on page 40.
Process	The workflow path that is followed to perform a series of actions. The specific path that the process takes depends on the following things: ■ The user's interaction with the process ■ The data that is provided as the process is worked ■ The decisions that the workflow itself makes as a result of the decisions and data ServiceDesk contains predefined, ITIL-compliant processes, which are ready to use. See "About the core processes in ServiceDesk" on page 35.
Ticket	An object that is created to accept the data that is entered during the initiation and working of a process. A ticket also contains the information that the various workers need to work the process. For example, an incident ticket contains the attributes that define the incident, such as the description, contact, and priority.
Task	The action that must be taken to work a ticket or perform some other job. A task is assigned to a group or a specific worker. For example, when a user submits an incident ticket, a task is created and assigned to a support technician or the support group. When the support technician completes that task, the ticket is updated and then it progresses to the next step in the workflow.

About ITIL

ITIL is an acronym for Information Technology Infrastructure Library, which is a method of IT service management that is widely followed in many organizations. ITIL attempts to define a set of best practices for companies to use to manage their IT operations. Companies attempt to manage their IT infrastructure, development, and operations using ITIL concepts and policies.

Organizations that implement ITIL processes seek to improve their operational efficiencies and improve customer and user satisfaction.

Effectively using ITIL processes can help organizations in the following ways:

- Manage user requests quickly.
- Determine the root causes of recurring issues so that they can be addressed, which can eliminate further issues in the future.

See "About the core processes in ServiceDesk" on page 35.

About the core processes in ServiceDesk

ServiceDesk contains predefined, ITIL-compliant processes, which let you manage service tickets and perform other service management activities.

See "About workflows, processes, tickets, and tasks" on page 33.

See "About ITIL" on page 34.

The predefined processes are ready to use. However, you can customize any process to meet the specific needs of your organization. You customize the workflow for a process in Workflow Designer.

See "About Workflow Designer" on page 40.

Table 2-2 Core processes in ServiceDesk

Workflow	Project name	Description
Change Management	SD.Change Management	Works on standardizing methods and procedures for the most efficient handling of all changes. The goal of the standardization is to reduce the effect of changes on the organization. See "About Change Management" on page 179.
Customer Survey	SD.CustomerServiceSurvey	Lets the user who is 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 438.
Incident Management	SD.Incident Management	Aims to address the user's issues and get the user back to their normal working conditions as quickly as possible. See "About Incident Management" on page 105.

Table 2-2 Core processes in ServiceDesk *(continued)*

Workflow	Project name	Description
Knowledge Management	SD.KnowledgeBase Submission	Provides a data repository holding information on incidents, problems, and known errors. Collecting information in the knowledge base enables organizations to match new incidents against previous ones and reuse established solutions and approaches.
Problem Management	SD.Problem Management	Investigates the problems that are the source of multiple incidents. Once problems are found, actions are taken to fix the situation, and possibly prevent it from happening again. See "About Problem Management" on page 208.

Table 2-3 Additional processes in ServiceDesk

Workflow	Project name	Description
Email Monitoring	SD.Email.Monitor SD.Email. InboundManagement	Monitors a specified inbox for all new, unread emails and processes them by creating incidents or routing them to the service manager for evaluation. See "About configuring the email monitoring" on page 443.
Routing	SD.RoutingRules	Routes (assigns) an incident. By default, all emergency and high priority incidents are assigned to the Support II group. All other incidents are assigned to Support I. The Determine Escalation model in this project contains the routing rules that define the criteria for escalating an incident. When an incident meets those criteria, it is escalated automatically. See "About incident routing and escalation" on page 167.
Service Level Agreement (SLA)	SD.DataServices, in the Setup SLA Requirements model.	Default SLA time frames are established based on incident priority. See "About the Service Level Agreement and Operating Level Agreement" on page 375.
Follow the Sun	SD.FollowTheSun	Assigns the incidents based on defined time zones and groups so that an incident can be worked on a 24x7 basis. See "About Follow the Sun routing" on page 378.

About the process ID

The process ID is a unique, alphanumeric value that is generated when a process is first run. Typically, that occurs when a process ticket is created. The process ID is searchable. You can use the process ID to view all the events and items that are associated with that process throughout its life cycle.

The process ID is sometimes referred to as the incident ID.

The process ID consists of several segments.

Table 2-4 Segments of the process ID

Segment	Description
Prefix	Represents the process type. The prefixes that are used in the process ID are as follows: ■ CM: Change Management ■ EM: Email Monitoring ■ IM: Incident Management ■ KB: Knowledge Management ■ PM: Problem Management ■ SDM: Migrated Incidents from Helpdesk Solution
Number	A numerical value that is generated automatically and incremented for each subsequent process of the same type. By default, the number is six digits long. However, you can change its length by editing the pad length in the appropriate process project in Workflow Designer. For example, if you specify a pad length of eight in the SD.Incident Management project, the first incident is numbered IM-00000001. For more information about editing workflow projects, see the *Workflow Solution User Guide*.
Task number	A numerical value that is appended to the process ID when a task is created for a specific process. The number is incremented every time the task is worked. For example, a new incident is assigned process ID IM-000009. The first task that is created for the incident is assigned task ID IM-000009-1. After the support technician works the incident, the next task that is created is assigned task ID IM-000009-2.

About cascading relationships among process tickets

In ServiceDesk, you can associate incidents, problems, and changes, with each other. These relationships are called cascading because when one type of ticket is resolved, a related ticket is closed.

An example of these relationships is as follows:

- When a specific issue is reported frequently, a support technician or other worker can create a problem ticket to fix the root cause. When the problem ticket is reviewed and approved, the problem reviewer creates a change request to initiate the problem correction. When the change is completed and verified, the associated problem ticket and its associated incidents are closed.

The tickets for the core process types can have the following relationships:

Incident and problem	A support technician or a problem analyst can create a ticket to resolve a systemic problem that is the cause of multiple incidents. When the problem ticket is closed, the associated incidents are closed.
Problem and change	When the resolution of a problem requires a fix, the problem reviewer can associate the problem with a change request. When the change is completed and closed, the associated problem is closed.
Incident and change	When the resolution of an incident requires a change, the support technician can associate the incident with a change request. When the change is completed and closed, any associated incidents are closed.

Two types of tickets can have a relationship only if the organization installed the modules for both processes.

See "About the Incident Management process" on page 106.

See "About the Problem Management process" on page 209.

See "About the Change Management process" on page 181.

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.

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

See "About the Configuration Management Database (CMDB)" on page 39.

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.

About 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.

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 38.

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 more information about CMDB Solution, see the *CMDB Solution User Guide*.

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.

For example, you can import Active Directory objects, such as users, computers, sites, and subnets, into the CMDB. This feature lets you leverage the data that already exists in Active Directory without re-creating it. You can schedule regular imports to keep your CMDB populated with up-to-date resources, allowing better management of your environment.

- 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.

About Workflow Designer

Workflow Designer lets an administrator customize workflows to meet the needs of the organization. With Workflow Designer, you can design workflows to apply rules, make decisions, display interfaces, interview users, and route documents.

Workflow Designer is a component of Workflow Solution. ServiceDesk is based on Workflow Solution.

A version of Workflow Designer is included with ServiceDesk.

See "About workflows, processes, tickets, and tasks" on page 33.

The Workflow Designer that is included with ServiceDesk lets you modify the ServiceDesk workflows in any way that you want. However, the ability to create a new workflow or use the data integration components require an Advanced Workflow license.

You can install Workflow Designer at the same time and on the same computer as the ServiceDesk application software. However, Workflow Designer is typically installed on a client computer instead of the ServiceDesk server computer.

About Workflow Server

The Workflow Server software is the server-side software that includes the workflow extensions that are required to run the core workflow processes. These extensions must run on the server to which the workflows have been deployed, which is the ServiceDesk server computer. The ServiceDesk server is sometimes referred to as the Workflow server.

When you customize workflows and other items in Workflow Designer, you must publish them to the Workflow Server. Publishing is the act of moving a project from the test environment to the production environment so that it can be run.

For more information about workflows, publishing, and Workflow Designer, see the *Workflow Solution User Guide*.

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.
  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 primary contact has the process view page open for any of the tickets that they submitted.
- 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.

Introducing ServiceDesk solution software

This chapter includes the following topics:

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 computer and applies the ServiceDesk licenses. The ServiceDesk solution software manages the consumption of the ServiceDesk licenses.
  See "About ServiceDesk licenses" on page 41.

- Downloading of the installation file that is used to install the ServiceDesk server software on the ServiceDesk server computer.
  The ServiceDesk server computer is different from the Symantec Management Platform computer.
  In the **Symantec Management Console**, you can access a page that lets you download the ServiceDesk installation file to the ServiceDesk server computer.
  Additional files might also be available for download.
- Creation of ServiceDesk incidents for the specific resources that are defined in the CMDB (Configuration Management Database).
  See "Creating an incident from the Symantec Management Platform" on page 138.
- Integration between the ServiceDesk application software and the CMDB.
  Web services perform the integration in real time. The web services are generated from a workflow project, SD.DataServices.
  See "About the Configuration Management Database (CMDB)" on page 39.

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 installation files for ServiceDesk.
- View all incidents that are associated with a resource and that have been reported from the ServiceDesk server computer.

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

See "Accessing the ServiceDesk Solution Console page" on page 44.

The ServiceDesk solution software is a component of the ServiceDesk product.

See "About ServiceDesk solution software" on page 43.

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 44.

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 **Service and Asset Management > ServiceDesk** and then click **ServiceDesk**.

Viewing the ServiceDesk incidents that are associated with a resource

The ServiceDesk solution software lets you view all incidents that are associated with a resource and that have been reported from the ServiceDesk server computer.

You can also obtain this information from the **ServiceDesk Solution Console** page.

See "Accessing the ServiceDesk Solution Console page" on page 44.

To view the ServiceDesk incidents that are associated with a resource

1. In the **Symantec Management Console**, on the **Manage** menu, click **Organizational Views and Groups**.
2. In the left pane, expand **Organizational Views**.
3. Under **Organizational Views**, navigate to and click the organizational group that contains the resource.
4. In the right pane, select the resource, and then in the **Actions** drop-down list, click **Show Incidents**.
5. When you finish viewing the information, you can close the report page.

Section 2

Working in the ServiceDesk portal

Chapter 4

Introducing the ServiceDesk portal

This chapter includes the following topics:

About the ServiceDesk portal

The ServiceDesk portal is a Web-based interface that provides access to the ServiceDesk application software. The users of ServiceDesk access the portal from their Web browsers and use it to run the workflow processes and perform other ServiceDesk activities.

Examples of the tasks that users can perform in the ServiceDesk 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 ServiceDesk, the permissions that you have been 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.

See "Logging on to the ServiceDesk portal" on page 51.

Table 4-1 Screen elements of the ServiceDesk portal

Element	Description
ServiceDesk portal	The browser window that appears when you double-click the **Symantec ProcessManager** shortcut.
Site Actions drop-down list	A drop-down list that can appear at the top of the ServiceDesk portal window. It appears only when you have permission to edit the current ServiceDesk portal page.
Link	The clickable text that appears at the upper right and lower left of the ServiceDesk portal window. Examples of links are **Help** and **Logout**.
Tab bar	The horizontal row of tabs that appears near the top of the ServiceDesk 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.

Table 4-1 Screen elements of the ServiceDesk portal *(continued)*

Element	Description
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 ServiceDesk 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. See "Logging on to the ServiceDesk portal" on page 51.
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 in a portal page or in a page that is accessed from a portal page. Portal pages can be customized 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 ServiceDesk portal pages" on page 76.
Section or Web part	The segments that appear on a ServiceDesk 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. See "Adding a Web part to a ServiceDesk portal page" on page 81. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.

Logging on to the ServiceDesk portal

The ServiceDesk portal is a Web-based interface that lets users submit incidents and lets ServiceDesk workers perform their service-related work.

See "About the ServiceDesk portal" on page 50.

During the setup of the ServiceDesk portal, each user is assigned a user name and initial password. We recommend that you change your password after you log on to the portal for the first time.

See "Changing your password" on page 101.

The permissions that you have been granted control all aspects of your use of the ServiceDesk portal. They determine which parts of the ServiceDesk portal you can access and what you can do in each part.

If you cannot see or work in a particular feature, you probably do not have the appropriate permissions. Your ServiceDesk administrator can help you with any permissions issues.

When you log on to the ServiceDesk 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

See "Setting your opening portal page" on page 76.

To log on to the ServiceDesk portal

1. Open your Web browser and in the **Address** bar, type the URL that has been provided for your ServiceDesk portal, as in the following example:

   http://*ServiceDesk/ProcessManager*

2. On the logon page, type your **Email Address or Username** and **Password**.
3. (Optional) Check **Remember Me**.

   This option creates a cookie on your local computer, which automatically logs you on to ServiceDesk. The cookie expires in one year.

4. Click **Login**.

Default ServiceDesk portal pages

See "About the ServiceDesk portal" on page 50.

The ServiceDesk portal contains a series of default portal pages. The role-based permissions that you have been granted determine the portal pages and actions that are available to you. If you cannot access a particular portal page or feature, you probably do not have the appropriate permissions.

You can perform all of the ServiceDesk functions on the default pages, which are ready to use. However, you might want to customize the pages or add new pages to meet your organization's specific requirements.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

If any page was customized, its appearance and contents might differ from the default page. Your ServiceDesk portal might contain pages other than or in addition to the default pages.

Table 4-2 Default ServiceDesk portal pages

Page	Description
Admin pages	Let the administrator configure settings for the ServiceDesk portal. The **Admin** pages are accessed by selecting a menu command from the **Admin** tab in the ServiceDesk portal. See "Commands on the Admin menu" on page 455.
Dashboard	Provides a high-level, graphical view of the number and status of incidents in the organization. Change managers and service managers can use this information to spot trends and potential problems in the resolution of incidents. The reports that appear on this page are actionable, which provides more value than a view of the state of the environment. For example, if a Web part contains a report in the form of a graph, you can click the graph to open a report view. You might also be able to drill down to the items in the report. If a Web part lists tasks, you can open a task and work it. You can also add custom Web parts to start processes, take further action, or help you perform other tasks. See "Dashboard page" on page 56.
Documents **Category View**	Lets you view, download, email, and perform other actions with documents in the document management system. Your permissions determine which documents you can view and what actions you can take with those documents. See "Documents page" on page 59.
Calendar	Lets the change manager plan changes and releases that coordinate with the existing schedule. It also lets users view the scheduled changes that might affect them. See "Calendar page" on page 60.
Home	Serves as the primary workspace for viewing the tickets that you submitted and performing other general ServiceDesk activities. See "Home page" on page 54.
Knowledge Base	Lets you view and manage knowledge base items. You can edit existing items and you can add new items outside of the normal knowledge base process. See "Knowledge Base page" on page 61.
Discussion **Knowledge Base** subpage	Lets you start, view, and participate in discussions. See "Discussions page" on page 58.
My Task List	Lets you view and work on the tasks that are assigned to you. The **My Task List** page is the primary workspace for working on your tasks. See "My Task List page" on page 62.

Table 4-2 Default ServiceDesk portal pages *(continued)*

Page	Description
Reports	Lets you view, create, delete, copy, email, and perform other actions with reports in ServiceDesk. See "Reports page" on page 64.
Submit Request	Lets you submit tickets and perform other self-service actions. For example, a user can submit an incident and a support technician can submit a change request. See "Submit Request page" on page 64.
Tickets **Tickets - Alternate View**	Displays the current tickets. By default, it lists the tickets that are assigned to you but it can also display other tickets. You can work tickets from this page. The alternate view presents a different layout, with the tickets listed on the left and the ticket contents on the page on the right. See "Tickets page" on page 65.
Workflow	The **Workflow** page in the ServiceDesk portal provides administrators and managers with a comprehensive view of the current tasks and processes. The **Workflow** page has the following views: ■ **Workflow Task List** Lists all the tasks that are assigned to you. ■ **Workflow Process List** Lists all the active processes and their associated tickets. The processes are arranged in workflow category order. See "Workflow page" on page 67.

Home page

The **Home** page in the ServiceDesk portal is the primary workspace for viewing the tickets that you submitted and performing other general ServiceDesk activities.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-3 Default sections on the **Home** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Search KB	Lets you search the knowledge base for articles. See "Searching the knowledge base" on page 281.
My Requests	Displays every request that you created along with its ticket number, name, age, percent complete, and status. You can select a ticket number to display the ticket's **Process View** page. See "Process View page" on page 89. Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. See "Options for customizing a ServiceDesk portal page list" on page 85. See "Changing the report for a ServiceDesk portal page list" on page 87.

Admin page

The **Admin** page in the ServiceDesk portal lets you access all the administrative functions that are available in ServiceDesk. Only administrators or other users with the appropriate permissions can access the options on the **Admin** page.

See "Commands on the Admin menu" on page 455.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Dashboard page

The **Dashboard** page in the ServiceDesk portal provides a high-level, graphical view of the number and status of incidents in the organization. Change managers and service managers can use this information to spot trends and potential problems in the resolution of incidents.

You can refine or change the contents of any of the data sections for this viewing session. These changes are lost when you click away from the **Dashboard** page.

See "Options for changing the contents of the dashboard pages" on page 57.

The contents of the **Dashboard** page can be customized permanently to display the information that is most useful to your organization. For example, a section can be edited to display a different report or other sections can be added, deleted, or moved.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-4 Default sections on the **Dashboard** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Search KB	Lets you search the knowledge base for articles. See "Searching the knowledge base" on page 281.
Trend New Incidents	Provides a graphical view of the incidents that have been submitted within a specific date range. The default date range is the current month. You can specify a different date range.
Incidents By Location	Provides a graphical view of the incidents that have been submitted this month in each location.

Table 4-4 Default sections on the **Dashboard** page *(continued)*

Section	Description
Open Incidents By Priority	Displays the number of open incidents for each priority. You can expand each priority group to view the individual incidents, and you can select an incident to open.
Current Open Processes	Displays the number of open process tickets for each priority. You can expand each priority group to view the individual process tickets, and you can select a ticket to open.

Options for changing the contents of the dashboard pages

In the ServiceDesk portal, when you open the **Dashboard** page, you can refine, change, or perform actions on the page contents. Any changes that you make are lost when you click away from the page.

On the dashboard page, within each data section (Web part), you can perform the following actions:

- Edit the **Report Settings** to change the date range, number of records, or other criteria.
- Select a different report to display.
- Search for text in the report data.
- Perform an action on the entire group of incidents.
  For example, you can add a comment to all the incidents that are displayed.
  See "Performing actions on multiple tickets" on page 232.
- Refresh the contents of a section.
- Generate a preview of the section's data in a new window, from which you can print or save the data.
- Export the section's data to an Excel worksheet.
- Export the data to a CSV (comma-separated values) file that you can import into another program.
- Subscribe to the data as an RSS feed.

Some of the sections do not contain all of these options or actions.

The contents of the dashboard page can be customized permanently to display the information that is most useful to your organization. For example, a Web part can be edited to display a different report or other Web parts can be added, deleted, or moved.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

ServiceDesk contains an extensive catalog of Web parts that you can add to the dashboard pages. You can view the available Web parts when you click **Admin > Portal > Web Parts** in the ServiceDesk portal.

Discussions page

The **Discussions** page in the ServiceDesk portal lets you start, view, and participate in discussions. The **Discussions** page displays the discussions that you have permission to view, and lets you expand the discussion posts.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-5 Default options on the **Discussions** page

Option	Description
 **Actions**	Opens a drop-down list of options that let you edit or delete the selected discussion item. The option to delete is not available if the item has one or more posts or responses.
	The location of this symbol determines its action as follows: ■ **Add Discussion** ■ **Add Thread** ■ **Add Post**
 **Delete**	Appears on the **Actions** drop-down list and lets you delete the selected discussion item. This option is not available if the item has one or more posts or responses. However, you can still delete the thread or the main discussion. First, you must delete the lowest level of the discussion, and then work backwards to the highest level. By deleting this information, you also delete the posting history.
	The location of this symbol determines its action as follows: ■ **Edit Discussion Info** ■ **Edit Thread Info** ■ **Edit Thread Item**

Table 4-5 Default options on the **Discussions** page *(continued)*

Option	Description
Search	Lets you type the search text. The search results display any discussions whose posts contains the search text.
Show Discussions Rated	Lets you filter the list of discussions that appears. The users who read the discussion posts can provide the ratings.
 **Reply**	Opens the **Reply** dialog box, where you can type and save a reply to the selected discussion item.

Documents page

The **Documents** page in the ServiceDesk portal lets you view, download, email, and perform other actions with documents in the Document Management system. Your permissions determine which documents you can view and what actions you can take with those documents. For example, you might have permissions to view certain documents, but not to delete or edit the document data for those documents.

Any documents that are added to incidents, changes, problems, and releases are automatically saved in the Document Management system. They are saved to hidden folders, which the administrator can access. They are organized in process order and then in ID order.

If your page was customized, its appearance and contents might differ from the default page.

See “About customizing the contents of ServiceDesk portal pages” on page 76.

Table 4-6 Default sections on the **Documents** page

Section	Description
Bulletin Board	Lets you view the scrolling Bulletin Board messages. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, or organizations. See “About the Bulletin Board” on page 251.

Table 4-6 Default sections on the **Documents** page *(continued)*

Section	Description
Search Documents	Lets you search the Document Management system for documents. This search is conducted on the document name only. See "Searching for documents" on page 309.
Browse	Lets you select the category for which to display the documents. You can display folders for the categories that are designated as hidden by checking **Show hidden folders**. You can also create a new document category. See "Adding a document category" on page 290.
Advanced Search	Lets you perform a more advanced search in the Document Management system by specifying different areas to search. This search is conducted on keywords.
Service Catalog	Lets you view and use the services in the Service Catalog that you have permission for. The service items are categorized in folders. When you select a folder, the service items in that category appear at the right of the portal page. You can click the service item name to perform the action. You can hide the description that appears under each service item by checking the **Hide Description** check box in this section.
Documents	Displays the documents that are in the category that you selected under **Browse**. Your permissions determine the documents that appear. You can open and view a document and perform several actions on the document. See "Viewing a document" on page 310. See "What you can do with ServiceDesk documents" on page 307.

Calendar page

The **Calendar** page in the ServiceDesk portal lets managers plan changes and releases that coordinate with the existing schedule.

By considering the entire schedule, the managers can avoid unforeseen schedule conflicts. It also lets users view the scheduled changes that might affect them.

See "About scheduling in ServiceDesk" on page 241.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-7 Default sections on the **Calendar** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the message can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public, or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Schedules	Lists the all the schedules that have been defined. You can add, edit, and delete schedules, and you can select the schedules that appear on the **Schedule Entries** calendar. See "Creating a new schedule" on page 244.
Search Entry	Lets you perform a text search for a schedule entry. See "Searching for a schedule entry" on page 243.
Service Catalog	Links to the Service Catalog items. See "About the Service Catalog and service items" on page 382.
Schedule Entries	Displays the calendar. The monthly view is the default. This section also displays the results of a schedule entry search.

See "Viewing the ServiceDesk schedule" on page 242.

Knowledge Base page

The **Knowledge Base** page in the ServiceDesk portal lets you view and manage knowledge base items. You can edit existing items and you can add new items outside the normal knowledge base process.

The **Knowledge Base** page appears by default when you click the **Knowledge Base** tab.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-8 Default sections on the **Knowledge Base** page

Section	Description
Bulletin Board	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the message can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public, or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Search Articles	Lets you search for knowledge base items. The body text of the items is searched for the search text that you enter.
Article Category List	Lets you select the category for which to display knowledge base items. You can include the items that are designated as obsolete by checking **Show Obsolete Articles**. You can also create a new knowledge base category. See "Adding a knowledge base category or subcategory" on page 268.
Service Catalog	Lets you view and use the services in the Service Catalog that you have permission for. The service entries are categorized in folders. When you select a folder, the service entries in that category appear at the right of the portal page. You can click the service item name to perform the action. You can hide the description that appears under each service item by checking the **Hide Description** check box in this section.
All Articles	Displays the articles that are in the category that you selected under **Categories**. Your permissions determine the articles that appear and what you can do with them. See "What you can do with a knowledge base item" on page 282.

My Task List page

The **My Task List** page in the ServiceDesk portal lets you view and work on the tasks that are assigned to you. The **My Task List** page is the primary workspace for working on your tasks.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-9 Default sections on the **My Task List** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Recent Items	Displays the items that you recently viewed, opened, or worked on. You can select a recent item to open it. By default, the last 10 items are displayed. If you want to change the number of items, click **Max Recent Items Count**. You can bookmark an item that is important to you. If you click the star symbol next to an item, that item is locked to the list even if 10 newer items exist.
Find Task	Lets you find a task by specifying its task number. You can view only the tasks for which you have the appropriate permissions.
Find Ticket	Lets you find a ticket by specifying its Process ID. You can view only the tasks for which you have the appropriate permissions.
Tasks Viewer	Displays the tasks that are assigned to you. You can select a task number to display the task's **Process View** page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with. See "Process View page" on page 89. Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. See "Customizing a ServiceDesk portal page list" on page 84. See "Changing the report for a ServiceDesk portal page list" on page 87.

Reports page

The **Reports** page in the ServiceDesk portal lets you view, create, delete, copy, email, and perform other actions with reports in ServiceDesk. Your permissions determine which reports you can view, and what actions you can take with those reports. For example, you might have permission to view certain reports, but not to delete those reports or edit the report definitions.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-10 Default sections on the **Reports** page

Section	Description
Report Search	Lets you search for a specific report. This search is conducted on the report name and the results are shown from all categories.
Report Categories	Lets you select the category for which to display the reports. You can also import a report category to the list from another ServiceDesk instance, and you can add a new report category. See "Adding report categories" on page 342.
Report Templates	Lets you create a new report from a predefined template. You can also edit, export, and delete a report template.
Reports	Displays the reports that are in the category that you selected under **Report Categories**. Your permissions determine the reports that appear. You can select a report to view or select any of several report actions. For example, you can edit, print, and export a report. You can also add a new report.

Submit Request page

The **Submit Request** page in the ServiceDesk portal lets you submit tickets and perform other self-service actions. The service items that are available depend on your permissions. For example, a user can submit an incident and a support technician can submit a change request.

A service item is a repeatable self-service action that performs a common task. The default service items represent common ServiceDesk actions. For example, the actions to submit an incident or to submit a request for a knowledge base article are default service items.

Your organization can create custom service items. For example, you might use a service item to request new equipment or to perform a self-service fix for an incident that you submitted.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-11 Default sections on the **Submit Request** page

Section	Description
Search Service Item	Lets you search for a specific service item by **Title** or **Description**. This search feature is useful when you do not know which folder contains the service item that you need.
Service Catalog	Lets you view and use the services in the Service Catalog that you have permission for. The service items are categorized in folders. See "About the Service Catalog and service items" on page 382. When you select a folder, the service items in that category appear at the right of the portal page. You can click the service item name to perform the action. You can hide the description that appears under each service item by checking the **Hide Description** check box in this section.
New Request (right side)	Displays the service items for the folder that you selected under **Service Catalog**. The service items that are available depend on your permissions.

Tickets page

The **Tickets** page in the ServiceDesk portal displays the current tickets. By default, it lists the tickets that are assigned to you but it can also display other tickets. For example, a support manager might view the **Tickets** page to monitor the progress of all open tickets. As a convenience, the **Start New Ticket** section lets you create a ticket from the **Tickets** page instead of requiring you to go to another page. Also, the **My Queues** section lets you work your own tasks from the **Tickets** page.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-12 Default sections on the **Tickets** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Recent Items	Displays the items that you recently viewed, opened, or worked on. You can select a recent item to open it. By default, the last 10 items are displayed. If you want to change the number of items, click **Max Recent Items Count**. You can bookmark an item that is important to you. If you click the star symbol next to an item, that item is locked to the list even if 10 newer items exist.
My Queues	Displays your tasks by user group and priority. You can sort the tasks by task number or priority, and you can search the tasks for specific text. You can select a task number to display the task's **Process View** page.
Changes This Week	Displays the changes that are scheduled to occur this week.
Find Ticket	Lets you find a ticket by specifying its process ID.
Start New Ticket	Lets you create a new ticket. The types of tickets or other service items that you can create depend on your permissions.

Table 4-12 Default sections on the **Tickets** page *(continued)*

Section	Description
My Open Tickets	Initially displays the open tickets that are assigned to you. You can select a ticket number to display the ticket's **Process View** page. If you have tickets in multiple processes, you must expand the appropriate process heading for the ticket that you want to work with. See "Process View page" on page 89. Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The type of ticket and your permissions determine the options that are available. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. See "Customizing a ServiceDesk portal page list" on page 84. See "Changing the report for a ServiceDesk portal page list" on page 87. The **Select a group action** drop-down list lets you perform certain actions on multiple tickets. See "Performing actions on multiple tickets" on page 232.

Workflow page

The **Workflow** page in the ServiceDesk portal provides administrators and managers with a comprehensive view of the current tasks and processes.

The **Workflow** page has the following views:

- **Workflow Task List**
  Lists all the tasks that are assigned to you.
- **Workflow Process List**
  Lists all the active processes and their associated tickets. The processes are arranged in workflow category order.

If your page was customized, its appearance and contents might differ from the default page.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Table 4-13 Default sections on the **Workflow** page

Section	Description
Bulletin Board This section is not labeled.	Lets you view the scrolling Bulletin Board messages that have been posted. For example, the messages can advertise current issues, announce outages, or provide information about a change that is planned to take place within the organization. You can stop the scrolling if you prefer. Bulletin Board messages can be made public or they can be restricted to specific users, groups, permissions, or organizational units. See "About the Bulletin Board" on page 251.
Open Task	Lets you open a specific task by specifying its **Task ID**.
Open Process	Lets you open a specific process by specifying its **Process ID**.
Service Catalog	Lets you view and use the services in the Service Catalog that you have permission for. The service items are categorized in folders. See "About the Service Catalog and service items" on page 382. When you select a folder, the service items in that category appear at the right of the portal page. You can click the service item name to perform the action.
Tasks Viewer	(**Workflow Task List** only) Displays the tasks that are assigned to you. You can select a task number to display the task's **Process View** page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with. See "Process View page" on page 89. Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. See "Customizing a ServiceDesk portal page list" on page 84. See "Changing the report for a ServiceDesk portal page list" on page 87.

Table 4-13 Default sections on the **Workflow** page *(continued)*

Section	Description
Process Viewer	(**Workflow Process List** only) Displays all the processes that are currently running. You can select a task number to display the task's **Process View** page. If you have tasks in multiple processes, you must expand the appropriate process heading for the task that you want to work with. See "Process View page" on page 89. Initially, the page displays the default report. If you select a different report to view, the contents of the list changes. You can print or export the report, search for data within the report, or select a different report. If the **Report Settings** option appears, you can click it to change the appearance or contents of the report. The options that are available depend on the type of ticket and your permissions. For example, you might be able to limit the number of records that appear, filter the display, or enter additional parameters for the report. See "Customizing a ServiceDesk portal page list" on page 84. See "Changing the report for a ServiceDesk portal page list" on page 87.

Managing portal pages

This chapter includes the following topics:

Exporting a ServiceDesk portal page

You can export the definition for a ServiceDesk portal page to a file in AXD, XML, or XSL format. No actual data is exported. The exported file can be imported to create a new page in the ServiceDesk portal.

For example, you might export a customized portal page so that it can be imported into other ServiceDesk installations within your organization. You might also share a portal page with a business partner or other company that uses ServiceDesk.

See "Importing a ServiceDesk portal page" on page 72.

To export a ServiceDesk portal page

1. In the ServiceDesk portal, click **Admin > Portal > Manage Pages**.
2. In the **Pages List** section, select the page to export.
3. In the **Page** section, click **Export Page**.
4. Click **Save**.
5. In the **Save As** dialog box, specify the save location, file name, and file format, and then click **Save**.
6. In the **Download complete** dialog box, click **Close**.

Importing a ServiceDesk portal page

You can import a ServiceDesk portal page to replace an existing page that has the same page ID or create a new page. For example, you can import a customized page into other ServiceDesk installations within your organization without having to redo the customization in each installation. The exported file must be in AXD, XML, or XSL format.

See "Exporting a ServiceDesk portal page" on page 71.

The new page contains the same layout, settings, and permissions as the original page. After you import the page, you can move it to the appropriate sequence in the page order.

See "Rearranging the sequence of ServiceDesk portal pages" on page 72.

To import a ServiceDesk portal page

1. In the ServiceDesk portal, click **Admin > Portal > Manage Pages**.
2. At the upper right of the **Pages List** section, click the **Import Page** symbol (white page with a green plus sign).
3. In the **Import Page** dialog box, in **Select File**, specify the file to import.
4. If the page that you import has the same page ID as an existing page in your ServiceDesk portal, select one of the following options:
   - **Overwrite existing page**
   - **Create new copy**
     The new page has the same name as the existing page with the same page ID.
5. Click **Import**.
6. In the **Import Page** dialog box, import another page or close the dialog box.
7. (Optional) Move the new page to the appropriate place in the page sequence. If the new page does not appear in the correct place

   See "Rearranging the sequence of ServiceDesk portal pages" on page 72.

Rearranging the sequence of ServiceDesk portal pages

You can organize the tab bar or menu bar of the ServiceDesk portal by changing the sequence of the portal pages that appear there. You can rearrange the existing portal pages and the pages that you create. You can also change subpages to root pages and root pages to subpages.

See "About the ServiceDesk portal" on page 50.

Caution: A subpage's permission settings must be the same as or more restrictive than the root page's permission settings. Because a subpage does not inherit the permissions of its root page, you must set the permissions for the subpage separately.

To rearrange the sequence of ServiceDesk portal pages

1. In the ServiceDesk portal, click **Admin > Portal > Manage Pages**.
2. In the **Pages List** section, select the page to move.
3. Under the **Page** section, select any of the following options:
   - **Move Up**
   - **Move Down**
   - **Move Level Up**
     Moves a subpage up to the next level.
   - **Make as Sub Page**
     Displays a list of the existing pages, from which you select the root page to place the subpage under.
4. Continue to move the page until it is in the correct position.
5. Move additional pages if needed.

Deleting ServiceDesk portal pages

ServiceDesk portal pages can be deleted. For example, you might delete a default page that does not apply to your organization or a page that is no longer used. When a portal page is deleted, any users who have the page open are not able to save any information on that page. Also, no one can access the page from that point forward.

An alternative to deleting a page is to disable it. That way, you can revert to using that page at any time by enabling it.

To delete a ServiceDesk portal page

1. In the ServiceDesk portal, click **Admin > Portal > Manage Pages**.
2. In the **Pages List** section, select the page to delete.
3. Click **Delete Page**.
4. In the confirmation dialog box, click **OK**.

Chapter 6

Customizing the contents of ServiceDesk portal pages

This chapter includes the following topics:

About customizing the contents of ServiceDesk portal pages

The ServiceDesk portal consists of pages, from which all ServiceDesk activities are performed. The portal pages can be customized to meet your organization's 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.

See "Enabling the customization of a ServiceDesk portal page" on page 77.

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

See "Customizing a ServiceDesk portal page (administrator)" on page 78.

See "Customizing your ServiceDesk portal pages (non-administrator)" on page 78.

You can also set a portal page to be the page that opens whenever you log on to the ServiceDesk portal.

See "Setting your opening portal page" on page 76.

Setting your opening portal page

Whenever you log on to the ServiceDesk portal, the portal opens to a specific page.

See "Logging on to the ServiceDesk portal" on page 51.

Initially, your permissions determine which page opens. However, you can set a different page to open when you log on. This page does not necessarily have to be the one that is labeled the **Home** page.

To set your opening page

1. In the ServiceDesk portal, open the page to make your home page.
2. At the bottom of the portal window, click **Make Home Page**.

Enabling the customization of a ServiceDesk portal page

See "About customizing the contents of ServiceDesk portal pages" on page 76.

Before anyone can customize a ServiceDesk portal page, the administrator must enable that page for customization. Enabling a page for customization consists of setting the appropriate privileges and permissions.

Table 6-1 Process for enabling the customization of a ServiceDesk portal page

Step	Action	Description
Step 1	Set customization privileges for a user or group.	The privilege setting for groups is **Portal.PersonalCustomization**. The privilege setting for users is **PersonalCustomization**, which is under the **Portal** category.
Step 2	Set customization permissions on the page.	For each page, set permissions for adding, editing, or deleting the page. On the **Admin** tab, under **Portal > Manage Pages**, you can edit the page to enable it for customization as follows: ■ The **Allow User Personalization** setting enables the **Modify My Page** option on the portal page. That option lets a user edit their own page without affecting that page for other users. ■ The page's **Permissions** settings let you allow users, groups, permissions, or organizational units to view, edit, or delete the page.

Customizing a ServiceDesk portal page (administrator)

By default, the administrator can customize any portal page that is able to be customized.

See "About customizing the contents of ServiceDesk portal pages" on page 76.

To customize a ServiceDesk portal page

1. In the ServiceDesk portal, go to the page to customize.
2. In the upper right of the page, in the **Site Actions** drop-down list, select an action to perform.

   See "Options on the Site Actions drop-down list" on page 79.
3. When you finish the customization, you can close the page.

Customizing your ServiceDesk portal pages (non-administrator)

You can customize any of your portal pages if you have permission to do so. The pages that you are most likely to customize are the **Task List** page and the **Home** page. For example, you might want to place a schedule on your **Home** page.

Before anyone can customize a ServiceDesk portal page, the administrator must enable that page for customization.

To customize a ServiceDesk portal page

1. In the ServiceDesk portal, go to the page to customize.
2. In the upper right of the page, in the **Site Actions** drop-down list, select one of the following options:

Modify Page	Lets you add, edit, and delete the Web parts that are on the page.
Modify My Page	The **Modify Page** option changes the page for everyone who has access to it. The **Modify My Page** option changes your version of the page only. See "Adding a Web part to a ServiceDesk portal page" on page 81. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.
Reset to Default	Discards any changes that you made to the portal page and reverts it to its original configuration. This option only appears if you select **Modify My Page** to modify the portal page. Note that if you select **Modify Page**, the option to **Reset to Default** does not appear, which means any changes that you make cannot be undone.
Share Page	Lets you specify a user, group, permission, or organizational unit can view your customized version of the portal page. See "Sharing a ServiceDesk portal page" on page 83.

   This drop-down list appears only on the pages that you have the permission to customize. The options that are available depend on your permissions.

   See "Options on the Site Actions drop-down list" on page 79.

3. When you finish the customization, you can close the page.

Options on the Site Actions drop-down list

The Site Actions drop-down list contains the options that are available for customizing a ServiceDesk portal page. This drop-down list appears only on the pages that you have the permission to customize. The options that are available depend on your permissions.

The options that are available also depend on where you are in the editing process. For example, when you are on a main portal page, the **Edit Page** option does not appear in the **Site Actions** drop-down list. However, after you click **Site Actions > Modify Page** and the page opens for editing, the **Edit Page** option becomes available.

Table 6-2 Options on the **Site Actions** drop-down list

Option	Description
Add Root Page	Lets you add a new portal page, which is visible from the top level of the ServiceDesk portal. The page name appears on the tab bar in the upper area of the ServiceDesk portal. Typically, only administrators have permission to create new pages.
Add Sub Page	Lets you add a new subpage, which is one or more levels under a root page. A subpage can appear on the menu of a root page. For example, the **Knowledge Base** page is a root page. You open it by clicking the **Knowledge Base** tab in the ServiceDesk portal. The **Discussions** page is a subpage. You open it by clicking the **Discussions** command on the **Knowledge Base** tab. Typically, only administrators have permission to create new pages.
Add Web Part	Lets you add one or more Web parts to the page. The sections on a ServiceDesk portal page are in the form of Web parts. See "Adding a Web part to a ServiceDesk portal page" on page 81.
Browse	Exits the editing mode and displays the page with the changes that you made.
Clear	Deletes all the Web parts from a portal page. **Warning:** This action cannot be undone. Use caution when you select this option because you are not prompted to confirm this action before the deletion occurs.
Edit Definition	Opens the Edit Page, which lets you configure customization settings and customization privileges for the current portal page. When you select **Save Page** or **Cancel**, it takes you to the **Manage Pages** page. This page also lets you customize privileges and configure settings for the portal page that you select in the **Pages List** pane. Typically, only administrators have permission to edit page definitions. See "Enabling the customization of a ServiceDesk portal page" on page 77.
Edit Page	Lets you edit and delete the Web parts that are on the page. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.
Modify Page	Lets you add, edit, and delete the Web parts that are on the page. The page is changed for everyone who has access to it.
Modify My Page	Lets you add, edit, and delete the Web parts that are on the page. Only your page is changed. This option appears only if the page is configured to allow it.
Page List	(Administrator only) Displays the **Pages List** page that lets you configure settings and customization permissions for any portal page.

Table 6-2 Options on the **Site Actions** drop-down list *(continued)*

Option	Description
Reset to Default	Discards any changes that were made to the portal page and reverts it to its original configuration. Portal page changes can be reverted as follows: ■ A user can discard the changes that they made with the **Modify My Page** option. ■ A user can discard the changes that someone else made with the **Modify My Page** and **Share Page** options. ■ A user cannot discard the changes that someone else made with the **Modify Page** option. However, assuming that the user has the permission to do so, they can delete the individual web parts that someone else added.
Share Page	Lets you specify a user, group, permission, or organizational unit that can view your customized version of a portal page. For example, the support manager can customize the **Task List** page and then share it with members of the Support 1 group. You can also provide additional permissions for this page as follows: ■ Let others edit this page. ■ Provide view, edit, and delete permissions to a specific user, group, permission, or organizational unit. For example, the administrator customizes a page, lets all users in a group view the page, and then lets a specific user edit the page.

Adding a Web part to a ServiceDesk portal page

The sections on a ServiceDesk portal page are in the form of Web parts. You can customize a portal page by adding one or more Web parts.

After you add a Web part, you can edit its properties.

See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.

To add a Web part to a portal page

1 In the ServiceDesk portal, access the page to customize.

2 In the upper right of the page, in the **Site Actions** drop-down list, select one of the following options:

Modify Page	Changes the page for everyone who has access to it.
Modify My Page	Changes your version of the page only.

3. After the page refreshes, in the **Site Actions** drop-down list, click **Add Web Part**.
4. In the **Catalog Zone** pop-up, select the catalog that contains the Web part to add.
5. In the **Catalog Zone** pop-up, under **Profiles**, select the check box for each Web part to add.
6. In the **Catalog Zone** pop-up, in the **Add to** drop-down list, select the page zone to add the Web part to.

   The zones that are available depend on the page's **Template Page** setting, which the administrator sets.
7. Click **Add**.
8. (Optional) To add another Web part, repeat from step 4.
9. When you finish adding Web parts, in the **Catalog Zone** pop-up, click **Close**.

Editing or deleting a Web part on a ServiceDesk portal page

The sections on a ServiceDesk portal page are in the form of Web parts. You can customize a portal page by editing or deleting one or more Web parts.

To edit a Web part on a portal page

1. In the ServiceDesk portal, access the page to customize.
2. In the upper right of the page, in the **Site Actions** drop-down list, select one of the following options:

Modify Page	Changes the page for everyone who has access to it.
Modify My Page	Changes your version of the page only.

3. In the upper right of the Web part to edit, click the **Verbs** symbol (orange lightning), and then select one of the following options:

Edit	Lets you edit the properties of the Web part.
Delete	Lets you delete the Web part.

4 If you clicked **Edit**, in the **Editor Zone**, edit the properties of the Web part, and then select one of the following options:

Apply	Saves the changes without closing the **Editor Zone**.
OK	Saves the changes and closes the **Editor Zone**. Select this option when you finish editing the properties for the current Web part.

5 (Optional) To edit or delete another Web part, repeat from step 3.

6 When you finish editing the Web parts, you can close the page or continue to edit it.

Sharing a ServiceDesk portal page

You can share your version of a ServiceDesk portal page with others to let them see any customizations that are on your page. Typically, you share the pages that you or someone else has customized.

You can share pages by providing the view, edit, and delete permissions to specific users, groups, permission, or organizational unit. For example, the administrator can customize a page and let all users in a certain group view the page. Then the administrator can let only one specific user within that group edit the page.

The users' portal permissions override any share permissions that you might provide. For example, a user who does not normally have permission to view the **Tickets** page cannot view a shared version of that page.

To share a ServiceDesk portal page

1 In the ServiceDesk portal, access the page to share.

2 (Optional) Customize the page.

See "Customizing a ServiceDesk portal page (administrator)" on page 78.

See "Customizing your ServiceDesk portal pages (non-administrator)" on page 78.

3 In the upper right of the page, in the **Site Actions** drop-down list, click **Share Page**.

4 Under **Page Permissions**, review the users, groups, or other entities that have permissions for this page.

5 Under **Share Page**, select an option in each of the following subsections:

Share With	Select the type of entity to give permissions for sharing this page.
Sharing Type	Select the type of share permissions to give. The **Custom (Advanced)** option provides additional ways to customize the permissions.

6 Under **Share Page**, click **Next**.

7 Specify the user, group, or other entity to share this page with, and then click **Share Page**.

8 When you are returned to the page, you can continue to edit it or close it.

Customizing a ServiceDesk portal page list

Several ServiceDesk portal pages contain the lists that you use to analyze or perform ServiceDesk activities. You can customize the lists that appear on your pages so that they display the information in the manner that is most useful to you. For example, on the **My Task List** page, you might want to change the task list so that it displays only your overdue tasks.

Examples of portal page lists are as follows:

- The task list that appears in the **Task Viewer** section on the **My Task List** page
  See "My Task List page" on page 62.
- The request list that appears in the **My Requests** section on the **Home** page
  See "Home page" on page 54.
- The tickets that appear in the **My Open Tickets** section on the **Tickets** page
  See "Tickets page" on page 65.

The primary way to customize a portal page list is to change the report that determines the contents of the list. You can also sort and filter the list to display a more specific subset of information. The changes that you make are active for the current session only. When you log off of ServiceDesk, the changes are lost. However, you can set a new default report that persists beyond a single session.

See "Changing the report for a ServiceDesk portal page list" on page 87.

To customize a ServiceDesk portal page list

1 In the ServiceDesk portal, click the tab that contains the list to edit.

2 On the page, under the list section, you can customize the list in the following ways:

- Sort the columns.
- Search and filter the list.
- Limit the number of records that appear.
- Select a new report.
- Set a new default report.
- Refresh the report.

See "Options for customizing a ServiceDesk portal page list" on page 85.

3 When you finish customizing the list, you can close the page or work on it.

Options for customizing a ServiceDesk portal page list

You can customize a portal page list so that it displays information in the manner that is most useful to you.

Examples of portal page lists are as follows:

- The task list that appears in the **Task Viewer** section on the **My Task List** page
  See "My Task List page" on page 62.
- The request list that appears in the **My Requests** section on the **Home** page
  See "Home page" on page 54.
- The tickets that appear in the **My Open Tickets** section on the **Tickets** page
  See "Tickets page" on page 65.

Table 6-3 Options for customizing a ServiceDesk portal page list

Option	Description
Sort the columns.	You can click any column heading to sort by that heading.

Table 6-3 Options for customizing a ServiceDesk portal page list *(continued)*

Option	Description
Search symbol 	You can search the list to filter the results. For example, to list only those items that have to do with printers, you can search for "printer". You can filter a list by using either of the following options: ■ The **Search** symbol. You can click the **Search** symbol to open a search box. ■ The search feature under **Report Settings**. You can expand the **Report Settings** section and click **Text contains** to open a search dialog box. You might not see the **Support Settings** section because it appears for certain reports only.
Limit the number of records that appear. **Report Settings**	Lets you change the number of records that appear in the list. Typically, the list contains the first 50 records that match the report criteria. You can change the number of records that appear by expanding the **Report Settings** section, clicking the **Return 50 first records** link, and specifying a new number. You might not see the **Support Settings** section because it appears for certain reports only. Other options might appear depending on the type of ticket.
Change Report symbol 	You can select a new report to display the list in a different configuration. For example, you select a report that displays all your open tasks. You can select a new report. Click the **Change Report** symbol. A list of folders opens, which contains the reports that are available. See "Changing the report for a ServiceDesk portal page list" on page 87.
(Set as default)	Lets you set the Current report as the default for this page. See "Changing the report for a ServiceDesk portal page list" on page 87.
Actions symbol 	Lets you output the report in the following ways: ■ **Print Preview** ■ **Export to Excel** ■ **Export to CSV** ■ **RSS**
Refresh symbol 	Lets you refresh the display after you select a new report.

Changing the report for a ServiceDesk portal page list

Each list on a ServiceDesk portal page is associated with a default report that determines the contents of the list. You can change the report to display the list in a different configuration. For example, you can select a report that displays all your open tasks.

When you change the report for a list, it is active for the current session only. The next time that you log on, the default report reappears.

You can also set a new default report that persists beyond a single session. You can select a predefined report or a customized report.

Setting the default report for a list does not save any additional filtering of the list.

To change the default report for a ServiceDesk portal page list

1. In the ServiceDesk portal, click the tab that contains the list to edit.
2. On the page, under the list section, click the **Change Report** symbol.
3. Select the report group, and then select the report to use.

   To quickly find a report, you can type search text in the box and click **Find**.
4. (Optional) To make the new report selection the default report, in the list section, click the **Actions** symbol (orange lightning), and then click **Set default report**.
5. When you finish customizing the list, you can close the page or work on it.

Chapter 7

Working in the Process View

This chapter includes the following topics:

Process View page

A **Process View** page is the primary interface for working a ticket. Each type of ticket has its own **Process View** page. The **Process View** page appears when you open a ticket.

The **Process View** page consists of multiple sections (Web parts) that display general information about the ticket and provide the actions that you can perform. The default **Process View** page layout is similar for all tickets. The actions that are available depend on the type of ticket and your permissions.

The types of tickets that have a default **Process View** page are as follows:

- Incident
- Change request
- Problem
- Release

If your organization uses customized **Process View** pages, you might see sections other than those that are listed here.

Table 7-1 Default sections on the **Process View** page

<table>
<tr><th>Section</th><th>Description</th></tr>
<tr><td>Top section (unlabeled)</td><td>Provides a quick view of the task’s identifying details and statistics.
This section also contains the following action links:
Refresh
Add Comment
Opens the Add Comment to Process dialog box.
Edit Process
Opens the Edit Process dialog box, which lets you edit some of the process details that appear in the top section.</td></tr>
<tr><td>Switch View</td><td>Lets you switch between the Full Process View and the Basic Process View.
The Full Process View is the default view. The Basic Process View is a simplified view that eliminates many of the options that normally appear. This view is useful for reviewing the process tickets that have extensive history.</td></tr>
<tr><td>Additional Data</td><td>Lists the additional statistics for the ticket. The information that appears depends on the type of ticket. For example, in an incident, this section can contain any classification information that a support technician entered.</td></tr>
<tr><td>All Contacts</td><td>Displays the users who are associated with the ticket or who work on the ticket. These users can be anyone who works on the ticket as well as anyone who is added at any phase of the process.
For example, the contacts for an incident are the primary contact and the submitter, if the submitter is different from the primary contact. The contacts for a change request are the primary contact, change manager, planners, implementers, testers, and others who are assigned to participate in the process.
You can view details about the contact or add a new contact if you have permission to do so.</td></tr>
<tr><td>Chat</td><td>Lets you initiate an instant messenger-type conversation with a process contact or other worker. The chat function provides a real-time setting in which to perform troubleshooting.
Chat history is added to the ticket, and you can specify whether you want to hide the chat from certain users or groups.
See “About chatting in the ServiceDesk portal” on page 323.</td></tr>
<tr><td>Description</td><td>(Read only) Displays the description that was entered during the task’s initial creation.</td></tr>
<tr><td>Documents</td><td>Displays any documents that are attached to the process or task and lets you attach additional documents.</td></tr>
</table>

Table 7-1 Default sections on the **Process View** page *(continued)*

Section	Description
History	Displays a record for each action that has occurred within the process. For example, a record can represent a status change, a task, or a user comment. Within the **History** section, you can view information about each record.
My Actions	Lists the actions that you can take to effectively work the ticket. The actions that appear depend on the type of ticket you open. For example, when a support technician opens an incident, the available actions include resolving the incident, escalating the incident, and suggesting a self service resolution. Some actions are common to all tickets. For example, most types of tickets let you send an email or search the knowledge base.
Others Actions	Lets you take an action that is assigned to someone else. For example, if the assigned support technician does not address an incident in a timely manner, the support manager can work on the ticket. If you open a ticket and the actions to work on the ticket are not listed under **My Actions**, you can expand **Others Actions**. If the check box to **Work Tasks Assigned To Others** appears there, you can check it and work the ticket.
Permissions	Lists the workers and groups who have permission to participate in the process and what they can do. You can edit or delete an existing permission, and you can add new permissions. Permissions are not checked when you make changes here. However, if the people who you enter do not have the appropriate permissions, they cannot participate in the process regardless of what you enter. This section does not appear in an incident.
Primary Contacts	Displays the primary contact for the ticket. Typically, the primary contact is the person who submits the ticket. For example, the user who creates an incident is the primary contact for that incident. If a support technician creates a change request from that incident, the support technician is the primary contact for that change request. In some processes, the primary contact can be someone other than the submitter. For example, if a support technician creates an incident on behalf of a user, the user is the primary contact for that incident. You can click the user's name to display the **User Browser** window, which displays information about the user.

Table 7-1 Default sections on the **Process View** page *(continued)*

Section	Description
Process Time	Displays the amount of time that has been recorded for a process ticket to date and lets you post additional time. The **Process Time** appears in incident tickets and problem tickets. ServiceDesk tracks the following times: ■ **Current User Process Time** The amount of time that accumulates for the worker who has the incident's **Process View** page open. ■ **User Process Time** The total amount of offline time that the workers have posted to the incident to date. ■ **Total Process Time** The amount of time that was spent on the incident to date, including the time that was recorded automatically and the time that workers posted. See "About the process time for tickets" on page 231.
Related processes	Lists any other tickets that can be associated with the current ticket. For example, in a change request, this section might list any additional incidents that require the same change.

About actions in ServiceDesk

Actions are the links that are shown on the right side of **Process View** pages. These links let you take actions or launch other processes that can help you with your task or process. The actions on the **Process View** pages save time and can improve the turnaround of tasks in ServiceDesk.

For example, when a technician views an incident, many steps may need to be taken to resolve it. The technician may want to start a chat with the submitter, or search the knowledge base for help on resolving the incident. Actions provide a quick way for the incident technician to launch those tasks from within the **Process View** page.

You can edit forms in Workflow Solution and add or remove actions to different **Process View** pages.

The actions that appear on the **Process View** page vary for different processes. Each **Process View** page includes the actions that are most relevant and useful for its particular process. For example, some of the actions that appear on an incident's **Process View** page are: resolve incident, create a problem ticket, suggest self service, and escalate incident. These actions are useful for incident management, but would not be useful on the process view page for a change request.

Examples of the default actions that might appear on **Process View** pages are as follows:

- **Add/Manage Bulletin Boards**
- **Add Incident**
- **Create Problem Ticket**
- **Create Subtasks**
- **Escalate Incident**
- **Find Recent Changes**
- **Go To Discussion**
- **Invite Participant**
- **Manage Equipment**
- **Reclassify**
- **Remove Problem**
- **Request Change**
- **Resolve Incident**
- **Schedule for Later**
- **Search Google**
- **Search Google Groups**
- **Search KB**
- **Search MS Technet**
- **Send email**
- **Start Chat**
- **Suggest Self Service**
- **View Forward Schedule Change**
- **View Previous Submissions**
- **View Problem**

About smart tasks

Smart tasks are links to the processes, Altiris Task Server functions, or third-party programs that can be launched directly from a process ticket within ServiceDesk.

The smart tasks typically appear on the **Process View** page, under the **My Actions** section. They can also appear in the dialog box that appears when you click the task under the **History** section.

The smart task links let the process workers perform all the actions that are necessary to work their tickets from a single page. The result is that process workers can complete their tasks more quickly.

Permissions control the ability to access smart tasks.

Each ServiceDesk process contains a set of default smart tasks that are ready to use. However, you can customize the smart tasks to meet the specific needs of your organization by editing the workflow projects in Workflow Designer.

You can add and remove smart tasks from the process forms and you can edit smart tasks. You can also make the smart tasks conditional. For example, if an incident's description contains the word Symantec, the smart task for searching the Symantec Knowledge Base appears on the **Process View** page.

For more information about adding smart tasks to a form, see the *ServiceDesk Customization Guide*.

Chapter 8

Performing common actions in the ServiceDesk portal

This chapter includes the following topics:

Setting permissions

Throughout the ServiceDesk portal, an administrator or other user who has the appropriate permissions can set permissions to provide access to various items. For example, permissions can be set on documents, knowledge base articles, Service Catalog categories, reports, portal pages, and schedules.

To set permissions

1. Access the **Permissions** page or tab.

   This step might vary depending on your task. Typically, you click a **Permissions** tab on the item's editing page.

2. On the **Permissions** page, click **Add New Permission**.

3. In the **Permission Type** drop-down list, select one of the following :

- **User**
- **Group**
- **Permission**
- **Organization**

4 Type the name of the entity to apply the permissions to.

   You can also click **Pick** to select the appropriate entity.

5 If you clicked **Pick**, select a specific entity as follows:

   - In the **User Picker** dialog box, select a user.
     See "Picking a user" on page 96.
   - In the **Group Picker** dialog box , provide the group name, click **Search**, and then click the **Select** link to the right of the appropriate group.
   - In the **Permission Picker** dialog box to the right of the appropriate permission, click the **Select** link.
   - In the **Organization Picker** dialog box, expand the organizations if necessary, and then select an organization.

6 To set permission for a single action, in the appropriate column, click the red X symbol to change it to a green check mark symbol.

7 To set the same permission for all the actions, select one of the following options under the appropriate column:

   - **Allow All**
   - **Deny All**
   - **Inherit All**

8 Click **Add**.

9 To set permissions for another entity, repeat step 2 through step 8.

10 When you finish setting permissions, on the **Permissions** page, click **Save**.

Picking a user

As you use the ServiceDesk portal, you occasionally need to select a user. For example, you select a user to grant permissions to, reassign a ticket to, or add to a group.

You search for and select a user in the **User Picker** dialog box.

To pick a user

1. In the ServiceDesk portal, at the point where you must select a user, click **Pick**.

   Typically, this location is the **Add User** dialog box.

2. In the **User Picker** dialog box, provide the criteria for a user search.

   For example, you can type part of the user's email address or name, or select the group or organization to which the user belongs.

3. Click **Search**.

4. In the **User Picker** dialog box to the right of the appropriate user, click the **Select** link .

   At this stage, the user is not added yet.

5. When you are returned to the point where you selected the **Pick** option, click **Add** to add the user that you selected.

6. To add more users, repeat step 1 through step 5.

7. When you finish adding users, click **Close**.

Capturing a screen image

ServiceDesk provides a Screen Capture utility that lets users capture images of their computer screens.

The Screen Capture utility is available from the Windows **Start** menu, from an incident, and from a chat session. For example, a user can capture an error message and attach it to an incident. Any process worker can attach an image to a chat session.

Before you can capture a screen image, the Screen Capture Utility must be installed on your computer.

Capturing a screen image

1 Open the **Screen Capture** window in any of the following ways:

On the **Create a New Incident** page	Click **Take Screenshot**. See "Submitting an incident" on page 117.
On the **Reason for Re-Opening Issue** page	Click **Take Screenshot**.
In the **Process Manager Chat** window	Click **Screen Capture**. See "Chatting in the ServiceDesk portal" on page 324.
Under the Windows **Start** menu programs	Click **Altiris > Workflow Designer > Tools > ScreenCapture Util**.

2 (From an incident only) If the **Screen Capture** window does not open automatically, on the **Screen Capture** page, click one of the following links:

Click Here to Start Capturing	Opens the **Screen Capture** window. If the window does not open, then it probably is not installed on your computer.
Click Here to Install	Installs the Screen Capture utility if it is not installed.

3 In the **Screen Capture** window, select one of the following options to capture the image:

Capture Region	Capture a specific part of the screen, which you select. For example, you might select an error message or a portion of the screen that shows the options you selected before an error occurred.
Capture Screen	Captures the entire screen, minus the **Screen Capture** window.
Capture Delayed	Lets you set an amount of time to wait before the image is captured.

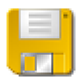
4 (Optional) Use any of the screen capture icons to edit the image as needed.

See "Screen Capture icons" on page 99.

5 When the image is finished, select one of the following icons:

The label on this icon differs depending on where you started the Screen Capture utility, as follows:

- **Send to Process Manager**
  If you accessed the **Screen Capture** window from an incident, this option places the image on the **Screen Capture** page. When you click **Completed** on the **Screen Capture** page, the file is saved and attached to the incident.
- **Send**
  If you accessed the **Screen Capture** window from a chat session, this option creates a file for the captured image and sends it to the chat session.
- **Send to Workflow**
  This option appears if you accessed the **Screen Capture** window from the Windows **Start** menu. This option applies to Workflow Solution only.



Save to File

Displays the **Save As** dialog box, where you can type a name for the file, and then click **Save**.

You can attach the saved file to the current process ticket, to any other process ticket, or to any other document.

Copy to Clipboard

Copies the captured image to the clipboard so you can paste it into a different image or any other document.

6 When you finish the capture, you can close the **Screen Capture** window to return to your starting point.

Screen Capture icons

The **Screen Capture** window lets you capture an image on your computer screen so you can attach it to a task or a process ticket. The icons that appear on this page represent the screen capture operations that you can perform. Some of these icons appear only during specific operations. For example, the editing icons do not appear until you capture a screen image.

See "Capturing a screen image" on page 97.

Table 8-1 Options in the **Screen Capture** window

Icon	Description
	**Add Note** Lets you add text to a captured image. When you click this symbol, additional icons appear at the left of the **Screen Capture** window to let you format the note.
panning arrows	Panning arrows let you move the image up, down, left, and right within the **Screen Capture** window when the image is larger than the window.
	**Capture Delayed** Lets you set an amount of time to wait before the image is captured.
	**Capture Region** Captures a specific part of the screen, which you select. For example, you might select an error message or a portion of the screen that shows the options you selected before an error occurred.
	**Capture Screen** Captures the entire screen, minus the **Screen Capture** window.
	**Change Border Color**
	**Change Border Width**
	**Change Fill**
	**Change Font**
	**Change Font Color**
	**Copy to Clipboard** Lets you paste the copied image into any other application.
	**Crop Image**

Table 8-1 Options in the **Screen Capture** window *(continued)*

Icon	Description
	**Draw Rectangle**
	**Open File**
	**Pan Image** Lets you move the image around within the **Screen Capture** window.
	**Paste** Lets you paste the contents of your Clipboard into the image. Use this option with the **Copy to Clipboard** option.
	**Redo** This icon is available only after you undo a change in the captured image.
	**Save to File**
	**Send to Process Manager**
	**Undo** This icon is available only after you make a change in the captured image.

Changing your password

ServiceDesk users who have permission to change their passwords can do so in the ServiceDesk portal.

Note: If your organization uses Active Directory to authenticate the users who log on to ServiceDesk, those users cannot change their passwords in the ServiceDesk portal.

To change your password

1. In the upper right of the ServiceDesk portal, click **Account**.
2. On the account page, at the far right of the **User Information** title bar, click the **Actions** symbol (orange lightning), and then click **Change Password**.
3. In the **Change Password** dialog box, enter your current password and your new password, and then confirm the new password.
4. Click **Change Password**.

Section 3

Managing incidents

Chapter 9

Introducing Incident Management

This chapter includes the following topics:

About Incident Management

Incident Management is one of the core ITIL 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.

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:

- 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 inclusion of a screen capture utility that lets users add screen images to their incident submission.

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 the Incident Management process

The goal of Incident Management is to recover from incidents and return the user to an operational state as quickly as possible.

ServiceDesk can be configured to send email notifications to users and other workers when certain actions are taken in the Incident Management process.

See "Email notifications from Incident Management" on page 112.

Table 9-1 Incident Management process

Step	Action	Description
Step 1	An incident is submitted.	An incident is a ServiceDesk ticket that reports an issue. Incidents can originate from user help calls or emails, support technicians, and external systems. See "Sources of ServiceDesk incidents" on page 111.

Table 9-1 Incident Management process *(continued)*

Step	Action	Description
Step 2	The incident data is analyzed and assigned to a support technician for resolution.	This step is an internal process. When the incident is submitted, the following actions occur: ■ Its data is stored. ■ Any configuration items that pertain to the incident are noted. For example, a specific computer or printer can be associated with the incident. ■ Its priority is calculated. ■ Its priority is evaluated and it is assigned to the Support I or Support II group. If assignment rules have been created, then they are evaluated to determine where to assign the incident.
Step 3	A support technician works the incident.	The incident appears in the task list for the technician, group, or organization. If the incident is assigned to a specific technician, the technician receives an email notification. See "Resolving an incident from the advanced incident form" on page 149. See "Resolving an incident from a task" on page 150. In addition to viewing and resolving the incident, the technician can perform other actions. Examples of incident actions are as follows: ■ Create a problem ticket, change request, or subtask. ■ View the current schedule, schedule the incident, or postpone the incident. ■ Search the ServiceDesk knowledge base or an external knowledge base. ■ Reclassify or escalate the incident. ■ Start a chat session or send an email.
Step 4	(Optional) A support technician escalates the incident.	An incident can be escalated when it is close to missing its required resolution date or when it must be resolved at a higher level. A support technician can escalate an incident from the incident's **Process View** page. If routing rules are defined for escalating an incident, any incident that meets those criteria is escalated automatically. See "About escalating incidents" on page 169.

Table 9-1 Incident Management process *(continued)*

Step	Action	Description
Step 5	The incident is resolved.	The support technician can resolve the incident or another process can resolve the incident automatically. For example, if the incident is associated with a change request and the change request is closed, the incident is resolved automatically. This type of automatic resolution is called a cascading closure. In some case, other processes might need to occur before the incident can be resolved. For example, when an incident has subtasks, one or more support technicians must resolve the subtasks before the incident is resolved.
Step 6	The user reviews the resolution and confirms or re-opens the incident.	The incident resolution appears in the user's task list and the user receives an email notification. The user views the incident's history, comments, and other information. If the support technician provided instructions for self-service or for testing, the user follows the instructions. If the resolution fixes the issue, the user confirms the fix and provides customer feedback. The incident is marked as Closed. See "Reviewing and closing a resolved incident" on page 126. If the resolution does not fix the problem, the user re-opens the incident. The incident is re-assigned to the support technician. See "Re-opening an incident" on page 127. If the user does not respond within two days, the incident's status is changed from Resolved to Closed.
Step 7	(Optional) The support technician performs the post-resolution activities.	The user's response appears in the support technician's task list and the technician receives an email notification. If the user closes the incident, the support technician can take any of the following actions: ■ Submit the resolution details to the knowledge base team to be integrated into an article or FAQ. ■ Re-open the incident. See "Re-opening an incident" on page 127. If the user or the technician re-opens the incident, the resolution steps are repeated.

Incident statuses

The incident status accurately reports the progression and outcome of the stages of the Incident Management process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the ServiceDesk portal. For example, they appear at the top of the ticket's **Process View** page.

Table 9-2 Incident statuses

Status	Description	Completion percentage
Closed	All manual actions and automated actions within the process are complete and the incident is closed.	100%
Escalated	The incident was escalated to a designated person or group for resolution.	70%
Hold	The incident is scheduled for later and is placed on hold. Typically, this status means that more research or analysis needs to be performed.	25%
Open	The incident was submitted and is ready to be worked.	10%
OUT OF TIME	The incident's due date passed and the incident was not resolved.	20%
Reopened	The user reviewed the incident and reopened it, which indicates that the incident is not fixed or the user is dissatisfied with the resolution. A new incident is created and the reopened incident is closed and added as an attachment.	10%
Resolved	A resolution for the entire incident was provided and the incident is ready for the user's approval. The resolution must apply to the entire incident, not to a single subtask.	90%
Responded	One or more of the incident's subtasks were responded to, regardless of whether a resolution was provided.	50%
Subtasks Created	One or more subtasks were created and assigned for the incident.	50%

Table 9-2 Incident statuses *(continued)*

Status	Description	Completion percentage
Time out/Exception	The incident exceeded the SLA window, therefore the incident is escalated.	20%

About the roles in Incident Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Incident Management process are tasked with submitting incidents and resolving them as quickly as possible.

See "About the Incident Management process" on page 106.

Table 9-3 Roles in Incident Management

Role	Description
User	The user can be anyone in or outside the organization who submits an incident. The user typically has limited access to the ServiceDesk processes.
Support technician	The support technician is a worker in the organization's support department who manages incidents. Organizations can have two or more levels of technicians. For example, first-level technicians can monitor incoming incidents, take support calls, and resolve incidents. If the problem cannot be resolved immediately or if it requires research or escalation, the technician can assign the incident to a second-level technician. The second-level technicians can perform incident analysis and resolve or escalate incidents. An incident can be assigned to a group or organization instead of to a specific technician. When an incident is assigned to a group or organization, it is added to a queue from which workers can select it. Some organizations might use a third level of support. Typically this level represents an external vendor or a manufacturer of hardware or software.

Table 9-3 Roles in Incident Management *(continued)*

Role	Description
Incident manager	The incident manager is responsible for the effective management of the incident process. The incident manager represents the first stage of escalation for the incidents that cannot be resolved within the agreed Service Levels. The incident manager is also responsible for incident reporting procedures.

Sources of ServiceDesk incidents

The creation of an incident triggers the Incident Management process. An incident can originate from several sources.

Table 9-4 Sources of ServiceDesk incidents

Source	Description
ServiceDesk portal	A user reports an issue by creating an incident in the ServiceDesk portal. See "Submitting an incident" on page 117.
User emails	A user can send an email to the ServiceDesk inbox and if it passes certain checks, it becomes an incident. See "Submitting an incident by email" on page 119.
Support technicians	Typically, a support technician creates an incident in response to a request from a user, either by telephone or email. See "About advanced incidents" on page 129.
Symantec Management Platform	You can create an incident for a specific resource in the Symantec Management Console. See "Creating an incident from the Symantec Management Platform" on page 138.
External systems	Your organization can make a web service call to Incident Management and pass in the data that is required to create an incident in ServiceDesk. For example, you might create incidents from Microsoft SharePoint, Microsoft InfoPath, Lotus Notes, Microsoft Systems Management Server (SMS), Adobe LifeCycle, and HP OpenView.

Email notifications from Incident Management

ServiceDesk sends email notifications at various stages of the Incident Management process. In this context, an incident event is any action that is taken to create or work an incident ticket. The type of event and the ServiceDesk configurations determine the recipients of the email notifications.

The email notifications from incidents, discussions, and problems can process replies to the notifications and add them to the history of the related ticket.

Replies are processed in the following situations:

- The email notification is sent from a process. Such emails contain an identifier to trigger the response.
- The email notification is sent from a template and the ServiceDesk worker selected the option to include a reply code.

Table 9-5 Default incident events that trigger email notifications

Event	Email recipient
An incident is submitted.	The submitter or the user on whose behalf someone submitted the incident Typically, the submitter is a user or a support technician. A setting in the ServiceDesk installation enables this type of notification.
An error occurs during the creation of an incident.	The Service Managers group An incident is not created, but a task is created for the group to review the data. The group can evaluate the error and decide to create an incident or resubmit the information. Resubmitting the incident information returns to point where the incident process was interrupted.
An incident or subtask is assigned to a specific support technician or group.	The assigned technician or group members
An incident is resolved.	The submitter The email asks the submitter to review the resolution and approve or re-open the incident. An option in the ServiceDesk installation enables this type of notification.
The support technician suggests a self-service option to resolve the incident.	The submitter The email suggests a tool that the submitter can use to resolve the problem.

Table 9-5 Default incident events that trigger email notifications *(continued)*

Event	Email recipient
The submitter closes the incident.	The submitter The email asks the submitter to complete the Customer Satisfaction Survey. By default, the survey is sent for every resolved incident, except for those that are closed with the Quick Close code. However, the administrator can change the frequency.
A user or a support technician starts a chat.	The person who is invited to chat

Process View page for incidents

The **Process View** page is the primary interface for working a task. The **Process View** page appears when you select a task from your **Task List** or from another list in the ServiceDesk portal.

The default sections on the **Process View** page are similar for all types of tasks. If your organization uses customized **Process View** pages, your views might look different.

See "Process View page" on page 89.

In addition to the common actions that you can perform for all tasks, the incident **Process View** page contains additional, incident-specific actions. The actions that are available depend on your permissions and the state of the incident. For example, if the incident has been escalated to a higher level, the **Resolve Incident** action is no longer available to you.

Groups of actions on an incident's **Process View** page

- **Incident**
  See Table 9-6.
- **Postponement**
  This section appears only in an incident that has been postponed.
  See Table 9-7.
- **Change and Problem Management Tools**
  See Table 9-8.
- **Reference Tools**
  See Table 9-9.
- **Smart Tasks**
  See Table 9-10.
- **Other Actions**

See Table 9-11.

Table 9-6 **Incident** actions

Action	Description
Resolve Incident	Lets you begin the incident resolution process. See "Resolving an incident from a task" on page 150.
Work Tasks Assigned to Others	Lets you work on a task that is assigned to someone else if you have the appropriate permissions. For example, a level-one support technician starts to work on an incident but leaves for lunch before the incident is resolved. The incident must be resolved before the technician is due to return. Another worker who is at the same level or higher can open the incident, select this option, and resolve the incident.

Table 9-7 **Postponement** actions

Action	Description
Remove From Hold	Lets you reopen an incident that has been postponed so that it can be worked. See "Reopening a postponed incident" on page 154.

Table 9-8 **Change and Problem Management Tools**

Action	Description
Create Problem Ticket	Lets you create a problem ticket based on the incident if the incident represents a recurring issue. See "Creating a problem ticket from an incident" on page 154.
Find Recent Changes	Displays any change requests that were completed within the last 14 days. The support technician can use this list to determine whether the current issue has been fixed.
Request Change	Lets you create a change request based on the incident if the incident represents a recurring issue. See "Creating a change request from an incident" on page 156.

Table 9-8 Change and Problem Management Tools *(continued)*

Action	Description
View Forward Schedule Change	Displays the Forward Schedule of Change. The ITIL Forward Schedule of Change (FSC) is an integrated view of all the approved changes and their release dates. See "Calendar page" on page 60. A support worker might view the FSC to determine if any scheduled activity might be the cause of an incident. For example, several users report that they cannot access email. By viewing the FSC, the support technician learns that the organization's email service is down for scheduled maintenance. The support technician can tell the users why the email is not available and when they can expect the service to be restored.

Table 9-9 Reference Tools

Action	Description
Search Google **Search Google Groups** **Search MS Technet**	Lets you search these external databases for any information that might relate to the incident or its resolution.

Table 9-10 Smart Tasks

Action	Description
Attach Process	Lets you add additional incidents, changes, and problems to this incident.
Create Subtasks	Lets you create one or more subtasks to record, assign, and track any additional actions that are required to resolve the incident. See "Creating a subtask for an incident" on page 161.
Reassign Incident	Lets you assign an incident to someone else and reset the priority. Select this option when the incident is close to missing its required resolution date or when it must be resolved at a higher level. See "Escalating an incident" on page 172.
Reclassify	Lets you change the incident's classifications, including the extended classifications.
Schedule For Later	Lets you change the task's due date. When you postpone an incident, it is removed from the incident queue until the scheduled date arrives. See "Scheduling an incident for later (postponing)" on page 153.

Table 9-10 Smart Tasks *(continued)*

Action	Description
Start PC Anywhere	Opens Symantec pcAnywhere to connect to a remote device. You can use this option when the incident is hardware-related.
Suggest Self Service	Lets you direct the submitter to a knowledge base article or a Service Catalog option that contains resolution instructions.
View Previous Submissions	Displays the submitter's past incidents. Viewing the user's submissions can let you see trends for the user or gather the history that might help analyze the current incident.

Table 9-11 Other Actions

Action	Description
Manage Equipment	Opens the **Add Equipment** page, which lets you add or delete the equipment that is related to the process. You can also access the quick tools for a piece of equipment.
Add/Manage Bulletin Boards	Lets you request a bulletin board entry. See "About the Bulletin Board" on page 251.
Send Email	Lets you send an email message regarding the ticket. See "Sending an email from a process ticket" on page 317.
Search KB	Lets you search the knowledge base for an article that is related to the ticket and then attach the article. See "Searching the knowledge base" on page 281.

Chapter 10

Submitting incidents (user method)

This chapter includes the following topics:

Submitting an incident

A user who has a problem and cannot find a resolution in the organization’s knowledge base can create an incident to report the problem. The user creates the incident in ServiceDesk using the general incident form. This form contains the minimum amount of information that is required to create an incident.

When you create an incident, you can perform the following actions:

- Attach a file to the incident.

See "Attaching a file to a new incident" on page 122.

- Capture a screen image and attach it to the incident.
  See "Capturing a screen image" on page 97.

If your ServiceDesk administrator allows it, you can also submit an incident by email.

See "Submitting an incident by email" on page 119.

To create an incident in ServiceDesk

1. In the ServiceDesk portal, click **Submit Request**.
2. On the right side of the page, click the **New Service Desk Request** link.
3. (Optional) To create an incident on behalf of another user, next to **Who does this issue affect?**, click **Someone Else**, and then click the **Search for User** link.

   Search for and add the user.
4. On the **Create a New Incident** page, enter information about the problem, and then click **Continue**.

   See "Create a New Incident page" on page 120.
5. To search the knowledge base or Service Catalog for any articles or self-service items that are related to your problem, click **Search the Knowledge Base**.

   See "Searching the knowledge base" on page 281.

   After the search, the options are as follows:

Answer Found	Lets you exit the incident submission process if you found an answer to your problem.
Continue with Incident	Lets you return to the **Create a New Incident** page if you did not find an answer to your problem.

6. If ServiceDesk has a record of the equipment that is assigned to you, the **Select Equipment** page appears. Select any equipment that this issue affects, and then click **Continue**.

   For example, if the incident involves a printer jam, you can select the printer that is jammed.
7. If you selected **Blocking Critical Business** as the urgency, on the **Critical Business Details** page, provide more information about the urgency, and then click **Continue**.

8 If the title or description of your incident matches that of a knowledge base article, the process suggests the articles that might provide a resolution. Your options are the same as in step 5.

9 On the **Review Request** page, verify that the information is correct, and then click **Submit**.

   If the information is not correct, you can click **Edit** to return to the incident.

10 When the **Thank You For Your Submission** page appears, make a note of the incident ID.

   This number identifies the incident in any future communications.

11 Click **Close** to exit the incident submission process or **Start Another** to open a new incident.

Submitting an incident by email

A user who has a problem and cannot find a resolution in the organization's knowledge base can report the problem by email. The incident is created automatically and assigned to a support group.

Your ServiceDesk administrator determines whether this feature is available.

When you create a new email message to report an incident, be sure to include the following information:

To submit an incident by email

◆ Create and send an email message that contains the following information:

Address	Use the address that your support organization provides.
Subject	Include any of the following phrases: ■ New Incident ■ New Ticket ■ Any other word or phrase that your support organization might require.
Message body	Provide details about the issue or provide any other information that your support organization requires. You might be provided with an email template to follow. If you leave the message body blank, this email might be classified as junk.

Create a New Incident page

This page lets you create an incident.

See "Submitting an incident" on page 117.

Table 10-1 Options on the **Create a New Incident** page

Option	Description
Who does this issue affect?	Lets you specify whether this issue affects you or someone else.
Search For User	Opens the **Select User** page, where you can specify the person who this issue affects. This link appears only when you specify that this issue affects someone else.
What is your issue?	Lets you type a brief description of the issue. Make this description as specific as possible. For example, instead of "email problem," you might type "Cannot receive external email". This description becomes the incident title, which identifies this incident in any incident lists in the ServiceDesk portal.
Details that might help resolve this issue	Lets you type additional information to describe the issue. For example, you might describe the steps to reproduce the issue or provide more information about what happened. The toolbar that appears in this section provides common text formatting tools.
Needed By Date	Lets you select the date on which this issue must be resolved. When you check this check box, a drop-down list appears. It lets you select the date from a calendar pop-up.
Change Location	Lets you specify the location that the incident affects. The affected user's location appears by default. When you click this link, the **Affected Location** page appears and you can select a different location if necessary. For example, you might encounter a problem with your email access during a visit to another corporate office. The location is for informational purposes only.
Change Department	Lets you specify the department that the incident affects. The affected user's department appears by default. When you click this link, the **Search for Affected Department** page appears and you can select a different department if necessary. The department is for informational purposes only.

Table 10-1 Options on the **Create a New Incident** page *(continued)*

Option	Description
Urgency of this need or issue	Lets you specify the severity of the issue. The options are as follows: ■ **No Immediate Urgency** ■ **Preventing Some Non-Urgent Work** ■ **Blocking Critical Business** Your organization or your manager might provide guidelines for when to use each of these options.
Who is affected?	Lets you specify how many people this issue affects. This information is combined with the urgency information to detrmine the incident's priority. The options are as follows: ■ **Single User** ■ **Entire Team or Group** ■ **Entire Department** ■ **Unsure**
Attach File	Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured. See "Attaching a file to a new incident" on page 122. See "Attach File to Incident dialog box" on page 122. Any files that you attach appear in the **Supporting Documents or Images** list.
Remove File	Lets you remove a file that is attached to the incident. The attached files are listed under **Supporting Documents** or **Images**.
Take Screenshot	Starts the Screen Capture utility so that you can capture an image of your computer screen, which you can attach to an incident. The Screen Capture utility also lets you edit the image. See "Capturing a screen image" on page 97. See "Screen Capture icons" on page 99.
Search the Knowledge Base	Lets you search the knowledge base for any articles that are related to your issue. You might find an article that answers your question and eliminates the need to submit an incident. See "Searching the knowledge base" on page 281.

Attaching a file to a new incident

During incident entry, you can attach one or more files to an incident to provide additional information about the issue. For example, you can attach an error log file or a screen image that you captured. Files larger than 4 MB are not supported.

See "Capturing a screen image" on page 97.

You can also attach a file to an incident after it has been created.

See "Attaching a file to an existing process ticket" on page 233.

The files that you attach to an incident are added to the **Documents** tab in the ServiceDesk portal. The files appear in a folder whose name is the incident number.

To attach a file to an incident

1. On the **Create a New Incident** page, click **Attach File**.

   See "Submitting an incident" on page 117.

2. In the **Attach File to Incident** dialog box, in **File to Add**, select a file.
3. (Optional) To add another file, click **Add Another**, and then select a file.

   Repeat this step for every additional file that you want to add.

4. When you finish adding files, click **Add and Close**.
5. On the **Create a New Incident** page, continue to enter information about the incident.

   See "Create a New Incident page" on page 120.

Attach File to Incident dialog box

This dialog box lets you attach one or more files to an incident to provide additional information about the issue. This dialog box appears when you choose to attach a file during the incident entry.

See "Attaching a file to a new incident" on page 122.

Table 10-2 Options in the **Attach File to Incident** dialog box

Option	Description
File to Add	Specify the file to add. You can add documents, spreadsheets, text files, logs, and many other file formats.

Table 10-2 Options in the **Attach File to Incident** dialog box *(continued)*

Option	Description
Current Attachments	Displays the files that are already attached to the ticket. The **Remove** link that appears next to each file lets you remove a file from the ticket.
Add Another	Adds the file to the **Current Attachments** list and lets you specify another file to attach without leaving the **Attach File to Incident** dialog box.
Add and Close	Adds the current attachments and closes the dialog box.

Capturing a screen image in an incident

When you create an incident, you can capture an image of your computer screen to help the ServiceDesk workers analyze the problem. For example, if an error message appears when you try to use an application, you can capture the message and attach it to the incident.

Before you can capture a screen image, you must have the Screen Capture Utility installed.

For more information, see the topics about installing the Screen Capture Utility in the *ServiceDesk Implementation Guide*.

To capture a screen image in an incident

1. On the **Create a New Incident** page, click **Take Screenshot**.

   See "Submitting an incident" on page 117.

2. If the Screen Capture utility does not open automatically, on the **Screen Capture** page, click one of the following links:

Click Here to Start Capturing	Opens the Screen Capture utility. If the utility does not open, then it probably is not installed on your computer.
Click Here to Install	Installs the Screen Capture utility if it is not installed.

3. In the **Screen Capture** window, select one of the icons to capture the image.

   See "Screen Capture icons" on page 99.

4. (Optional) You can edit the image in the following ways:

   - Add a note.

- Draw a rectangle.
- Crop the image.

5 When the image is finished, select one of the following symbols:

Send to Process Manager

Places the image on the **Screen Capture** page. When you click **Completed** on the **Screen Capture** page, the file is saved and attached to the incident.

Save to File

Displays the **Save As** dialog box, where you can type a name for the file, and then click **Save**.

You can attach the saved file to this incident, to any other incident or ticket, or to any other document.

Copy to Clipboard

Copies the captured image to the clipboard so you can paste it into a different image or any other document. You can return to the **Screen Capture** page and click **Cancel** to return to the incident.

6 When you finish the capture, you can close the **Screen Capture** window to return to the **Screen Capture** page, and then click **Cancel** to return to the incident.

7 When you return to the **Create a New Incident** page, you can continue the incident entry.

Finding and reviewing your incidents

You can review the incidents that you create. Although you cannot edit an incident, you can perform other actions that are related to the incident.

If the incident is open or in progress and you have the appropriate permissions, you can perform the following actions:

- Add a comment.
- Add or remove bulletin board entries.
- Add, remove, or manage the equipment that is associated with the incident.
- Send an email.
- Search the knowledge base.

- Open a chat session.

If the incident is closed, you can only view it.

To find and review an incident

1. In the ServiceDesk portal, click **Home**.
2. Under **My Requests**, if the incident is not listed, click the **Search** symbol, enter one or more keywords in the search box, and then click **Find In Report Data**.
3. Under **My Requests**, select the incident by its ticket number.
4. On the incident's **Process View** page, view the incident or take whatever actions are necessary.
5. When you finish, close the incident window.

Confirming an incident's resolution

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution.

Until you complete the confirmation task, the incident is considered to be 90 percent complete and open. If you do not respond within a specified number of days, the incident's status is changed from Resolved to Closed. Your ServiceDesk administrator determines the number of days that are allowed.

Table 10-3 Confirming an incident's resolution

Step	Action	Description
Step 1	Review the task and if necessary, take any steps that the support technician recommends.	You might need to take steps to resolve the issue yourself if the support technician provided instructions for doing so. For example, you might be directed to a knowledge base article or a Service Catalog option that contains resolution instructions.
Step 2	Test to confirm that the issue is fixed.	This step is important whether you resolved the issue or it was resolved for you.
Step 3	If the issue is not fixed or if you are dissatisfied with the resolution, re-open the incident.	When you re-open the incident, it is returned to a support technician. See "Re-opening an incident" on page 127. After you re-open the incident, wait for another task to notify you that it is resolved.

Table 10-3 Confirming an incident's resolution *(continued)*

Step	Action	Description
Step 4	If the issue is fixed, close the incident.	If you are satisfied with the resolution, you can mark the incident as resolved. The incident is closed. See "Reviewing and closing a resolved incident" on page 126. When you confirm that an incident is resolved, you might be asked to complete a Customer Satisfaction Survey.

Reviewing and closing a resolved incident

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution.

See "Confirming an incident's resolution" on page 125.

If the resolution fixes the issue, you can confirm the fix.

To submit feedback on an incident resolution

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.
3. In the list of tasks, find and open the task that requires feedback.
4. On the incident's **Process View** page, review the information that appears under **History**, and then expand the **Documents** section and read any documents as appropriate.
5. Expand the **My Actions** section, and then click **Click Here To Review and Close Your Incident**.
6. On the **Issue Resolved** page, review the details about the resolution and if you are satisfied with the resolution, click **Issue Resolved**.
7. If the **Welcome** page of the Customer Satisfaction Survey appears, follow the on-screen instructions to provide feedback and when you finish, click **Continue**.
8. When the **Thank You** page appears, you can close the page, and then you can close the incident's **Process View** page.

Re-opening an incident

After an incident is resolved, it appears in the affected user's task list for review of its history, comments, and other information about its resolution.

See "Confirming an incident's resolution" on page 125.

If the issue is not fixed or if you are dissatisfied with the resolution, you can re-open the incident.

Re-opening an incident creates a duplicate incident that refers back to the original one. The duplicate incident is returned to a support technician. The technician either resolves the issue or escalates it to a higher level of support. When the incident is resolved again, you are asked to verify the resolution and provide feedback.

See "Reviewing and closing a resolved incident" on page 126.

To re-open an incident

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.Incident Management**.
3. In the list of tasks, find and open the task that requires feedback.
4. On the incident's **Process View** page, expand the **My Actions** section, and then click **Click Here To Review and Close Your Incident**.
5. On the **Issue Resolved** page, review the details about the resolution and if you are not satisfied with the resolution, click **Re-Open Issue**.
6. On the **Reason for Re-Opening Issue** page, in the text box, type an explanation of why you need to re-open the incident.

   Provide details about the steps that you took to test the fix and the results of your test.

7 (Optional) You can attach files to the incident to support your explanation.

The options are as follows:

Add File	Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured. See "Attaching a file to a new incident" on page 122.
Remove	Lets you remove a file that is attached to the incident. The attached files are listed under **Supporting Documents** or **Images**.
Take Screenshot	Starts the Screen Capture utility so that you can capture an image of your computer screen, which you can attach to an incident. The Screen Capture utility also lets you edit the image. See "Capturing a screen image" on page 97. See "Screen Capture icons" on page 99.

8 On the **Reason for Re-Opening Issue** page, click **Continue** to submit the re-opened incident.

Submitting incidents (technician method)

This chapter includes the following topics:

About advanced incidents

Support technicians or other workers who submit incidents on behalf of users can use the advanced incident form, which collects additional details.

The advanced incident form lets you perform the following actions:

- Use a template to quickly populate the incident.
- Categorize the incident.

- Verify the configuration items for the user.
- Assign the incident to a worker or group.
- Set the impact and priority.
- Search the ServiceDesk knowledge base or external knowledge bases for any articles that might facilitate the incident resolution.
- Add contacts in addition to the primary contact.
- Specify the equipment, location, and services to associate with the incident.
- Associate the incident with similar incidents, changes, and problems.
- Start a chat session.
- Send an email to the user.
- Add an attachment.
- Save your input as a new template.
- Create a ticket for the incident.
- Resolve the incident.

See "Creating an incident for a user" on page 131.

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 that its purpose is to report break or fix issues only, which are what incidents handle. 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.

See "About the Service Catalog and service items" on page 382.

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 "Creating an incident template" on page 137.

See "Creating an incident from a template" on page 132.

Creating an incident for a user

A support technician typically creates an incident in response to a help call from a user. The technician can also create an incident on their own behalf.

The support technician uses the advanced incident form, which allows for the entry of more information than the general incident form that users typically submit.

See "About advanced incidents" on page 129.

Before you create an incident template, be sure that its purpose is to report break or fix issues only, which are what incidents handle. 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.

See "About the Service Catalog and service items" on page 382.

To create an incident with the advanced incident form

1. In the ServiceDesk portal, click **Submit Request**.
2. On the **Requests** page, under **New Requests** and under **Service Catalog**, click **ServiceDesk**.
3. On the right side of the page, click the **Submit Incident (Advanced)** link.
4. (Optional) To use a template to create the incident, on the **Create Incident** page, under **Select Template**, select a template from the list, and then click **Use Template**.

   See "Creating an incident from a template" on page 132.

5. On the **Create Incident** page, enter the information about the issue.

   See "Create Incident page: advanced form" on page 133.

   If you plan to create a new template, enter only the information that needs to appear in the template.

6. When you finish entering the information, select one of the following options:

Resolve	Lets you enter a resolution to the incident. See "Resolving an incident from the advanced incident form" on page 149.
Create Ticket	Submits the ticket without a resolution. On the **Thank You** page, you can start another incident or close the page.
Save As Template	Lets you save the incident information as a template for future use. See "Incident Template page" on page 138. When you finish creating the template, you are returned to the **Create Incident** page, where you can continue to create an incident or close the page.

Creating an incident from a template

When you create an incident with the advanced form, you can use a template to fill in some of the incident information.

See "About incident templates" on page 130.

To create an incident from a template

1. In the ServiceDesk portal, click **Submit Request**.
2. On the **Requests** page, under **Service Catalog**, click **ServiceDesk**.
3. On the right side of the page, click the **Submit Incident (Advanced)** link.
4. On the **Create Incident** page, under **Select Template**, select a template in the drop-down list and then click **Use Template**.

5 On the **Create Incident** page, enter any information that was not filled in by the template. You can also edit any of the pre-filled information.

See "Create Incident page: advanced form" on page 133.

6 When you finish entering the information, select one of the following options:

Resolve	Lets you enter a resolution to the incident. See "Resolving an incident from the advanced incident form" on page 149.
Create Ticket	Submits the ticket without a resolution. On the **Thank You** page, you can start another incident or close the page.

Create Incident page: advanced form

This page lets you create an incident with the advanced incident form.

See "Creating an incident for a user" on page 131.

See "Incident Template page" on page 138.

Table 11-1 Options on the **Create Incident** advanced form

Section	Option	Description
User Information	**Select User**	Lets you specify the primary contact for the incident. Typically, the primary contact is the person who encounters or reports the issue. You can specify the primary contact in any of the following ways: ■ You can type the user's email address and click the **Check if User Exists** symbol to the right of the box to verify the user in the database. ■ You can type part or all of the following information: Email address, first name, last name, nickname , phone number, manager, or employee ID, and then click the **Search** symbol (a magnifying glass).

Table 11-1 Options on the **Create Incident** advanced form *(continued)*

Section	Option	Description
User Information	**Location** **Department** **Phone No** **Address** **Associated Equipment**	Displays the information that is associated with the primary contact in the CMDB (Configuration Management Database). This display is for informational purposes only; it is not saved with the incident. However, you can click the **>>** option that appears next to any of these items to add the item to the incident.
User Information	**Tickets**	Lists the incidents that have been submitted for this user. The incidents in all states except Closed are displayed. To include the closed incidents in the list, click **Show Closed Tickets**.
User Information	**Show Closed Tickets**	Includes any closed tickets in the list of this user's previous tickets.
Select Template	Drop-down list	Lets you select from existing incident templates to create a new incident.
Select Template	**Save as Template**	Saves the information in the current incident as an incident template. You can create a template for your use only or you can make it available to others. See "Creating an incident template" on page 137.
Select Template	**Use Template**	Opens the template that you select from the **Select Template** drop-down list. See "Creating an incident from a template" on page 132.
Ticket Information	**Primary Contact**	Displays the user name (email address) of the person who is specified as the primary contact.
Ticket Information	**Title**	Identifies this incident in any incident lists in the ServiceDesk portal. When you type the title, make it as specific as possible. For example, instead of "email problem," you might type "Cannot receive external email".
Ticket Information	**Description**	Lets you type additional information to describe the issue. For example, you might describe the steps to reproduce the issue or provide more information about what happened. The toolbar that appears in this section provides common text formatting tools.
Ticket Information	**Classification** **Click Here to Classify**	Lets you select a classification for the incident. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification.

Table 11-1 Options on the **Create Incident** advanced form *(continued)*

Section	Option	Description
Ticket Information	**Type**	Lets you select the category that the incident belongs to. The default categories are as follows: ■ **How To** ■ **Break-Fix** ■ **Add-Install** ■ **Change-Move** ■ **Backup** ■ **Authorize-Approve** ■ **Delete-Remove** ■ **Request** Other categories might appear if your organization has customized them. See "About incident categories and the data hierarchy" on page 431.
Ticket Information	**Extend Classification**	Populates the page with the configuration items from the CMDB (Configuration Management Database). You can select one or more classifications as appropriate to put the incident in the correct classification.
Ticket Information	**Urgency**	Lets you specify how much the issue affects the submitter or the primary contact. See "Default priority, urgency, and impact values" on page 373.
Ticket Information	**Impact**	Lets you define the extent of the issue by specifying how many people are affected. See "Default priority, urgency, and impact values" on page 373.
Ticket Information	**Priority**	Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See "About the incident priority" on page 372. See "Default priority, urgency, and impact values" on page 373.
Ticket Information	**Attachments**	Opens the **Attach File to Incident** dialog box, which lets you attach files. For example, you can attach any file that helps the user understand or resolve the issue. See "Attach File to Incident dialog box" on page 122.

Table 11-1 Options on the **Create Incident** advanced form *(continued)*

Section	Option	Description
Ticket Information	**Assignments**	Lets you assign the ticket to another user, group, or organization.
Ticket Information	**Postpone Date**	Lets you specify the date on which the incident is assigned. The incident is created immediately but is not assigned until that date.
KB Articles	**Search External KB**	Displays any entries that are found by using the incident title as the search text. The entries that appear here are shown as a potential resolution to the incident. Lets you search Google, Technet, or another external database that your organization might provide access to.
Additional Contacts	None	Lets you add contacts to the incident. For example, if a user needs new equipment, you might add the user's manager to obtain approval for the purchase.
Related Processes	None	Lets you search for other incidents, changes, and problems to attach to this incident.
Location, Department, Equipment, Services	**Location**	Lets you specify the location that the incident affects. The location is for informational purposes only.
Location, Department, Equipment, Services	**Department**	Lets you specify the department that the incident affects.
Location, Department, Equipment, Services	**Equipment**	Lets you select any equipment that is related to the incident. For example, if the incident involves a printer jam, you can specify the printer that is jammed.
Location, Department, Equipment, Services	**Services** **Multiple**	Lets you select the business services that the incident affects. The **Multiple** check box opens the **Business Services** dialog box, where you can select multiple business services that are affected.

Create Incident Details page

This page lets you resolve an incident from the advanced incident form that is available to support technicians.

Table 11-2 Options on the **Create Incident Details** page

Option	Description
Close Code	Lets you select a code that indicates the nature of the resolution. ServiceDesk contains a set of predefined close codes. Other codes might appear if your organization has customized them. See "About incident close codes" on page 460.
Resolution Notes	Lets you type information in the text box about how the incident was resolved.
Relevant Articles	Displays any articles that are found automatically by using the incident title as the search text. The articles that appear here are shown to the user as a potential resolution to the incident.
Create a KB Article	Lets you request an entry that can provide help for the same kind of issue in the future. For example, if the issue was resolved by training the user, the technician can request a knowledge base article that contains the same information. Users who encounter that issue in the future can find and read the knowledge base article instead of creating an incident. When you select this option and resolve the incident, the request becomes a task for the knowledge base (KB) editor.

Creating an incident template

During the creation of an incident with the advanced form, you can use a template to fill in some of the information automatically.

See "About incident templates" on page 130.

To create an incident template

1. In the ServiceDesk portal, click **Submit Request**.
2. On the **Requests** page, under **Service Catalog**, click **ServiceDesk**.
3. On the right side of the page, click the **Submit Incident (Advanced)** link.
4. On the **Select Primary Contact** page, specify a primary contact if one is required.

   This contact does not appear when the template is used to create a new incident. If you plan to continue to create an incident after you create the template, then specify the user who reported the issue.

5 On the **Create Incident** page, enter only the information that needs to appear in the template.

See "Create Incident page: advanced form" on page 133.

6 On the **Create Incident** page, click **Save As Template**.

7 On the **Incident Template** page, provide information to identify and describe this template, and then click **Save Template**.

8 When you are returned to the **Create Incident** page, you can continue to create an incident or cancel it.

Canceling the incident does not affect the template that you created.

Incident Template page

This page lets you create a template that you and others can use to quickly create advanced incidents.

See "Creating an incident for a user" on page 131.

See "About incident templates" on page 130.

Table 11-3 Options on the **Incident Template** page

Option	Description
Template Name	Identifies this template in any list of templates. Make the name descriptive enough for you and others to easily understand the purpose of the template.
Template Description	Lets you type a description to further identify this template and make it more recognizable. Do not include critical information in the description because it is not intended to appear in all the lists that contain the name.
User Only Template	Lets you make this template available to you only or to others as well as you.

Creating an incident from the Symantec Management Platform

You can create an incident for a specific resource (configuration item) in the Symantec Management Console.

This integration between the Symantec Management Platform and the ServiceDesk portal provides a shortcut for creating incidents. When an incident is created with this method, the resource information is automatically added to the incident creation page. The person who creates the incident becomes the primary contact.

To enable this functionality, the SD.Feeder.CreateIncidentForAssetInNS package must be installed and then deployed to the production server.

For more information, see the *ServiceDesk Customization Guide* or the *Workflow Solution User Guide*.

To create an incident from the Symantec Management Platform

1. In the **Symantec Management Console**, on the **Manage** menu, click **Organizational Views and Groups**.
2. In the left pane, expand **Organizational Views**.
3. Under **Organizational Views**, navigate to and click the organizational group that contains the resource.
4. In the right pane, select the resource, and then in the **Actions** drop-down list, click **Create Incident in ServiceDesk**.
5. On the **New Incident From CI** page, complete the information about the incident, and then click **Continue**.

   See "New Incident From CI page" on page 139.
6. On the Thank You page, click **Close**.

New Incident From CI page

This page lets you create an incident for a specific resource (configuration item) in the Symantec Management Console.

See "Creating an incident from the Symantec Management Platform" on page 138.

Table 11-4 Options on the **New Incident From CI** page

Option	Description
What is your issue?	Contains the resource name by default. You can edit this information to make it more specific about the nature of the problem with the resource. This description becomes the incident title, which identifies this incident in any incident lists in the ServiceDesk portal.
Please provide any details that might help	Lets you type additional information to describe the issue. For example, you might describe what is wrong with the resource.

Table 11-4 Options on the **New Incident From CI** page *(continued)*

Option	Description
Priority	Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See "About the incident priority" on page 372. See "Default priority, urgency, and impact values" on page 373.
Urgency	Lets you specify how much the issue affects the submitter or the primary contact. See "Default priority, urgency, and impact values" on page 373.
Impact	Lets you define the extent of the issue by specifying how many people are affected. See "Default priority, urgency, and impact values" on page 373.
Add File	Lets you attach one or more files that provide additional information about the incident. For example, you can attach an error log file or a screen image that you captured. See "Attaching a file to a new incident" on page 122. See "Attach File to Incident dialog box" on page 122. Any files that you attach appear in the **Supporting Documents or Images** list.
Take Screenshot	Starts the Screen Capture utility so that you can capture an image of your computer screen, which you can attach to an incident. The Screen Capture utility also lets you edit the image. See "Capturing a screen image" on page 97. See "Screen Capture icons" on page 99. This action requires that you have the Screen Capture utility installed.

Chapter 12

Creating incidents from user emails

This chapter includes the following topics:

About the creation of incidents from emails

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. After an incident is created from an email, it can be worked the same way as any other incident.

The email monitoring process is defined in the SD.Email.Monitor and SD.Email.InboundManagement projects. 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 443.

Table 12-1 How the email contents populate the incident's values

Email values	Resulting incident values
Sender	Primary contact When the sender is not a ServiceDesk user, the incident's contact is set to guest@logicbase.com. However, because this guest user is not added as the primary contact, the support technician must add a primary contact to the incident.
Subject line	Incident title
Message body	Incident description The email monitoring process can be customized to parse the message for specific words or phrases and then populate the appropriate values in the incident. For example, the process might look for the words Windows, Word, Excel, or printer.

The default values for normal ServiceDesk incidents are used to populate additional information in the incident. For example, the status and urgency are assigned the default values.

Table 12-2 How emails are processed for incident creation

Criteria	How the email is processed
The subject line contains any of the following phrases: ■ New Incident ■ New Ticket ■ Any other word or phrase that you might have customized the process to look for.	The email monitoring process performs the following actions: ■ Creates a new incident that contains data from the email message. ■ Assigns the task according to the organization's usual routing process. ■ Sends a return email that contains the incident ID and the standard links for monitoring the incident.

Table 12-2 How emails are processed for incident creation *(continued)*

Criteria	How the email is processed
The subject line does not contain any of the required words or phrases.	The email monitoring process creates a task for the Service Managers group to review and classify the email. The manager can process the email as follows: ■ Create an incident or an advanced incident. ■ Add the email's contents to an existing incident. ■ Create a problem ticket. ■ Create a change request. ■ Create a request for a knowledge base item. ■ Suggest a self-service item from the Service Catalog. See "Email Classification page" on page 144.

The email monitoring process performs the following actions:

- Reads the response code that is associated with the email.
- Adds the email content to the incident's history.
- Creates a task for an incident worker to review the updated incident.

Evaluating and classifying incident email submissions

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.

See "About the creation of incidents from emails" on page 141.

When ServiceDesk cannot process an email automatically, it creates a task for the Service Managers group to evaluate the email. When you work the task, you can review it, request additional information, create an incident, change request, or problem ticket, or perform other actions.

To classify an incident email

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.
3. In the list of tasks, find and open the task that requires email classification.
4. On the incident's **Process View** page, expand the **My Actions** section, and then click **Classify Email Message**.

5 On the **Email Classification** page, select an option to process the email.

For example, you can create an incident, a change request, or a problem ticket based on the information in the email.

See "Email Classification page" on page 144.

6 Depending on the option that you choose on the **Email Classification** page, take one of the following actions:

- If another page appears, complete the page.
- If you are returned to the evaluation task's **Process View** page, you can close it.

Email Classification page

This page lets you review the content of an issue that was submitted in an email and decide how to process that issue in ServiceDesk.

When ServiceDesk cannot process an email automatically, it creates a task for the Service Managers group to evaluate the email. This page appears when the service manager works the evaluation task.

See "Evaluating and classifying incident email submissions" on page 143.

See "About the creation of incidents from emails" on page 141.

Whenever a process ticket is created as a result of the service manager's action, the process sends a return email. The email contains the process ID and the standard links for monitoring the ticket.

Table 12-3 Options on the **Email Classification** page

Option	Description
Self Service Suggestions	Presents a list of all the available Service Catalog items. When you select an item, a return email with a link to that self service item is sent.
Attachments	Displays any attachments that were included with the email.

Table 12-3 Options on the **Email Classification** page *(continued)*

Option	Description
Create Incident	Presents a series of options when you hover the mouse pointer over this option, as follows: ■ **Create an Incident Quickly** Creates an incident and sends a return email. ■ **Create Incident by Setting Priority** Opens the **Set Incident Priority** page, which lets you specify the priority, impact, urgency, and business service for the new incident. A return email is sent. See "Set Incident Priority page" on page 145. ■ **Search Incidents** Performs an automatic search of all the other incidents that are associated with the sender and displays them on the **Search for Related Processes** page. You can also search for other incidents. When you select one of the displayed incidents, the email contents are added to the history section of that incident. See "Search for Related Processes page" on page 146.
Create Problem	Creates a problem ticket and sends a return email.
Create Change Request	Creates a change request ticket and sends a return email.
Create KB Article	Creates a knowledge base article request and sends a return email.
Junk	Moves the email to the junk folder and ends the process.
Blacklist	Adds the sender to the blacklist, marks the email as read, and ends the process. By blacklisting a sender, you prevent the receipt of future emails from that sender. If you use the POP protocol for email, the user is blacklisted. If you use the IMAP protocol, the domain is blacklisted. The mail server manages the blacklist. When the service manager blacklists a sender, the email process communicates with the mail server and tells it to block that address. The next time an email from that address tries to enter the inbox that ServiceDesk monitors, the mail server software disallows it.

Set Incident Priority page

This page lets you specify the priority, impact, urgency, and business service for a new incident that you create from an email. This page appears when you click **Create Incident by Setting Priority** on the **Email Classification** page.

See "Email Classification page" on page 144.

Table 12-4 Options on the **Set Incident Priority** page

Option	Description
Urgency	Lets you specify how much the issue affects the submitter or the primary contact. See "Default priority, urgency, and impact values" on page 373.
Business Impact	Lets you define the extent of the issue by specifying how many people are affected. See "Default priority, urgency, and impact values" on page 373.
Priority	Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See "About the incident priority" on page 372. See "Default priority, urgency, and impact values" on page 373.
Business Services Affected	Lets you select the business services that the incident affects.
Attachments	Displays any attachments that were included with the email.
Submit	Creates an incident that contains the information that you entered. The contact information, subject, and description are obtained from the email. A task is sent to the incident's current assignee to notify them of the update.

Search for Related Processes page

This page lets you add the contents of an email submission to an existing incident. It performs an automatic search of all the other incidents that are associated with the sender. You can select from those incidents or search for additional ones.

When you select one of the displayed incidents, the email contents are added to the history section of that incident. A task is sent to the incident's current assignee to notify them of the update.

This page appears when you click **Search Incidents** on the **Email Classification** page.

See "Email Classification page" on page 144.

Table 12-5 Options on the **Search for Related Processes** page

Option	Description
Search for	Lets you type the search text and find an incident to attach the email information to.
Advanced Search **Click here for process view**	Lets you specify additional search criteria to help find the incident.
Search Results	Displays the incidents that result from your search and lets you select one to attach the email information to.
Processes Associated With This User	Displays the sender's past incidents.
Email Information	Displays the email information that is added to the incident.

Chapter 13

Resolving incidents

This chapter includes the following topics:

Resolving an incident from the advanced incident form

In response to a telephone call or email from a user, a support technician can record the incident on the advanced incident form. If the incident is resolved immediately, the support technician can resolve the incident at the same time as the incident entry.

For example, a user calls the Support Desk because of a printer jam. During the call, the support technician talks the user through the process of clearing the printer jam. When the call is over, the support technician creates and resolves the incident on the advanced incident form.

Resolving an incident is part of the Incident Management process.

See "About the Incident Management process" on page 106.

If you cannot resolve the incident, you might need to escalate it to another worker.

See "Escalating an incident" on page 172.

To resolve an incident from the advanced incident form

1 In the ServiceDesk portal, create an incident with the advanced incident form.

   See "Creating an incident for a user" on page 131.

2 When you finish entering information about the incident, on the **Create Incident** page, click **Resolve**.

3 On the **Create Incident Details** page, enter information about the resolution.

   You can also request a knowledge base article or other content based on this resolution.

   See "Create Incident Details page" on page 136.

4 When you finish entering details about the resolution, on the **Create Incident Details** page, click **Resolve Ticket**.

5 On the **Thank You** page, you can click **Start Another** or **Close**.

Resolving an incident from a task

The most common method for resolving an incident is to open its task from the **Task List** and work the incident from the incident's **Process View** page.

Resolving an incident is part of the Incident Management process.

See "About the Incident Management process" on page 106.

If you cannot resolve the incident, you might need to escalate it to another worker.

See "Escalating an incident" on page 172.

To resolve an incident from a task

1 In the ServiceDesk portal, click **My Task List**.

2 Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.

3 In the list of tasks, find and open a task that requires resolution.

4 On the incident's **Process View** page, expand the **My Actions** section, and then click **Resolve Incident**.

5 On the **Incident Response** page, enter information about the resolution and use any actions that are necessary.

   See "Incident Response page" on page 151.

6 When you finish entering information about the resolution, select one of the following options:

Save	Saves the changes without resolving the incident. You or another worker can re-open the incident and resolve it later.
Resolve	Resolves the incident.

7 When the resolved incident is closed and you are returned to the incident's **Process View** page, you can close it.

Incident Response page

This page lets you resolve an incident from a task. It appears when you work an incident task and select the **Resolve Incident** option.

See "Resolving an incident from the advanced incident form" on page 149.

See "Resolving an incident from a task" on page 150.

Table 13-1 Options on the **Incident Response** page

Option	Description
Classification	Lets you select a classification for the incident. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification.
Extend Classification	Populates the page with the configuration items from the CMDB (Configuration Management Database). You can select one or more classifications as appropriate to put the incident in the correct classification.
Incident Type	Lets you select the category that the incident belongs to. The default categories are as follows: ■ **How To** ■ **Break-Fix** ■ **Add-Install** ■ **Change-Move** ■ **Backup** ■ **Authorize-Approve** ■ **Delete-Remove** ■ **Request** Other categories might appear if your organization has customized them. See "About incident categories and the data hierarchy" on page 431.

Table 13-1 Options on the **Incident Response** page *(continued)*

Option	Description
Impact	Lets you define the extent of the issue by specifying how many people are affected See "Default priority, urgency, and impact values" on page 373.
Urgency	Lets you specify how much the issue affects the submitter or the primary contact See "Default priority, urgency, and impact values" on page 373.
Priority	Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See "About the incident priority" on page 372. See "Default priority, urgency, and impact values" on page 373.
Location Affected **Change Location**	Lets you specify the location that the incident affects. The location is for informational purposes only. When you click this link, the **Set Location Affected** page appears. It displays your default location but you can change it when you report the incident from a different location.
Close Code	Lets you select a code that indicates the nature of the resolution. The default close codes are as follows: ■ **Completed Success** ■ **Training Required** ■ **Review Documentation** ■ **No Fault Found** ■ **Monitoring Required** ■ **Advice Given** ■ **Change Required** Other codes might appear if your organization has customized them.
Follow the Sun	Lets you set the incident to be passed to or picked up by another location when the originating office closes. If your service organization provides 24-hour support by using service desks in various counties, you can use Follow the Sun routing. An incident can be submitted in one location and then passed from location to location as each office closes, until the incident is resolved.
Specify Time Worked	Lets you enter the amount of time that you spent on the incident offline. See "Posting process time to a ticket" on page 231.
Response	Lets you type information in the text box about how the incident was resolved.

Table 13-1 Options on the **Incident Response** page *(continued)*

Option	Description
Was Resolved on First Attempt	Lets you provide this information for reporting purposes.
Save	Saves the changes without resolving the incident. You or another worker can re-open the incident and resolve it later.
Resolve	Resolves the incident.

Scheduling an incident for later (postponing)

You can postpone the assignment and resolution of an incident by changing the task's due date.

When you postpone an incident, the following things happen:

- The status is changed to Hold.
- The task is removed from the **Tasks Viewer**.
- Any workers who are assigned to the task are unassigned.
- A comment is added to the task's **History** section.

These actions are reversed when the postponement date arrives or when someone reopens the incident.

See "Reopening a postponed incident" on page 154.

To schedule an incident for later

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.IncidentManagement**.
3. In the list of tasks, find and open the task to postpone.
4. On the incident's **Process View** page, expand the **Smart Tasks** section, and then click **Schedule For Later**.
5. On the **Schedule Incident** page, provide a reason for the postponement, specify the postpone date and time, and then click **Schedule**.
6. Close the incident page.

Reopening a postponed incident

You can postpone the assignment and resolution of an incident by changing its due date. When you postpose an incident, it is put on hold and cannot be worked until the postponement date arrives.

See "Scheduling an incident for later (postponing)" on page 153.

If you are ready to work the incident before the postponement date, you can reopen the incident.

When you reopen an incident that was postponed, the following things happen:

- The status is changed to Open.
- The task appears the **Tasks Viewer**.
- Any workers who were originally assigned to the task are re-assigned.
- A comment is added to the task's **History** section.
- The incident is added back to the SLA clock at its original level. It is not re-evaluated.

To reopen a postponed incident

1. In the ServiceDesk portal, click **My Task List**.
2. Because the incidents that are on hold do not appear in the **Tasks Viewer**, find the incident in one of the following ways:
   - Under **Tasks Viewer**, click the **Change Report** symbol that appears to the far right of the section, and then click **Incident Management > List Incidents On Hold**. Select the incident from the resulting list.
   - Under **Find Task**, type the Task ID and then click **Open**.
   - Under **Find Ticket**, type the ticket **ID** and then click **Open**.
3. On the incident's **Process View** page, under **Postponement**, click **Remove From Hold**.
4. In the **Incident Postponement Removal** dialog box, click **Close**.

Creating a problem ticket from an incident

When the cause of an incident is a systemic problem rather than an isolated issue, you can associate the incident with a problem ticket. The problem analyst and problem reviewer can analyze the root cause of the problem and suggest a workaround or fix that can resolve the incident.

You can create a new problem ticket or associate the incident with an existing problem ticket. For example, a new incident might report an issue that is already associated with a problem ticket. Problem tickets can be associated with multiple incidents.

See "About cascading relationships among process tickets" on page 38.

To create a problem ticket from an incident

1. In the ServiceDesk portal, find and open the incident.
2. On the incident's **Process View** page, under **My Actions**, expand **Change and Problem Management Tools**, and then click **Create Problem Ticket**.
3. On the **Submit Problem** page, take one of the following actions:

To attach the incident to an existing problem	Under **Associate with existing problems**, find and select the problem as follows: ■ In **Search for**, type the search text and search for a problem ticket. ■ Under **Search Results**, click the **Select** link to the right of the problem to add to. **Note:** A problem is created as soon as you click **Select**. **Note:** If you click this link by mistake, you can remove the relationship between the incident and the problem, or you can delete the problem ticket.
To create a new problem ticket	Under **Create a new problem**, define the new ticket as follows: ■ Review the suggested title and description and edit them if necessary. The title and description that default from the incident might be too specific or user-oriented to be appropriate for a problem ticket. ■ Click **Create New Problem**.

See "Submit Problem page" on page 155.

Submit Problem page

This page lets you associate an incident with an existing problem ticket or a create new problem ticket. It appears when you click **Create Problem Ticket** on the incident's **Process View** page.

See "Creating a problem ticket from an incident" on page 154.

Table 13-2 Options on the **Submit Problem** page

Option	Description
Search for	Lets you type the search text for finding a problem ticket.
Search Results	Displays the problem tickets that result from the search and lets you select the problem to add the incident to.
Title **Problem Description**	Lets you edit the problem title and description if necessary. The title and description that default from the incident might be too specific or user-oriented to be appropriate for a problem ticket.
Create New Problem	Creates a problem that is based on the incident.

Creating a change request from an incident

A support technician or other worker who works an incident can create a change request.

Creating a change request is a step in the Change Management process.

See "About the Change Management process" on page 181.

To create a change request from an incident

1 Open the incident.

2 Expand the **Actions** section.

3 Under **Actions**, expand the **ServiceDesk** section and click **Request Change**.

   If this action is not available, the task is probably not assigned to you. To enable this action and work the task anyway, under **Others Actions**, click **Work Tasks Assigned To Others** if that option is available.

Closing multiple incidents

When multiple incidents are ready to be closed, you can close them all at the same time.

To close multiple incidents

1 In the ServiceDesk portal, click **Submit Request**.

2 On the **Submit Request** page, under **Service Catalog**, click the **Service Desk** link.

3 On the right side of the page, click the **Close Incidents** link.

4 On the **Search Incidents** page, select the incidents to close as follows:

- In **Search for**, type the search text, and then click the **Search** symbol. You can search on the incident title or description.
- Under **Found Incidents**, select the check box next to each incident to close or click **Select All**.
- Click **Add Selected** to move the selected incidents to the **Incidents to Close** list.

5 (Optional) At any time, you can click **View Selected** under either list to view the incidents that are in that list.

6 (Optional) If you need to remove an incident from the **Incidents to Close** list, select the check box next to the incident and click **Remove Selected**.

7 Click **Close Incident(s)**.

8 On the **Close Incidents** page, complete the following information:

Reason for Closing Incidents	Explain why the incidents can be closed.
Close Code	Select a code that indicates the nature of the resolution.

9 Click **Close Incidents**.

Chapter 14

Creating incident subtasks

This chapter includes the following topics:

About subtasks

Before you resolve an incident, several additional actions might need to be taken. You can create subtasks to record, assign, and track the additional actions for an incident. For example, you might create a subtask to review a server's specifications to determine whether that server can accommodate a software upgrade.

See "Creating a subtask for an incident" on page 161.

During the subtask creation, you can create a subtask template and you can create a subtask from a template.

See "About subtask templates" on page 160.

The subtask workers can view the subtasks in their Task Lists and work the subtasks the same as any other incident tasks. The support technician who created the subtasks can view the parent incident's status changes and it history.

The support technician who creates the subtasks can determine how the resolution of the subtasks affects the parent incident. The **Return Incident On Completion** check box on the **Subtasks** page determines how the parent incident is affected.

See "Subtasks page" on page 162.

The resolution of the subtasks can affect the parent incident in the following ways:

The parent incident is returned to the support technician.	When all the subtasks are resolved, the parent incident is returned to the support technician who created the subtasks. The subtask resolutions are merged to provide part of the incident resolution. Use this method when the support technician must take additional action on the incident after the subtasks are resolved. For example, the subtasks might represent any research that determines how the technician resolves the parent incident. This method is used when **Return Incident On Completion** is checked.
The parent incident is closed.	When all the subtasks are resolved, the parent incident is closed automatically. The subtask resolutions are merged to provide the incident resolution. Use this method when no additional action is required after the subtasks are resolved. This method is used when **Return Incident On Completion** is not checked.

About subtask templates

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.

Using templates not only speeds the entry of subtasks, but it also helps to standardize and increase the accuracy of the subtask information.

You can both create and use subtask templates on the **Subtasks** page.

See "Creating a subtask template" on page 165.

See "Creating a subtask from a template" on page 162.

Creating a subtask for an incident

When the resolution of an incident requires that additional actions are taken, you can create subtasks to record, assign, and track the additional actions.

See "About subtasks" on page 159.

To speed the creation of a subtask, you can create a subtask from a template.

See "Creating a subtask from a template" on page 162.

To create a subtask for an incident

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.
3. In the list of tasks, find and open the task that requires a subtask.
4. On the incident's **Process View** page, expand the **Smart Tasks** section, and then click **Create Subtasks**.
5. On the **Subtasks** page, click **Add Subtasks**.

   See "Subtasks page" on page 162.
6. On the **Create Subtask(s)** page, click **Choose Assignee**.
7. On the **Subtask Assignment** page, do the following:
   - Search for users or groups to add to the **Search Results** section.
   - Under **Search Results**, click the **Add** link next to the users or groups to add.
   - Click **Add Assignments**.

   See "Subtask Assignment page" on page 164.
8. On the **Create Subtask(s)** page, enter the details about the subtask, and then click **Add Task**.

   See "Create Subtask(s) page" on page 163.
9. (Optional) Assign and create additional subtasks as needed.
10. When you finish adding subtasks, on the **Subtasks** page, click **Complete**.

Creating a subtask from a template

When you create a subtask, you can use a template to quickly fill in some of the subtask information.

See "About subtask templates" on page 160.

See "Creating a subtask for an incident" on page 161.

To create a subtask from a template

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.
3. In the list of tasks, find and open a task that requires resolution.
4. On the incident's **Process View** page, expand the **Smart Tasks** section, and then click **Create Subtasks**.
5. On the **Subtasks** page, in **Select a Template**, select a template to use.

   See "Subtasks page" on page 162.
6. Click **Use Template**.
7. On the **Subtasks** page, enter any information that was not filled in by the template.

   You can also edit any of the pre-filled information, and you can click **Add Subtask** to add and assign additional subtasks.

   See "Create Subtask(s) page" on page 163.
8. When you finish editing and adding information, on the **Subtasks** page, click **Complete**.

Subtasks page

This page lets you create subtasks for an incident. Subtasks represent the additional actions that need to be taken to resolve the incident. This page appears when you click **Create Subtasks** on an incident's **Process View** page.

See "Creating a subtask for an incident" on page 161.

Table 14-1 Options on the **Subtasks** page

Option	Description
Remove	Deletes the subtask to the left of this link.
Edit	Lets you edit the subtask to the left of this link.

Table 14-1 Options on the **Subtasks** page *(continued)*

Option	Description
Leave Incident Open After Subtask Completion	Determines what happens when the subtasks for an incident are resolved. The options are as follows: ■ This option is selected. When all the subtasks are resolved, the parent incident is returned to the support technician who created the subtasks. The subtask resolutions are merged to provide part of the incident resolution. ■ This option is not selected When all the subtasks are resolved, the parent incident is closed automatically. The subtask resolutions are merged to provide the incident resolution.
Select a Template	Lets you select from existing subtask templates to create a new subtask.
Use Template	Opens the template that you select from the **Select Template** drop-down list.
Add Subtask	Opens the **Create Subtask(s)** page, where you can enter the subtask details and make assignments. See "Create Subtask(s) page" on page 163.
Save As Template	Saves the information in the current subtask as a subtask template. You can create a template for your use only or you can make it available to others.
Complete	Saves the subtasks that are listed and closes the **Subtasks** page.

Create Subtask(s) page

This page lets you add one or more subtasks to an incident and assign the subtasks to other workers. It appears when you click **Add Subtask** on the **Subtasks** page.

See "Creating a subtask for an incident" on page 161.

Table 14-2 Options on the **Create Subtask(s)** page

Option	Description
Choose Assignee	Lets you assign the subtask to one or more users or groups. See "Subtask Assignment page" on page 164.

Table 14-2 Options on the **Create Subtask(s)** page *(continued)*

Option	Description
Subtask Title	Identifies this subtask in any task lists or ticket lists in the ServiceDesk portal. When you type the title, make it as specific as possible.
Description	Lets you type additional information to describe the subtask. Provide sufficient details to let the assignee know what to do. The toolbar that appears in this section provides common text formatting tools.
Warn Date	Lets you specify the date on which the assignee should be warned to resolve the subtask.
Late Date	Lets you specify the date on which the subtask must be resolved. If this date passes and the incident is still unresolved, it is marked as late.
Priority	Lets you select the priority for resolving this incident. The priority determines how the incident is routed and when it is escalated. See "About the incident priority" on page 372. See "Default priority, urgency, and impact values" on page 373.
Add Another	Lets you create additional subtasks without having to click **Add Task** after each addition.
Add Task	Creates the subtask and adds it to the list on the **Subtasks** page.

Subtask Assignment page

This page lets you assign a subtask to one or more users or groups. It appears when you click **Choose Assignee** on the **Create Subtask(s)** page

See "Creating a subtask for an incident" on page 161.

Table 14-3 Sections and options on the **Subtask Assignment** page

Section or option	Description
User **Group**	Let you specify whether to search for users or groups.
Search For	Lets you type the search text, and then click the **Search** symbol.

Table 14-3 Sections and options on the **Subtask Assignment** page *(continued)*

Section or option	Description
Search Results section	Lists the users or groups that you searched for and lets you select one or more of them to add to the **Selected Assignments** section.
Selected Assignments section	Lists the users and groups that you added from the **Search Results** section.
Remove	Lets you remove a user or group from the **Selected Assignments** section.
Add Assignments	Assigns the subtask to the users and groups that appear in the **Selected Assignments** section.

Creating a subtask template

During the creation of a subtask, you can use a template to fill in some of the information automatically. You can create a template during the subtask entry.

See "About subtask templates" on page 160.

To create a subtask template

1. In the ServiceDesk portal, open an incident's **Process View** page.
2. On the incident's **Process View** page, expand the **Smart Tasks** section, and then click **Create Subtasks**.
3. On the **Subtasks** page, click **Add Subtasks**.

   See "Subtasks page" on page 162.
4. On the **Create Subtask(s)** page, enter only the information that needs to appear in the template, including any assignments.

   See "Create Subtask(s) page" on page 163.
5. When you finish creating subtasks and making assignments, on the **Create Subtask(s)** page, click **Add Task**.
6. On the **Subtasks** page, review the subtasks that appear under **Subtask List**.
7. If applicable, check **Return Incident On Completion**.
8. Click **Save As Template**.

9. In the **Create Subtask Template** dialog box, provide a name for the template, and then click **Save Template**.
10. When you are returned to the **Subtasks** page, you can continue to create a subtask or closing the page.

    Closing the page does not affect the template that you created.

Chapter 15

Routing and escalating incidents

This chapter includes the following topics:

About incident routing and escalation

A key feature of ServiceDesk is its ability to route (assign) and escalate incident tickets to provide efficient and timely incident handling.

Routing rules determine the users or groups that new ServiceDesk incidents are assigned to. The rules also determine how incidents are escalated. ServiceDesk contains predefined routing rules and other settings that are ready to use, but you can customize them to meet your organization's requirements. Most organizations perform some level of customization.

The default routing rules in ServiceDesk assign new incidents based on each incident's priority setting as follows:

- The incidents that have a priority setting other than High or Emergency are assigned to the Support I group.

- The incidents that have a priority setting of High or Emergency are assigned to the Support II group.

The additional ServiceDesk settings that can affect the incident routing are as follows:

The Service Level Agreement (SLA) time frames and the **AllowAutoEscalation** option in the **Application Properties** settings	By default, the automatic escalation is enabled. The SLA time frame determines when an incident is escalated automatically. For example, if an incident that is assigned to the Support I group is not completed within six days, it is escalated to Support II. The incidents that are escalated automatically are assigned to the Support II group. The incidents that have a priority setting of High or Emergency follow a shorter SLA time frame than the other incidents. See "About the Service Level Agreement (SLA) time frames" on page 376.
The **Follow the Sun** option that can be set for individual incidents	An incident is worked in one location and then passed to or picked up by another location when the originating office closes. The incident is then passed from location to location as each one closes, until the incident is resolved. See "About Follow the Sun routing" on page 378.
Customized rules that are created in the **Automation Rules** interface	**Automation Rules** interface allows ServiceDesk administrator to create custom rule sets. Every incident is evaluated against existing rule set and if condition(s) are met, the incident is routed accordingly.

Process workers can override the default routing and escalation by reassigning and escalating the tickets manually.

See "Reassigning incidents, problems, or change tickets" on page 235.

See "About escalating incidents" on page 169.

You can customize the routing rules to define more specific criteria for routing and escalating incidents. For example, you can customize the routing rules to assign incidents to a specific group based on the group's location. Another way to customize your incident routing is to combine rules. For example, you can route incidents to a specific group if their priority is High, their category is Server, and their location is Corporate Headquarters.

You can customize the routing rules in Workflow Designer, in the SD.RoutingRules project.

For more information about editing workflow projects, see the *Workflow Solution User Guide*.

About escalating incidents

An incident can be escalated when it is close to missing its required resolution date or when it must be resolved at a higher level.

Escalation means that you assign an incident to someone else and reset the priority. You can escalate an incident to a higher-level user or group. An escalated incident appears in the Task List with a priority of High. An escalated incident must be resolved as soon as possible.

Table 15-1 Methods for escalating incidents

Method	Description
In the ServiceDesk portal	A support technician can escalate an incident from the incident's **Process View** page. See "Escalating an incident" on page 172. For example, a technician might escalate an incident when they cannot resolve it in the required amount of time.
Automatically	ServiceDesk contains the routing rules that define the criteria for escalating an incident. When an incident meets those criteria, it is escalated automatically. You can modify the existing routing rules and create new routing rules in Workflow Solution. See "About incident routing and escalation" on page 167. Examples of the criteria for escalating an incident are as follows: ■ No activity is posted to the incident within a specific amount of time. ■ The incident is not resolved within a specific amount of time. ■ A user who does not have privileged escalation rights escalates an incident. A setting in the ServiceDesk installation determines whether automatic escalation is available.

ServiceDesk allows two types of escalation: unprivileged and privileged. The user group that you belong to determines the type of escalation that you can perform.

You can edit the escalation assignments in Workflow Designer, in the SD.RoutingRules project.

For more information about editing workflow projects, see the *Workflow Solution User Guide*.

Table 15-2 Types of escalation by user group

Escalation type	Default group	Description
Unprivileged	First-level support (Support I)	The incident is escalated to the next-highest user, group, or organizational unit that is defined in the process. For example, your organization's incident process is configured to escalate to the next-highest group. Therefore, when a level-one support technician escalates an incident, it is assigned to the Support II group.
Privileged	Second-level support (Support II) and higher	You can escalate an incident to one or more specific users, groups, or organizations that you select. For example, your organization's incident process is configured to escalate to the next-highest group. A level-two support technician determines that only a specific person in that group can resolve a particular incident. The technician can escalate the incident directly to that person instead of to the entire group. When you escalate an incident to multiple users, each user that you escalate to can work on the task. Whoever begins working on the task first becomes the assignee.

About automation rules

Automation rules interface lets you create incident routing rules for any applications that are workflow-based and include service automation library. By default, ServiceDesk provides service automation library for incident management service with three predefined rule sets:

- Escalation Routing
- Reclassification Routing
- Initial Routing

The Administrator can configure routing and notification rules for specific events within the incident management process. A rule is comprised of two variables: composite condition and an action to take. One rule can have multiple conditions.

Available condition properties are as follows:

- Affected Assets
- Affected User
- Incident Classification

- Department
- Impact
- Location
- Priority
- Submitter
- Urgency
- Any
- Contacts

Note that you can sequence multiple rules for fine-tuning .

See “Creating new automation rules for incident management” on page 171.

Creating new automation rules for incident management

You can reprioritize a low priority incident as an emergency incident if the affected user is a VIP.

See “About Incident Management” on page 105.

To create a new automation rule for incident managment

1. In the portal, click **Admin > Automation Rules**
2. In the right pane, in the **Select Ruleset** drop-down list, select **Inital Routing**.
3. Click **Add Rule** (orange lightning bolt icon) and select **Add Rule**.
4. On the **Add Rule** page, in the **Condition** drop-down list, select **Affected User**.
5. In the drop-down list appearing to the right of the **Condition** drop-down list, select **Is VIP**.
6. In the **Action** drop-down list, select **Set Priority**.
7. In the right-most drop-down list on the **Action** line, select **Emergency**.
8. In the **Disposition** drop-down list, select **Stop**.
9. Click **Save.**

Escalating an incident

An incident can be escalated when it is close to missing its required resolution date or when it must be resolved at a higher level.

Escalation means that you assign an incident to someone else and reset the priority. You can escalate an incident to a higher-level user or group. An escalated incident appears in the **Task List** with a priority of High. An escalated incident must be resolved as soon as possible.

ServiceDesk allows two types of escalations: unprivileged and privileged. The user group that you belong to determines the type of escalation that you can perform.

See "About escalating incidents" on page 169.

To escalate an incident

1 In the ServiceDesk portal, click **My Task List**.

2 Under **Tasks Viewer**, under **Project Name**, expand **SD.Incident Management**.

3 In the list of tasks, find and open the task that requires escalation.

4 On the incident's **Process View** page, expand the **Smart Tasks** section, and then click **Escalate Incident**.

5 On the **Escalate** page, under **Justification**, describe why escalation is required and provide any other relevant information.

   For example, you might describe any unsuccessful attempts to resolve the incident.

6 (Unprivileged escalation only) On the **Escalate** page, click **Escalate to Support II**.

   Skip to step 8

7 (Privileged escalation only) On the **Escalate** page, under **Select a User or Group**, take any of the following actions:

Search for a user or group to escalate to.	In the **Search for** box, type the search text, and then click the **Search** symbol.
Escalate to a user or group that appears under **Users/Groups**.	Click the **Escalate** link next to the user or group.
Escalate to multiple users and groups.	Click **Advanced**, and then complete the **Escalate to Multiple Users/Groups** page. See "Escalate to Multiple Users/Groups page" on page 174.
Escalate to the next-highest group that is defined in the process.	Click **Escalate to Support II**.

8 On the **Confirm Escalation** page, verify that the escalation information is correct, and then click **Confirm**.

9 When you are returned to the incident's **Process View** page, you can close it.

Escalate page

This page lets you escalate an incident and provide information about the escalation.

See "Escalating an incident" on page 172.

The options that let you escalate an incident to specific users or groups appear only if you perform a privileged escalation.

The user group that you belong to determines the type of escalation that you can perform.

See "About escalating incidents" on page 169.

Table 15-3 Options on the **Escalate** page

Option	Description
Justification	Lets you provide justification for escalating the incident. This justification is required.

Table 15-3 Options on the **Escalate** page *(continued)*

Option	Description
Search for	(Privileged only) Lets you search for a user or group to escalate to. You can click **User** or **Group**, and then type the search text and click the **Search** symbol. Your selections appear in the **Users/Groups** list.
Advanced	(Privileged only) Lets you escalate the incident to multiple users and groups. See "Escalate to Multiple Users/Groups page" on page 174.
Escalate link **Add** link	(Privileged only) Adds a user or group to the escalation list when you click this link next to the user name or group in the **Users/Groups** list. You can add more than one user or group. Both these links do the same thing.
Auto Escalate	Lets you escalate the incident to a user or group that is one level higher than your own.

Escalate to Multiple Users/Groups page

This page lets you escalate an incident to multiple users or groups. It appears when you click **Advanced** on the **Escalate** page.

See "Escalate page" on page 173.

This page is available only if you perform a privileged escalation. The user group that you belong to determines the type of escalation that you can perform.

See "About escalating incidents" on page 169.

When you escalate an incident to multiple people, each person has the ability to work on the task. The task becomes assigned to and leased to the first person who begins working on the task.

See "About restricting access to open tasks (leasing)" on page 229.

Table 15-4 Sections and options on the **Escalate to Multiple Users/Groups** page

Section	Option	Description
Groups with Permissions	**Add**	Lists the groups that have permission to work on incidents and add one or more groups to the **Escalation List** section.
Available Contacts	**Add**	Lists the users who have permission to work on incidents and lets you add one or more users to the **Escalation List** section.
Escalation List	**Remove**	Lists the users and groups that you added from the other sections and lets you remove one or more of them from this list.
Search Results	**Select**	Lists the users or groups that you searched for and lets you select one or more of them to add to the **Escalation List** section.
none	**User** **Group**	Let you specify whether to search for users or groups.
none	**Search for**	Lets you type the text to search for.
none	**Escalate**	Escalates the incident to the users and groups that are in the **Escalation List**.

Section 4

Managing changes

Chapter 16

Introducing Change Management

This chapter includes the following topics:

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 so that 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 181.

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 179.

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.

See "About cascading relationships among process tickets" on page 38.

The Change management process consists of the following states:

- Received
  See "Change Management process: Received State" on page 183.
- Planned
  See "Change Management process: Planned state" on page 182.
- Reviewed
  See "Change Management process: Reviewed state" on page 183.
- Closed
  See "Change Management process: Closed state" on page 184.

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. 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 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.

A normal change is one that occurs as a result of normal activity. For example, once a computer has become obsolete, it experiences a normal change of repurposing or disposal.

Change Management process: Planned state

The Planned state is a state in the Change Management process.

See "About the Change Management process" on page 181.

The Change Manager has submitted the change plan to the CAB for approval. the change manager selects the CAB during the Received state. The CAB can either approve or reject the plan. The CAB can opt to schedule it for a later time. This state is skipped if the Change Manager chooses the Standard plan type.

The table describes the details of the Planned state in the Change Management process.

State name:	Planned
Brief description:	Change Manager submits the change plan to the CAB for approval.
Initiated by:	Change Manager completes and submits change plan
Outcome/Next status:	■ Change scheduled for implementation (Reviewed) ■ Change plan denied (Closed: DeniedByCab)
Players:	Change Approval Board (CAB/ECAB)
Available actions:	■ Task: Approve Change plan. ■ Process Action: Edit Change plan. ■ Process action: Manage CABs. ■ Process action: Manage equipment.

Change Management process: Received State

The Received state is a state in the Change Management process.

See "About the Change Management process" on page 181.

In this state, the change manager receives the change request and is ready for planning. During this state, the Change Manager can delegate portions of the planning to others.

The table describes the details of the Received state in the Change Management process.

State name:	Received
Brief description:	The request has been received and the Change Manager reviews it.
Initiated by:	Change request submitted
Outcome/Next status:	■ Plan completed and submitted to CAB for review (Planned) ■ CAB approval is bypassed and change is scheduled (Reviewed) ■ Request denied (Closed: DeniedByCm)
Players:	Change manager, selected delegates
Available actions:	■ Task: Submit change plan. ■ Smart task: Delegate Implementation plan. ■ Smart task: Delegate Test plan. ■ Smart task: Delegate Backout plan. ■ Smart task: Delegate other task. ■ Smart task: Manage delegations. ■ Process action: Edit Change plan. ■ Process action: Manage CABs. ■ Process action: Manage equipment.

Change Management process: Reviewed state

The Reviewed state is a state in the Change Management process.

See "About the Change Management process" on page 181.

In this state, CAB approval was either provided or was not needed. During this phase the change is implemented, either immediately or at the scheduled time.

The table describes the details of the Reviewed state in the Change Management process.

State name:	Reviewed
Brief description:	The change plan has been approved and is scheduled for implementation
Initiated by:	CAB approves Change plan or the Change Manager initiates change directly (for Standard plan)
Outcome/Next status:	■ Change successfully implemented (Closed: Success) ■ Change cannot be implemented (Closed: Failure)
Players:	Implementer is selected during the planning phase
Available actions:	■ Task: Indicate Change completed

Change Management process: Closed state

The Closed state is a state in the Change Management process.

See “About the Change Management process” on page 181.

To reach this state, a close code must be provided. It can be one of the following:

- Success – The change was implemented.
- Failure – The change cannot be implemented for some reason.
- DeniedByCm – Change manager denies Request.
- DeniedByCab – CAB denies the plan.

The table describes the details of the Closed state in the Change Management process.

State name:	Closed
Brief description:	No further action is taken on the ticket
Initiated by:	Change Manager denies change request, CAB denies change plan, or Implementer marked change as Completed

Outcome/Next status:	N/A
Players:	N/A
Available actions:	N/A

Actions in the Change Management process states

In each state in the Change Management process, specific types of actions are available. Each action is associated with a specific user role.

See "About the Change Management process" on page 181.

The following types of actions are available in the Change Management process:

- **Task**
  A **Task** is an actual workflow step. The completion of a task moves the process along.
- **Smart Task**
  A **Smart Task** is an additional action available to a specific user or group at a specific moment in the process. After the user or group completes the main task that is assigned to them, this smart task is no longer available. It may or may not provide an alternative to completing the main task, advancing the process along.
- **Process Action**
  A **Process Action** is an action that can be performed by anyone with the appropriate access level to the process, regardless of process state. This action can be used to edit ticket data directly, and so forth.

Table 16-1 Change Management process actions

Action	Initiator of Action	Type	Description
Submit Change Plan	Change Manager	Task	■ Provide state-sensitive elements of the change plan, such as the designated CAB, the change type, and the implementer. ■ Submit the change plan to the CAB, moving the process to the Planned state.

Table 16-1 Change Management process actions *(continued)*

Action	Initiator of Action	Type	Description
Delegate [Plan Element]	Change Manager	Smart task	■ Create tasks for selected delegates to complete portions of the change plan, like the implementation plan or the testing plan. Sets the status for the affected plan elements to Assigned. ■ Remove delegated tasks or change their assignments.
Delegate Other Task	Change Manager	Smart task	■ Provide a generic tasking ability for the Change Manager to use to assign tasks like testing a change ahead of implementing it. These tasks are not bound to the process state, so they do not delay the main process.
Edit Change Plan	Change Manager, selected delegates, CAB	Process Action	■ Provide non-state-sensitive elements of the change plan, such as the risk, cost, and plan elements (implementation, testing, backout). ■ Implemented as a Process Action to allow editing of a change plan at any process state, by anyone with administrative or edit rights to the process. ■ Used by the plan element delegates to provide details for their plan element.
Manage CABs	Change Manager	Process Action, Service Catalog Item	■ Add, remove, and edit CABs (available only to those with administrative rights to the process).

Table 16-1 Change Management process actions *(continued)*

Action	Initiator of Action	Type	Description
Manage Equipment	Change Manager	Process Action	■ Associate configuration items from the CMDB with the change request.
Manage related incidents	Change Manager	Process Action	■ Lets you add or remove incidents that are associated with the change request. ■ Adding incidents to a change request creates a cascading relationship, whereby the successful completion of the change triggers the closure of any associated incidents.
Manage related problems	Change Manager	Process action	■ Lets you add or remove the problems that are associated with the change request. ■ Adding problems to a change request creates a cascading relationship, whereby the successful completion of the change triggers the closure of any associated incidents.
Approve Change Plan	CAB/ECAB	Task	■ Used by the CAB to move the process to the next state. ■ Can approve or deny change plan. ■ Can add process documents
Fulfill Request	Implementer	Task	■ Used by the implementer to indicate that he or she has completed the task. ■ Can choose close code of Success or Failure. ■ Must enter comments if close code is Failure.

Configuring Change Management

You can configure change management by defining the change manager group, configuring access to the Service Catalog items, configuring access to the change request process view, setting up email templates, and configuring 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 16-2 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, depending 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. See "About the roles in Change Management" on page 193.
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. See "Creating a new change request" on page 196.

Table 16-2 Process for configuring Change Management *(continued)*

Step	Action	Description
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, 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 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" on page 192.
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. See "Configuring change request rulesets" on page 190.

Change request rulesets

Rulesets allow the administrator to configure the Change Management process. Configurations based on ticket routing, prioritization, and urgency can play a role in change requests.

The following table describes the change request rulesets that allow for routing, and prioritization.

Table 16-3 Change Request Rulesets

Ruleset	Description
OnCabApproval	Executed when the CAB approves a change plan and submits it for implementation.
OnChangeReceived	Executed when the system receives a change request. Use for routing, prioritization, auto-planning, and notification.
OnImplementationCompleted	Executed when a change has been successfully completed.
OnImplementationDateReached	Executed when the Planned Start Date for a change has been reached.
OnImplementationFailed	Executed when implementer indicates that they were unable to implement the change.
OnPlanningCompleted	Executed when the change manager (Gatekeeper) approves and submits a change request.
OnPlanRejectedByCab	Executed when the CAB rejects a change plan .
OnRequestRejectedByCm	Executed when the CM (Gatekeeper) has denied a change request.

You can configure change request rulesets.

See "Configuring change request rulesets" on page 190.

Configuring change request rulesets

You can configure change request rulesets. The set of rulesets is known as the automation library.

To configure change request rulesets

1. In the ServiceDesk portal, click **Admin > Process Automation > Automation Rules**.
2. In the **Available Services** pane, under **Change Management**, click **Rulesets Found**.
3. In the **Manage Rulesets** pane, click the **Select Ruleset** drop-down list, and select a ruleset.

   The rulesets are defined in Change Request Rulesets.

   See "Change request rulesets" on page 190.
4. On the **Ruleset*selected ruleset*** line, click the **Modify** icon on the far right, and click **Add Rule**.
5. In **Add Condition**, select a condition and enter the information related to the condition you have chosen. Click the **Plus** icon to the right to add more conditions. Check **Not** to set a condition that executes opposite to what has been selected. The Not operator only applies to the first drop-down of the rule, not to the entire rule.

   You can choose from the following conditions:

   - **Affected assets**
   - **Affected business services**
   - **Change plan type**
   - **Impact**
   - **Urgency**
   - **Any**
   - **Contacts**
6. In **Actions**, select an action you want to execute if the condition is met.

   You can choose from the following actions

   - **Send email**
   - **Set assigned CAB**
   - **Set change plan type**
   - **Set implementer**
   - **Set initial routing**
   - **Set ticket owner**

- **Set priority**
- **Set change plan template**
- **Add contact**
- **Grant ticket access**
- **Do nothing**
- **Remove ticket access**

7 Under **Parameters**, click the **Disposition** drop-down list, and select an option.

You can choose from the following items:

- **Continue**
- **Stop**

8 (Optional) Click **Advanced** and check one of the following actions that you want to include in the ruleset:

Continue 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)
Continue If Condition Fails to Execute:	If an error occurs while the condition executes, the ruleset attempts to continue executing.

9 Click **Save**.

Creating email templates

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. For more information, See "Change request rulesets" on page 190.

To create an email template

1 In the ServiceDesk portal, click **Admin > Process Automation > Automation Rulesets**.

2 In **Email Templates**, click **Add Email Template**.

3 Type a name for the email template. This name displays on the **Email Templates** section of the **Manage Rulesets** page.

4 In the **Description** box, type a description.

5 In the **From** box, type the name of the user or group sending the message.

6 Type the subject of the email in the **Subject** box.

Type a message in the **Body** box.

7 (Optional) To add additional information to certain fields, click the radio button of the field you want to add the field to, and then click the field you want to add in the **Available Fields** list.

8 Click **Save**.

About the roles in Change Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Change Management process are tasked with efficiently managing all changes to minimize the effect of any related incidents on service quality.

Table 16-4 Roles in Change Management

Role	Description
Submitter	The submitter is any worker who can request a change. Typically, the submitter is a support technician or manager, a change worker, or a problem manager. See "Sources of change requests" on page 195.
Change manager (CM)	The change manager can be anyone who is assigned to the Change Manager group. The change manager is responsible for the daily activities of the Change Management process. The change manager authorizes and documents all changes in the IT infrastructure and its components (configuration items) to reduce the amount of unplanned down time.
Change Approval Board (CAB)	The Change Advisory Board (CAB) is a group of people who can advise the change manager in the assessment, prioritization, and scheduling of changes.

See "About the Change Management process" on page 181.

Submitting change requests

This chapter includes the following topics:

Sources of change requests

The creation of a change request triggers the Change Management process. A change request can originate from several sources.

Table 17-1 Sources of change requests

Source	Description
Incident Management	A support technician or manager can create a change request as follows: ■ From an incident See "Creating a change request from an incident" on page 156. ■ From the **New Request for Change** page. See "Creating a new change request" on page 196. Support technicians typically creates change requests when they see a pattern of similar incidents.
Problem Management	If the resolution of a problem requires a fix or change, the problem manager can create a change request from a problem ticket. See "Reviewing a proposed fix or workaround " on page 223.

Table 17-1 Sources of change requests *(continued)*

Source	Description
Change Management	A change worker can create a new change request but in most cases, the change worker works on the change requests that other workers submit. A change worker can also clone an existing, completed change request. For example, if a change was made at one location, and you need to make the same change elsewhere, you can clone the original change.

Creating a new change request

A change worker or incident technician can create a change request that is not associated with other process tickets.

Creating a change request is a step in the Change Management process.

See "About the Change Management process" on page 181.

Change requests can also be created from incidents and from problem tickets.

See "Sources of change requests" on page 195.

To create a new change request

1. In the ServiceDesk portal, click **Submit Request**.
2. Under **Service Catalog**, click **ServiceDesk**.
3. On the right side of the page, click the **Request Change** link.
4. On the **Enter Change Request Details** page, enter information about the change.
5. (Optional) To attach a file to the change request, click the **Browse** button in the **Upload a File** box, select the file(s) to upload, and click **Attach**.

   You can also attach a file to the change request after it has been created.

   See "Attaching a file to an existing process ticket" on page 233.
6. When you finish entering the information, on the **Enter Change Request Details** page, click **Finish** if you are finished or click **Next** to enter more information.
7. (Optional) On the **Provide Risk Assessment** page, select a risk score from the drop-down list (Low, Moderate, High, or Very High), type a justification for the score in the **Explanation** box, and then click **Finish** or **Next**.

8 (Optional) In the **Provide Cost Information** page, type in a cost to implement and a cost not to implement, and click **Finish** or **Next**.

9 (Optional) In the **Provide Implementation Details** page, enter details on the Implementation Plan, Testing Plan, and Backout Plan, and then click **Finish** or **Next**.

10 (Optional) In the **What equipment and services are affected by this change?** page, **Search** to search the CMDB, select the item, and click **Add Selected**. When you are finished, click **Finish**.

Attach File to Change dialog box

This dialog box lets you attach one or more files to a change request to provide additional information about the change. This dialog box appears when you choose to attach a file during the change request entry.

See "Creating a new change request" on page 196.

Table 17-2 Options in the **Attach File to Change** dialog box

Option	Description
File to Add	Specify the file to add. You can add documents, spreadsheets, text files, logs, and many other file formats.
Current Attachments	Displays the files that are already attached to the ticket. The **Remove** link that appears next to each file lets you remove a file from the ticket.
Add	Adds the file to the **Current Attachments** list and lets you specify another file to attach without leaving the **Attach File to Incident** dialog box.
Continue	Adds the current attachments and closes the dialog box.

About change request templates

When you create a change request, you can use a template to fill in some of the request information. Templates are useful when you have standardized plans for rolling out periodic maintenance changes. For example, you can use a template to create requests for deploying hotfixes from Microsoft every two months. Once created, change templates are available from within the change request.

Using templates not only speeds the entry of change requests, but it also helps to standardize and increase the accuracy of the 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.

You can both create and use change request templates on the **Create New Request For Change** page.

See "Creating a new change request" on page 196.

Chapter 18

Scheduling and planning changes

This chapter includes the following topics:

- Scheduling a change request

Scheduling a change request

Scheduling a change request is a step in the Change Management process.

See "About the Change Management process" on page 181.

Before you can schedule a change, all the risk assessments must be completed.

The CM or other assigned scheduler designates a start time and duration for the proposed change. The change's schedule can be recorded in the Forward Schedule of Change.

See "About scheduling in ServiceDesk" on page 241.

After the schedule is proposed, the implementation plans must be created.

To schedule a change request

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, find and open the task to work on.
3. On the change request's **Process View** page, under **Actions**, click **Create Schedule**.

   If this action is not available, the task is probably not assigned to you. To enable this action and work the task anyway, under **Others Actions**, click **Work Tasks Assigned To Others** if that option is available.

4. On the **Propose Schedule** page, schedule the change in one of the following ways:
   - Complete the options on the page to define the schedule.
   - Click **Forward Schedule of Change**.
     Lets you view the Forward Schedule of Change.
     See "Calendar page" on page 60.
5. In **Proposed Schedule Comments**, type any remarks about the schedule.
6. (Optional) To set this change to repeat on a schedule, click **Make this a Recurring Change**, and then complete the options under **Recurring Change Details**.

   The recurring change details include information about the type and duration of the recurrence. You can also select the change process steps to skip when the change repeats, as follows:
   - **On Recurrence Skip CAB Approval**
   - **On Recurrence Skip CM Approval**
   - **On Recurrence Skip Planning**
   - **On Recurrence Skip Risk Assessment**
   - **On Recurrence Skip Scheduling**
7. On the **Propose Schedule** page, click **Submit**.
8. (Optional) On the **Process View** page, perform any of the other actions that are available as needed.
9. Close the change request's **Process View** page.

Approving and implementing changes

This chapter includes the following topics:

- Authorizing a change (CAB)
- Approving a change (change manager)

Authorizing a change (CAB)

The Change Advisory Board's (CAB's) authorization of a change request is part of the Change Management process. This step is skipped when the Emergency change type is used. Instead, the plan is assigned directly to the change manager for final approval.

After the CAB members review the plans for a change request, each member can approve or deny the plan through the voting process. When all authorizations are submitted, the approvals and denials are counted and the change is marked as approved or denied. By default, a change request is approved if the number of approvals is greater than the number of denials.

After the change is authorized, the change manager provides the final approval for implementing the change.

See "Approving a change (change manager)" on page 202.

To authorize a change

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, find and open the task to work on.
3. On the change request's **Process View** page, under **Tasks and Actions**, click **Authorize Change**.

4. On the **Authorize Change** page, review the risk assessment, impact assessment, and change schedule, and then click **Continue**.
5. On the **Plan Approval** page, view each of the plan documents, and then click **Continue**.

   If you did not view all the plan documents, you have the option to **No - View More Plans**
6. On the **Plan Approval** page, click **Yes - Continue**.
7. (Optional) On the **Change Authorization** page, click **Request Details** to view the change information once more.
8. On the **Change Authorization** page, click **Deny** or **Approve**.
9. When you finish, you can close the change request's **Process View** page.

To vote on a change

1. In the change request's **Process View** page, click **Approve Change Plan**.
2. Click **Initiate Voting**.
3. Ibn the CAB Voting wizard, type a title for the voting task in the **Set Title for Voting Task** text box.
4. Type a description for the voting task in the **Set Description for Voting Task** text box.
5. Set a priority for the voting task, and click **Continue**.

   Every member of the CAB receives a task to vote. The task appears in the change request and also in the ServiceDesk portal.

   The proxy for the CAB can view who as voted and how they voted in the **CAB Approval** page.

Approving a change (change manager)

Approving a change is part of the Change Management process.

See "About the Change Management process" on page 181.

After the change is approved, the change is implemented and tested in a test environment.

To approve a change

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, find and open the task to work on.

3 On the change request's **Process View** page, under **Actions**, click **Approve Change**.

4 On the **CM Final Review** page, review the risk assessment, impact assessment, and change schedule.

5 (Optional) In the upper left of the page, click **Request Details** to view the change information once more.

6 (Optional) Check **Mark RFC as "Unplanned"**.

   This information is for reporting purposes only. It indicates that the change was unplanned.

7 Click **Continue**.

8 After the **CM Final Review** page refreshes, click **Reject** or **Approve**.

9 Close the change request's **Process View** page.

Section 5

Managing problems

Chapter 20

Managing problems

This chapter includes the following topics:

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 "About cascading relationships among process tickets" on page 38.

About the Problem Management process

The goal of Problem Management is to minimize the effect of problems and known errors that result from systemic issues within the IT infrastructure. The Problem Management process lets you track and diagnose problems, propose actions to resolve the problems, and take action on the problem resolutions.

The Problem Management process is initiated when someone creates a problem ticket.

To identify problems, ServiceDesk workers can take the following approaches:

Proactive	A problem analyst or manager identifies problems and known issues before they occur.
Reactive	Another ServiceDesk worker reports a problem in response to one or more incidents. For example, the support manager notices a significant increase in requests to unlock user accounts.

See "About cascading relationships among process tickets" on page 38.

Table 20-1 The Problem Management process

Step	Action	Description
Step 1	Someone creates a problem ticket.	A problem ticket can be created in the following ways: ■ A problem analyst reviews incidents to find the errors that reoccur frequently and creates a problem ticket for those errors. See "Creating a new problem ticket" on page 216. ■ A support worker creates a problem ticket from within an incident. See "Creating a problem ticket from an incident" on page 154. The creation of a problem ticket creates a task for the problem analyst.

Table 20-1 The Problem Management process *(continued)*

Step	Action	Description
Step 2	The problem analyst works the problem ticket.	The problem analyst views the ticket and researches the problem. After the analysis is finished, the analyst updates the problem ticket with additional details, proposes a fix or workaround, and submits the problem for review. See "Working a problem ticket" on page 220. When the problem is submitted, a task is created for the problem reviewer.
Step 3	(Optional) A problem worker can add incidents to the problem ticket.	If the problem is related to one or more incidents, they can be associated with the problem ticket. The incidents can help to uncover root causes. Incidents can be added to a problem ticket at any time before the problem reviewer approves the fix or workaround. See "Adding incidents to a problem ticket" on page 219.
Step 4	The problem reviewer reviews the proposal.	The problem reviewer reviews the proposed fix or workaround and decides how to handle it. See "Reviewing a proposed fix or workaround " on page 223. When the proposal is accepted, the problem reviewer decides whether to create a change request, request the creation of a knowledge base article, or both. If a change request is not created, the problem is closed and the process skips to the final step. When the proposal is rejected, the problem reviewer provides a reason for the rejection. A task is created for the problem analyst, who can decide to remove the problem or rework the problem by repeating Step 2. See "Reworking a problem ticket" on page 224.
Step 5	If the problem reviewer requests a change, the problem process waits for the change process.	The change manager reviews the change request and approves or rejects it. When the change request is accepted, the Problem Management process pauses until the change is completed. If the change is rejected, a task is created for the problem reviewer. The problem reviewer decides to either remove the problem or rework the problem by repeating Step 2.

Table 20-1 The Problem Management process *(continued)*

Step	Action	Description
Step 6	The problem is closed.	The problem ticket can be closed in the following ways: ■ The problem reviewer accepts the problem proposal, chooses to request a knowledge base article, and closes the problem ticket. ■ All changes that are associated with the problem are completed. The closure of the problem triggers a cascading closure, in which the changes and the incidents that are associated with the problem are closed. Any incidents that are associated with those changes are also closed.

Problem statuses

The problem status accurately reports the progression and outcome of the stages of the Problem Management process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the ServiceDesk portal. For example, they appear at the top of the ticket's **Process View** page.

Table 20-2 Problem statuses

Status	Description	Completion percentage
Analyze New Problem	The problem ticket is in a waiting state for the problem analyst to review the ticket and propose a resolution.	5%
Awaiting proposal review.	The problem analyst proposed a resolution and submitted the problem ticket, which is in a waiting state for the problem reviewer to review the ticket.	50%
Waiting on Change Management	A change was requested to resolve the problem, which is in a waiting state for the completion of the change process.	75%
Closed	The problem process is complete. The closure occurs when the problem analyst or reviewer closes the problem ticket or all the changes that are associated with the release are closed.	100%
Schedule Change has been submitted	A change request is submitted to resolve the problem.	85%

Table 20-2 Problem statuses *(continued)*

Status	Description	Completion percentage
Create Document	A fix or workaround for the problem is submitted as a new knowledge base article request	80%
Solution was rejected	The problem reviewer rejected the problem and returned it to the problem analyst. The problem ticket is in a waiting state for the problem analyst to rework or remove the problem.	5%
Exception	The SLA time was surpassed.	85%

Roles in Problem Management

Depending on their structure, some organizations might have different hierarchy levels and multiple roles for Problem Management. ServiceDesk contains two default groups for Problem Management: Problem Analyst and Problem Reviewer.

Table 20-3 Roles in Problem Management

Role	Description
Problem analyst	Analyzes the root cause of the problem, proposes a solution, and submits the proposal. The proposal can be in the form of a fix or a workaround. Analysts can also remove the problem. In many organizations, the same person fills both the problem analyst and the problem reviewer roles. However, in larger organizations the problem analyst role is assigned to one or more people other than the problem reviewer.
Problem reviewer	Approves the proposed fix or workaround and decides how to handle the problem, or returns the problem to the problem analyst for rework.

ITIL recommends that the same person should not be involved in both Problem Management and Incident Management. The priorities of those processes are not always consistent with each other.

Sources of problem tickets

The creation of a problem ticket triggers the Problem Management process. A problem ticket can originate from several sources.

Table 20-4 Sources of problem tickets

Source	Description
ServiceDesk portal	A problem analyst or other ServiceDesk worker creates a problem ticket from the **Submit a Problem** link in the Service Catalog.
Incident Management	A support worker creates a problem from the **Create Problem Ticket** action in an incident's **Process View** page.

Email notifications from Problem Management

ServiceDesk sends email notifications at various stages of the Problem Management process. In this context, a problem event is any action that is taken to create or work a problem ticket. The type of event and the ServiceDesk configurations determine the recipients of the email notifications.

The email notifications from incidents, discussions, and problems can process replies to the notifications and add them to the history of the related ticket.

Replies are processed in the following situations:

- The email notification is sent from a process. Such emails contain an identifier to trigger the response.
- The email notification is sent from a template and the ServiceDesk worker selected the option to include a reply code.

Table 20-5 Default problem events that trigger email notifications

Event	Email recipient
A problem ticket is created.	The submitter and the primary contact, if they are not the same person
A problem worker starts a chat.	The person who is invited to chat
A problem worker decides to handle the problem by creating a knowledge base article.	The knowledge base editor The email message requests an article that describes how to handle the problem.

Process View page for problem tickets

The **Process View** page is the primary interface for working a task. The **Process View** page appears when you select a task from your **Task List** or from another list in the ServiceDesk portal.

The default sections on the **Process View** page are similar for all types of tasks. If your organization uses customized **Process View** pages, your views might look different.

See "Process View page" on page 89.

In addition to the common actions that you can perform for all tasks, the problem **Process View** page contains additional, problem-specific actions. The actions that are available depend on your permissions and the state of the problem ticket. For example, the **Review Fix or Workaround** action appears only after the problem ticket is reviewed and analyzed.

Table 20-6 Actions on the problem ticket's **Process View** page

Action	Description
Add Incident	Lets you add one or more incidents that are related to the problem. See "Adding incidents to a problem ticket" on page 219.
Add/Manage Bulletin Boards	Lets you manage bulletin boards, if you have permission to do so. It also lets you create a bulletin board entry.
Assignments	Lets you assign the ticket to another user, group, or organization. This action appears under **Actions** on the task pop-up that appears when you click the task in the **History** section.
Change Priority	Lets you change the problem ticket's priority. For example, after a problem is created, many incidents that are related to the problem are submitted. In this situation, you might change the problem's priority to a higher level.
Edit Description	Lets you describe the problem accurately. For example, when you create a problem from an incident, the problem inherits the incident's description. However, the incident's description is likely to be user-specific while the problem typically represents a more general issue.
Go To Discussion	Lets you view and add to the posts in a discussion about the problem. A discussion is formed when a problem is created. See "About discussions in the Problem Management process" on page 215.
Invite Participant	Lets you invite another user to become a contact on the problem. You can also choose whether to send an email to notify the user of the addition.

Table 20-6 Actions on the problem ticket's **Process View** page *(continued)*

Action	Description
Manage Equipment	Opens the **Add Equipment** dialog box, which lets you add or delete the equipment that is related to the process. You can also access the quick tools for a piece of equipment.
Remove Problem	Displays the **Remove Problem** page, where you must provide a detailed reason for the deletion. Examples of why you might remove a problem are as follows: ■ You determine that the issue is not a problem and does not require further processing. ■ You determine that this issue is related to or is a duplicate of another problem. In this situation, you can choose to move any attached incidents to another problem ticket.
Review Fix Or Workaround	Lets you review the proposed fix or workaround, determine how to handle the problem, and approve the problem or return it to the analyst. See "Reviewing a proposed fix or workaround " on page 223.
Search KB	Lets you search the knowledge base for an article that is related to the ticket and then attach the article. See "Searching the knowledge base" on page 281.
Send Email	Lets you send an email message regarding the ticket. See "Sending an email from a process ticket" on page 317.
View Problem	Lets you view the details of the problem ticket and select the options that appear under **Other Actions**. For example, you can send emails or participate in a discussion.
Work Problem	Lets you perform the following actions: ■ Resume work on a ticket that you started and then saved without completing. The ticket is saved as a draft and a task is created to complete the ticket. ■ Update a problem ticket to provide the cause and a detailed description of the problem. You can also categorize the problem and propose a workaround or a fix. See "Working a problem ticket" on page 220.

About discussions in the Problem Management process

You can use discussions to help you research or resolve a problem. Discussions are started automatically from within the Problem Management process.

When a problem ticket is created, the problem's name and ID become the title of the new discussion. The problem's description becomes the discussion's description. Anyone who works the problem can use the **Go to Discussion** smart task to create posts and view any posts that have been made for the problem.

See "About discussions in the ServiceDesk portal" on page 329.

See "Creating a new problem ticket" on page 216.

Creating a new problem ticket

Create a problem ticket to initiate the process of taking measures to prevent an issue that can lead to incidents in your organization. Creating a problem ticket is the first step in the Problem Management process.

See "About the Problem Management process" on page 209.

A problem ticket can also be created from an incident, which creates an association between the incident and the problem.

See "Creating a problem ticket from an incident" on page 154.

When the problem ticket is created, a new discussion is created and associated with the problem.

See "About discussions in the Problem Management process" on page 215.

After the problem ticket is created, the problem analyst works the ticket by entering the results of the analysis and proposing a fix or workaround

See "Working a problem ticket" on page 220.

To create a new problem ticket

1. In the ServiceDesk portal, click **Submit Request**.
2. Under **Service Catalog**, click **ServiceDesk**.
3. On the right side of the page, click **Submit a Problem**.
4. (Optional) To attach one or more incidents to the problem ticket, on the **Create Problem** page, take the following steps:
   - In **Search for**, type the search text to evaluate against incident descriptions, and then click the **Search** symbol.
     Incidents that are already attached to a problem do not appear in the search results.
   - Under **Incidents with Possible Relation to Current Problem**, click the **Add** link to the right of each incident to attach, or click **Add All Listed** to add all the incidents that you found.

   See "Create Problem page" on page 217.

5 (Optional) If you choose not to attach any incidents, on the **Create Problem** page, click **Verify you are not attaching incidents**.

6 On the **Create Problem** page, click **Create a New Problem**.

7 On the **Submit a New Problem** page, define the problem, and then click **Continue**.

See "Submit a New Problem page" on page 218.

8 On the **Review New Problem** page, verify that the information is correct, remove incidents if necessary, and then select one of the following options:

Close Without Saving	Cancels your entry without creating a problem ticket.
Back to Incident Search	Returns to the **Create Problem** page, where you can add or remove incidents. Repeat from step 4.
Create Problem	Creates the problem ticket.

9 On the **Submission Complete** page, click **Close**.

Create Problem page

This page lets you define the incidents to attach to a new problem ticket. You can also choose not to attach incidents.

See "Creating a new problem ticket" on page 216.

See "Adding incidents to a problem ticket" on page 219.

Table 20-7 Options on the **Create Problem** page

Option	Description
Search for	Lets you find one or more related incidents to attach to the problem ticket. The search text that you enter is evaluated against the text in the incident's description or title. For example, if several users could not access a network printer, you might search for all incidents that are related to the network printer.
Incidents with Possible Relation to Current Problem	Displays the search results and lets you review each incident or add it to the problem ticket. Incidents that are already attached to a problem do not appear in the search results.

Table 20-7 Options on the **Create Problem** page *(continued)*

Option	Description
Currently Added Incidents	Lists the incidents that you add to the problem ticket.
Add All Listed	Adds all the incidents that are listed under **Incidents with Possible Relation to Current Problem** to the problem ticket.
Remove all listed	Removes all the incidents that are listed under **Currently Added Incidents** from the list.
Add to Existing Problem	Lets you select an existing problem to attach the incidents to.
Create New Problem	Creates a problem ticket.
Verify you are not attaching incidents.	Lets you choose not to attach incidents to the problem ticket. However, because it is more typical to attach tickets, you must verify your choice not to do so.

Submit a New Problem page

This page lets you define the details of a problem. It appears during the creation of a new problem ticket.

See "Creating a new problem ticket" on page 216.

Table 20-8 Options on the **Submit a New Problem** page

Option	Description
Primary Contact	Lets you specify the primary contact for the problem ticket. Typically, the primary contact is the person who encounters or reports the problem.
Search for User	Opens the **Select User** page, where you can specify the person who this problem affects. This link appears only when you specify that this problem affects someone else.
Title	Becomes the title that identifies the problem in the ServiceDesk portal. Make the name descriptive enough for you and others to easily understand the nature of the problem.

Table 20-8 Options on the **Submit a New Problem** page *(continued)*

Option	Description
Detailed description of the problem	Lets you type additional information to describe the problem. For example, you might describe the steps to reproduce the problem or provide information about what happens as a result of the problem.
Cause of the problem	Lets you describe what causes the problem.
Business Impact	Lets you define the extent of the problem by specifying how many people are affected. See “Default priority, urgency, and impact values” on page 373.
Urgency	Lets you specify how much the problem affects the submitter or the primary contact. See “Default priority, urgency, and impact values” on page 373.

Adding incidents to a problem ticket

If a problem is related to one or more incidents, you can associate the incidents with the problem ticket. You might add the incidents that triggered the problem process, or you might add the related incidents that you discover during the problem analysis.

Adding incidents to a problem ticket is an optional step in the Problem Management process. You can add incidents to a problem ticket at any time before the proposed fix or workaround is approved.

See “About the Problem Management process” on page 209.

To add incidents to an existing problem ticket

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.Problem Management**.
3. In the list of tasks, find and open the task to work on.
4. On the ticket’s **Process View** page, expand **My Actions**, expand **Smart Tasks**, and then click **Add Incident**.
5. In the **Associate Incidents** page, in **Search for**, type the search text, and then click the **Search** symbol.
6. In the list of search results, click the **Add to Problem** link to the right of each incident to attach.

7. When you finish adding incidents, click **Close**.
8. When the ticket's **Process View** page reappears, you can continue to work the ticket or close it.

Working a problem ticket

After you analyze a problem, you update the problem ticket to provide the cause and a detailed description of the problem. You also categorize the problem and propose a fix or a workaround.

You can also use the actions that are available in the ticket to help with your research. For example, you can communicate with other users by opening a chat session or posting to the discussion that is associated with the problem.

Working a problem ticket is a step in the Problem Management process.

See "About the Problem Management process" on page 209.

After you propose a resolution to the problem, the problem reviewer views and takes action on the proposal.

See "Reviewing a proposed fix or workaround " on page 223.

To work a problem ticket

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.Problem Management**.
3. In the list of tasks, find and open the task.
4. On the ticket's **Process View** page, under **My Actions**, click **Work Problem**.
5. On the **Examination and Analysis** page, record the results of your analysis.
6. When you finish describing the analysis, select one of the following options:
   - **Save and Close**
     Saves the information and closes the page. Use this option when you plan to continue to work the problem later.
   - **Propose a Workaround**
   - **Propose a Fix**

   See "Propose Workaround page, Propose a Fix page" on page 222.
7. On the **Propose Workaround** page or the **Propose Fix** page, enter information about the proposal, and then click **Submit Proposal**.
8. When the ticket's **Process View** page reappears, you can continue to work the ticket.

Examination and Analysis page

This page lets you record the results of your problem analysis. It appears when you select **Work Problem** on a problem ticket's **Process View** page.

See "Working a problem ticket" on page 220.

Table 20-9 Options on the **Examination and Analysis** page

Action	Description
Classification **Click here to classify**	Lets you select a classification for the problem. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification. You can select from several default classifications as well as any custom classifications that your organization added.
Root Cause	Lets you describe what you think is the cause of the problem. This option defaults to the text from the problem entry and lets you type additional text.
Category	Lets you select the category that the problem belongs to. The default categories are as follows: ■ **Add/Install** ■ **Break/Fix** ■ **Request**
Business Services Affected	Lets you select one or more business services that the problem affects. If the problem originated from an incident, any business service that is associated with the incident appears as a related item on the **Process View** page.
Problem Description	Contains the text from the problem entry and lets you type additional text.
Supporting Documents **Add File** **Remove File**	Lets you attach documents or other files that provide additional information about the problem. For example, you can attach error logs.
Add Location	Lets you specify the location that the problem affects. The location is for informational purposes only. When you click this link, the **Location Affected** page appears. It displays your default location but you can change it when you report the problem from a different location.
Save and Close	Saves the information and closes the page. Use this option when you plan to continue to work the problem later.

Table 20-9 Options on the **Examination and Analysis** page *(continued)*

Action	Description
Propose a Workaround **Propose a Fix**	Lets you document a workaround or a fix to a problem. See "Propose Workaround page, Propose a Fix page" on page 222.

Propose Workaround page, Propose a Fix page

These pages let you document a workaround or a fix to a problem. They appear when you work a problem ticket.

See "Working a problem ticket" on page 220.

Table 20-10 Options on the **Propose a Workaround** and **Propose a Fix** pages

Action	Description
Classification **Click here to classify**	Lets you change the problem's classification. Depending on the classification that you select, additional classification links might appear to let you narrow the scope of the classification. You can select from several default classifications as well as any custom classifications that your organization added.
Category	Read-only.
Workaround Instructions **Detailed Fix Instructions**	Lets you type instructions for performing the workaround or fix.
Details	(Read only) Contains the text from the problem entry.
Business Impact	Lets you define the extent of the problem by specifying how many people are affected. See "Default priority, urgency, and impact values" on page 373.
Urgency	Lets you specify how much the problem affects the submitter or the primary contact. See "Default priority, urgency, and impact values" on page 373.
Priority	Lets you select the priority for resolving this problem. See "Default priority, urgency, and impact values" on page 373.

Table 20-10 Options on the **Propose a Workaround** and **Propose a Fix** pages *(continued)*

Action	Description
Submit Proposal	Submits the fix or workaround to the problem reviewer for approval.

Reviewing a proposed fix or workaround

After a problem analyst proposes a solution to a problem, you can review the proposal and accept or reject it. When you accept a proposal, you can decide whether to create a change request, request the creation of a knowledge base article, or both. When you reject a proposal, you return the problem to the problem analyst, who can remove the problem or provide additional information and resubmit it.

Reviewing a fix or workaround is a step in the Problem Management process.

If you submit a change request after your review, a problem task with the status **Waiting for Change Request to Complete** appears in the task list. This task cannot be worked; it is a reminder that the problem is on hold pending the completion of the change request.

See "About the Problem Management process" on page 209.

To review a fix or workaround

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.Problem Management**.
3. In the list of tasks, find and open the task.
4. On the ticket's **Process View** page, under **My Actions**, click **Review Fix Or Workaround**.
5. On the **Review Proposal** page, review the information about the proposed workaround or fix.
6. In **How this Problem will be Handled**, select one of the following options:
   - **Create KB Article**
     Creates a new request for a knowledge base article and sends a notification email to the knowledge base editor.
   - **Create Change Ticket**
     Lets you create a change request from this problem ticket.
   - **Create Change and Article**

7 Select one of the following options:

- **Close**
  Saves the information and closes the page.
- **Return Problem to Analyst**
  Go to step 8.
- **Approve proposal**
  Go to step 9.

8 If you chose to return the problem to the analyst, on the **Return to Analyst** page, provide the reason for returning the problem, and then click **Submit**.

See "Reworking a problem ticket" on page 224.

9 If you chose to create a change request, on the **Submit Change Request** page, provide the information for the change ticket, and then click **Submit Change Request**.

See "Submit Change Request page" on page 224.

10 When the ticket's **Process View** page reappears, you can close it.

Submit Change Request page

This page lets you provide the information for a change ticket that you create from a problem ticket. It appears when you choose to create a change ticket during the problem review task.

See "Reviewing a proposed fix or workaround " on page 223.

Table 20-11 Options on the **Submit Change Request** page

Option	Description
Change Description	Lets you describe in detail the change that needs to be made.
Change Needed By	Lets you specify when the change must be made.
Priority	Lets you specify the priority for the change request.
Submit Change Request	Creates a change request ticket and assigns it to the change queue.

Reworking a problem ticket

During the review of a problem ticket, the problem reviewer can choose to return the problem to the analyst. The reviewer provides guidance to the analyst by including a reason for the rejection. For example, the reviewer might request a more detailed workaround description, or decide that a change is required instead of a workaround.

See "Reviewing a proposed fix or workaround " on page 223.

The problem analyst can rework the problem ticket to provide the information that the reviewer requested. The analyst can also remove the problem ticket at the reviewer's recommendation or as a result of additional research.

If the analyst removes the problem, the process ends and triggers a cascading closure of any changes and incidents that are associated with the problem.

To rework a problem ticket

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.Problem Management**.
3. In the list of tasks, find and open the task.
4. On the ticket's **Process View** page, under **My Actions**, click **Work Problem**.
5. On the **Rejection Reason** page, review the problem reviewer's comments, and then select one of the following options:.

Close	Saves the problem and closes the page. Select this option if you plan to take either of the following actions: ■ Resume work on the problem later. ■ Remove the problem ticket. This option itself does not remove the problem ticket. However, it lets you return to the problem's **Process View** page, from which you can access the **Remove Problem** smart task.
Rework Proposal	Opens the **Examination and Analysis**, where you can continue to work the problem as usual. See "Working a problem ticket" on page 220.

Section 6

Working with process tickets

Chapter 21

Performing common ticket actions

This chapter includes the following topics:

About restricting access to open tasks (leasing)

To prevent multiple workers from changing a task at the same time, ServiceDesk can restrict access to the task while someone works on it. This process is referred to as leasing.

The administrator can enable and configure settings for leasing in the Portal Master Settings.

If leasing is enabled, when a worker opens a task and takes a specific action, the task is immediately leased to that worker. For example, an incident task is leased as soon as the worker begins to escalate it. No other worker can work on that task until the lease is released or broken. The option to work on the incidents that are assigned to others does not override a lease.

A lease is released or broken in the following situations:

- The leasing worker closes the task.

- The maximum allowable lease time passes.

  The administrator configures the setting that determines the amount of time that a task can be leased from the time that the lease begins. After a task has been leased for that amount of time, the lease is released automatically, even if the worker has not completed the task.

- The administrator breaks the lease.

  The administrator can open a leased task and break its lease. For example, a worker begins work on an emergency task and then leaves their desk before the task is completed. Another worker sees the task on the **Process View** page and notices that it is leased. The second worker notifies the administrator to break the lease. After the lease is broken, the second worker or the administrator can finish the task.

  See "Breaking the lease on a task" on page 230.

Other workers can see leased tasks on the **Process View** page. They can also see leased tasks in their task lists if the administrator enabled the setting to allow leased items to appear there. When a leased task is opened, a message on the task page identifies it as leased. Other workers can view the task's details but cannot make any changes.

Breaking the lease on a task

If leasing is enabled, when a worker opens a task and takes a specific action, the task is immediately leased to that worker. No other worker can work on that task until the lease is released or broken.

See "About restricting access to open tasks (leasing)" on page 229.

The administrator can open a leased task and break its lease.

To break the lease on a task

1. In the ServiceDesk portal, open the task.
2. Under **History**, at the right of the current task line, click the green down arrow symbol.
3. On the new page, under **Actions**, click **Break Lease**, and then close the page.
4. (Optional) Work the task yourself or let someone else work it.
5. Close the task window.

About the process time for tickets

Process time represents the amount of time that it takes to work on and resolve a process ticket. The process time is used for reporting purposes. For example, you might need to report the time that was spent on a specific customer's incidents. You might also track how much time certain kinds of incidents take to resolve, to help you analyze whether to create a problem ticket.

ServiceDesk can track either the entire time that a process ticket is open or only the time that someone actively works on it. A setting in the ServiceDesk installation determines how the time is tracked.

ServiceDesk process workers can also record the time that they spend on a ticket offline, which ServiceDesk cannot record automatically. Process time is not recorded during the ticket creation.

See "Posting process time to a ticket" on page 231.

ServiceDesk tracks the following times:

- **Current User Process Time**
  The amount of time that accumulates for the worker who has the **Process View** page open.
- **User Process Time**
  The total amount of offline time that workers have posted to the ticket to date.
- **Total Process Time**
  The amount of time that was spent on the ticket to date, including the time that was recorded automatically and the time that workers posted.

A ticket's process time appears on the **Process View** page, under the top section that contains the ticket's statistics and under the **Process Time** section.

Posting process time to a ticket

ServiceDesk tracks the amount of time that a process ticket is open or worked on and adds it to the ticket's total process time. However, ServiceDesk cannot automatically record the time that process workers spend on a ticket offline. For example, a support technician might spend time researching an issue or trying to reproduce the issue. You can add the time that you spend offline to a ticket's total process time.

See "About the process time for tickets" on page 231.

You can post time on the process ticket's **Process View** page. For incidents, you can also post time on a page that appears during the incident resolution.

See "Resolving an incident from a task" on page 150.

To post process time to a process ticket

1. In the ServiceDesk portal, find and open the task on which you spent time.
2. On the process ticket's **Process View** page, expand the **Process Time** section, and then click **Post Process Time**.
3. On the **Post User Time** page, enter the amount of time that you spent on the process ticket offline and an optional description, and then click **Save**.
4. When you are returned to the process ticket's **Process View** page, you can continue to work the ticket or close it.

Performing actions on multiple tickets

In the ServiceDesk portal, you can perform certain actions on a group of process tickets at one time. For example, you can add a comment to multiple process tickets or reassign a group of tickets.

The option to perform group actions can appear on any portal page that contains a list of process tickets. By default, the option appears on the **Home** page, **My Task List** page, and **Tickets** page.

You can also choose to close a group of incidents. This option is available on the Service Catalog.

See "Closing multiple incidents" on page 156.

To perform an action on multiple tickets

1. In the ServiceDesk portal, go to any page that contains a list of tickets.

   For example, a task list appears on the following portal pages: **Home**, **My Task List**, and **Tickets**.
2. On the portal page, click in the **Select a group action** drop-down list, and then select the action to take.
3. After the screen refreshes, click the check box to the left of each ticket to act on.
4. Under **My Open Tickets**, click **Do action**.
5. The action that you select determines what happens next. If a dialog box appears, complete the dialog box.

Attaching a file to an existing process ticket

You can attach one or more files to a process ticket to provide additional information to support the ticket. For example, you can attach an error log file or a screen image that you captured.

Files larger than 4 MB are not supported.

The files that you attach to a process ticket are added to the Document Management system. In the ServiceDesk portal, on the **Documents** page, the files appear in a folder whose name is the process ID.

See "Documents page" on page 59.

To attach a file to an existing process ticket

1. In the ServiceDesk portal, find and open the ticket to attach a file to.
2. On the process ticket's **Process View** page, expand the **Documents** section, and then click **Add Attachments**.
3. In the **Add Documents** dialog box, on the **Documents Information** tab, in **File**, type or browse to the file to attach.
4. (Optional) Click the **Optional** tab and enter additional information about the file as follows:

Document Type	Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can attach any type of file even if it is not listed.
Override Name	Identifies this file in any list of documents in the ServiceDesk portal. Make the name descriptive enough for you and others to easily understand the purpose of the file. If you do not provide a name, the file name is used.
Description	Provide additional information to describe the file and its contents.

5. When you finish entering the document information, click **Save**.

Assigning and delegating process tickets

This chapter includes the following topics:

Reassigning incidents, problems, or change tickets

ServiceDesk incidents, problems, and change tickets can be assigned to another entity such as a user, group, permission, or organizational unit. For example, if an employee is out of the office unexpectedly, you can reassign that employee's tickets to someone else.

You can assign a ticket to multiple users, groups, permissions, and organizational units.

If you need to reassign the incoming tickets for an employee, you can use the delegation function.

See "Delegating your tickets to another user" on page 238.

See "Delegating a user's tickets to another user" on page 237.

To reassign an incident, problem, or change ticket

1. In the ServiceDesk portal, open the ticket to reassign.
2. On the ticket's **Process View** page, under **History**, click the task's name.
3. On the ticket's **Workflow Task Details** page, under **Actions**, click **Assignments**.
4. In the **Edit Assignments** dialog box, in **Assign To**, select a user, group, permission, or organizational unit.
5. In **User**, **Group**, **Permission**, or **Organization**, type the name of the entity to assign the ticket to.

   You can also click **Pick** to select the appropriate entity.
6. If you clicked **Pick**, in the **Picker** dialog box, select a specific entity as follows:

User Picker dialog box	Select a user. See "Picking a user" on page 96.
Group Picker dialog box	Click the **select** link to the right of the appropriate group.
Permission Picker dialog box	Click the **select** link to the right of the appropriate permission.
Organisation Picker dialog box	Expand the organizations if necessary, and then click an organization.

7. (Optional) In **Assign From** and **Assign To**, specify a start date and end date for the assignment.

   When the end date passes, if the incident is still not resolved, it is escalated automatically.
8. Click **Add**.
9. Repeat step 4 through step 8 to add additional assignments if necessary.
10. To remove any assignees, click the red X next to the assignment record, and then click **OK** in the confirmation dialog box.
11. When you finish editing the assignments, click **Close**.

Edit Assignments dialog box

This dialog box lets you reassign a process ticket to another entity such as a user, group, permission, or organizational unit.

You can assign a ticket to multiple users, groups, permissions, and organizational units.

See “Reassigning incidents, problems, or change tickets” on page 235.

Table 22-1 Options in the **Edit Assignments** dialog box

Option	Description
Delete  symbol	Lets you delete any of the current assignees that appear at the top of the dialog box.
Assign To (Drop-down list)	Lets you select the entity to assign the task to. You can assign a task to a user, group, permission, or organizational unit.
User **Group** **Permission** **Organization**	Lets you type or select the name of a specific assignee.
Pick	Opens a **Picker** dialog box, which lets you search for a specific assignee.
Assign From **Assign To**	(Optional) specify a start date and end date for the assignment. When the end date passes, if the incident is still not resolved, it is escalated automatically.
Add	Adds the selected assignee without closing the dialog box.

Delegating a user’s tickets to another user

The delegation function lets you route all the incoming tickets for one user to another user for a specified period. For example, you might delegate incoming tickets when a user is on leave or vacation, or is otherwise unable to work their tickets.

The administrator or another user with the appropriate permissions typically performs this task.

If you need to reassign existing tickets to someone else, you can use the reassignment function.

See “Reassigning incidents, problems, or change tickets” on page 235.

To delegate a user’s tickets to another user

1. In the ServiceDesk portal, select **Admin > Users > Manage Delegations**.
2. In the **Delegations** section, click the **Add Delegation** symbol (green plus sign).
3. In the **Add Delegation** dialog box, specify the following information:
   - The user whose tickets you plan to delegate.
   - The user to whom you plan to delegate the tickets.
   - The starting date and ending date of the delegation period.

   See “Add Delegation dialog box” on page 239.
4. Click **Save**.

Deleting a ticket delegation

Delegations route all the incoming tickets for one user to another user for a specified period.

A delegation expires on its specified end date, and the tickets resume being routed to the original user’s queue. If you need to end a delegation early, you can delete the delegation.

The administrator or another user with the appropriate permissions typically performs this task.

To delete a ticket delegation

1. In the ServiceDesk portal, click **Admin > Users > Manage Delegations**.
2. In the **Delegations** section, click the **Delete** symbol (red X) that appears next to the delegation to delete.
3. In the confirmation message, click **OK**.

Delegating your tickets to another user

Delegations route all the incoming tickets for one user to another user for a specified period. You can use delegation to ensure that someone else handles the incoming tickets that are assigned to you while you cannot work on them. When the end date for the delegation passes, the tickets resume being routed to your queue.

For example, you might set up a delegation during your vacation time and set the end date for when you plan to return to work.

If you need to reassign existing tickets to someone else, you can use the reassignment function.

See "Reassigning incidents, problems, or change tickets" on page 235.

To delegate your tickets to another user

1 In the upper right of the ServiceDesk portal, click **Account**.

2 Scroll to the **Manage Delegations** section, and then click the **Add Delegations** symbol (green plus sign).

3 In the **Add Delegation** dialog box, specify the following information:

   - The user whose tickets you plan to delegate.
   - The user to whom you plan to delegate the tickets.
   - The starting date and ending date of the delegation period.

   See "Add Delegation dialog box" on page 239.

4 Click **Save**.

Add Delegation dialog box

This dialog box lets you route all the incoming tickets for one user to another user for a specified period.

See "Delegating a user's tickets to another user" on page 237.

See "Delegating your tickets to another user" on page 238.

Table 22-2 Options in the **Add Delegation** dialog box

Option	Description
Delegate From	Lets you specify the user whose tickets you plan to delegate. You can also click **Pick** to select the appropriate user. See "Picking a user" on page 96.
Delegate To	Lets you specify the user to delegate the tickets to. You can also click **Pick** to select the appropriate user. See "Picking a user" on page 96.
From	Lets you specify the date on which the ticket delegation begins.

Table 22-2 Options in the **Add Delegation** dialog box *(continued)*

Option	Description
Until	Lets you specify the date on which the ticket delegation begins.

Chapter 23

Managing the ServiceDesk schedule

This chapter includes the following topics:

About scheduling in ServiceDesk

In ServiceDesk, schedules record various date-related events and functions in a calendar-like structure that is called the Forward Schedule of Change.

The Calendar is an integrated view of all the approved changes and their release dates. This schedule lets the change manager plan changes and releases that coordinate with the existing schedule. When you consider the scheduled events together instead of in isolation, you can avoid unforeseen conflicts.

The schedule also provides the information that you can use to communicate planned downtime to management and the users who the implementation affects.

Table 23-1 Elements of the Calendar

Element	Description
Schedules	A group of entries that are of a specific type. Each schedule contains entries for the events of the appropriate type. For example, the **Changes Waiting for Release** schedule contains entries for the changes that are approved and that need to be included in a release. All the entries in the individual schedules are combined on a single calendar. ServiceDesk contains the following default schedules: ■ **Changes Waiting for Release** ■ **Scheduled Changes** See "Scheduling a change request" on page 199. ■ **Scheduled Releases** You can use the default schedules and you can add customized schedules. See "Creating a new schedule" on page 244.
Schedule entries	The scheduled time for a specific event. A schedule entry is associated with a schedule. The Change Management process updates the schedules directly. The process places the entry in the appropriate schedule based on the status of the process ticket. Schedule entries can also be entered manually. For example, you might add a company meeting, a training session, or other non-process event that can affect the process-related schedules. See "Adding an entry to the schedule" on page 245.
Calendar	A page that displays the schedule entries. You can display the entries for all the schedules or for only the schedules that you select. The format options for viewing the schedule are as follows: ■ **Today** ■ **Three Days** ■ **Work Week** ■ **Week** ■ **Month** ■ **Gantt View** Displays the schedule in a Gantt style so that you can see other task dependencies in one view. You can select a start date and an end date, and then click **Go** to display the interactions.

Viewing the ServiceDesk schedule

You can view the **Calendar** page to review an integrated view of all the approved changes and their release dates.

See “Calendar page” on page 60.

The schedule is also visible when you view or schedule a process ticket.

To view the ServiceDesk schedule

1. In the ServiceDesk portal, click **Calendar**.
2. Under **Schedules**, check the check box for each schedule to display and uncheck the check box for each schedule to hide.

   You can check or uncheck the check boxes at any time and the schedule display changes immediately.
3. To change the display color for a specific schedule, select a color from the drop-down list to the right of the schedule name.
4. To change the format of the schedule display, click one of the following options:
   - **Today**
   - **Three Days**
   - **Work Week**
   - **Week**
   - **Month**
   - **Gantt View**
     Displays the schedule in a Gantt style so that you can see other task dependencies in one view. You can select a start date and an end date, and then click **Go** to display the interactions.
5. To move the display forward or backward in time, click the arrows that appear at the far right and far left on the schedule heading.

Searching for a schedule entry

When you need to find a specific schedule event, you can search the Calendar. The search checks both the title and description for the search text. The search results and their start dates and end dates appear in the right pane of the Calendar page.

See “Calendar page” on page 60.

To search for a schedule entry

1. In the ServiceDesk portal, click **Calendar**.
2. Under **Search Schedule Entry**, enter one or more words from the entry’s title or description, and then click the **Search** symbol.

Creating a new schedule

In ServiceDesk, a schedule represents a certain type of schedule entry. For example, the **Scheduled Changes** schedule contains entries for the changes that have been approved and assigned a release date.

You can create additional schedules to extend the organization of schedule entries. For example, each location or organizational unit can have its own schedule.

When you create a new schedule, it appears in the ServiceDesk portal on the **Calendar** page.

To add a schedule

1. In the ServiceDesk portal, click **Calendar**.
2. At the right of the **Schedules** section, click the **Add Schedule** symbol (a white page with a green plus sign).
3. On the **Add Schedule** page, define the schedule.

   See "Add Schedule dialog box" on page 244.
4. To add permissions to the schedule, click **Add New Permissions**, and then complete the information on the **Permissions** page that appears.

   See "Setting permissions" on page 95.
5. When you finish defining the schedule and its permissions, click **Save**.

Add Schedule dialog box

This dialog box lets you create a new schedule in the Forward Schedule of Change. In ServiceDesk, a schedule represents a certain type of schedule entry. For example, the **Scheduled Changes** schedule contains entries for the changes that have been approved and assigned a release date.

See "Creating a new schedule" on page 244.

The **Add Schedule** dialog box contains the following tabs:

Schedule Information	Lets you define the schedule. See Table 23-2 on page 245.
Permissions	Lets you set the permissions for accessing this schedule. See "Setting permissions" on page 95.

Table 23-2 Options on the **Add Schedule Information** tab

Option	Description
Name	Identifies this schedule in any schedule list or display in the ServiceDesk portal. For example, if this schedule is for a specific location, you might use the location name.
Description	Lets you provide additional information to describe the schedule.
Color	Lets you select the color in which to display the items that appear in this schedule.
Process Notifications	Sends the email notifications when events occur on this schedule. For example, notifications can be sent when a schedule entry is added, edited, or deleted. The notifications are sent to those who have notify permissions for this schedule. This option is selected by default.

Adding an entry to the schedule

A schedule entry represents the scheduled time for a specific event in ServiceDesk. For example, an entry can represent a change or a release. Most event entries are created through the ServiceDesk processes. However, you can add an event to the schedule manually. For example, you might add a company meeting, a training session, or other non-process event that can affect the process-related schedules.

The entries that you create appear on the Forward Schedule of Change.

See "Calendar page" on page 60.

To add an entry to the schedule

1. In the ServiceDesk portal, click **FSC**.
2. At the right of the **Schedule Entries** section, click the **Add Entry** symbol (a white page with a green plus sign).
3. In the **Add Entry** dialog box, on the **Entry Information** tab, define the schedule entry.

   See "Add Entry dialog box" on page 246.
4. To apply a profile value to the entry, on the **Profiles** tab, click **RC Implementers and Testers**.

5 When you finish defining the schedule entry, click **Save**.

Add Entry dialog box

This dialog box lets you define an event that you add to a schedule in ServiceDesk.

See "Adding an entry to the schedule" on page 245.

The **Add Entry** dialog box contains the following tabs:

Entry Information	Lets you define the event entry. See Table 23-2 on page 245.
Profiles	Lets you apply a profile value to the entry by clicking **RC Implementers and Testers**. See "Setting permissions" on page 95.

Table 23-3 Options on the **Entry Information** tab

Option	Description
Schedules	Lets you select the schedule to associate the entry with. The entry takes the appearance and permissions that are associated with the selected schedule.
Name	Identifies the entry on the calendar display.
Start Date **End Date**	Defines when the entry event begins and ends.
Popup Description	Lets you provide a brief description that appears when someone hovers over the entry on the calendar display.
Item Color	Lets you select the color in which to display the item on the schedule. You can use different colors to highlight certain types of entries or entries for a specific type of schedule.
Url	Lets you display the content of the schedule entry in a specific page. For example, if your organization has an intranet page to announce a special event, you can specify that page's URL. When someone views the schedule entry for that event, the intranet page for that event opens.
Description	Lets you provide additional information to describe the entry event.

Section 7

Managing your organization's knowledge

Chapter 24

Introducing Knowledge Management

This chapter includes the following topics:

- About Knowledge Management
- Types of knowledge base items
- About the Bulletin Board
- Knowledge base statuses
- Email notifications from Knowledge Management
- About permissions in the knowledge base

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.
  See "About the Bulletin Board" on page 251.
- The ability to set up a nested category hierarchy to organize knowledge base items and make them easier for users to find.
  See "Adding a knowledge base category or subcategory" on page 268.
- The ability to set permissions at both the category level and the individual document level.
  See "About permissions in the knowledge base" on page 254.
- A knowledge base approval process that helps to ensure that the content is relevant and accurate before publication.
  See "Processing requests for knowledge base entries" on page 255.
- 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 "Processing requests for knowledge base entries" on page 255.

Types of knowledge base items

The ServiceDesk knowledge base can contain several types of items. These items help organize the information and provide users with different levels of information to meet a variety of needs.

Table 24-1 Types of knowledge base items

Knowledge base item	Description
Article	A general-purpose, informational document. The article format provides the most flexibility. In addition to text, an article can contain images, formatted HTML, and links. An article has no size limitations.
FAQ (frequently asked question)	Provides the information in a question-and-answer format. FAQ items typically provide self-service information but can be used for other purposes as well.
Bulletin board message	A message that provides users with time-sensitive, critical information. Bulletin board items have date restrictions and a priority. Bulletin Board items appear on the Bulletin Board Web part in the ServiceDesk portal. See "About the Bulletin Board" on page 251.
Wiki article	A group of related articles, entries, or other documents and files about a specific topic.

About the Bulletin Board

The Bulletin Board is a Web part that appears on most of the main pages in the ServiceDesk portal. It contains any number of messages, which scroll up the Bulletin Board section. A bulletin board message provides users with time-sensitive, critical information.

The bulletin board messages are components of the ServiceDesk knowledge base. However, the Bulletin Board provides a proactive way to display the time-sensitive messages to ServiceDesk users without requiring them to access the **Knowledge Base** page.

Examples of how you can use the Bulletin Board are as follows:

- Inform users about critical, known issues.
  For example, if email 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.

- Inform users about upcoming outages and planned disruptions in service.
- Leave public or private messages for specific users, groups, or organizational units.
  Like the other items in the knowledge base, you can set permissions on bulletin board messages. Therefore, you can create messages for certain segments of your organization. You can also provide creation permissions so that others can create messages for the members of their groups or departments.

Bulletin Board messages can be created as a result of the Knowledge Management process or outside the process on the **Knowledge Base** page. Bulletin Board messages can also be created by using the **Add/Manage Bulletin Boards** action that appears on the **Process View** page of each ServiceDesk process.

See "Processing requests for knowledge base entries" on page 255.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

Knowledge base statuses

The knowledge base request status accurately reports the progression and outcome of the stages of the knowledge base process. The percentage represents the level of completion that the process has reached. For example, if the status percentage is 60, it means that the process is 60 percent complete.

The status and percentage appear in several places in the ServiceDesk portal. For example, they appear at the top of the ticket's **Process View** page.

Table 24-2 Knowledge base statuses

Status	Description	Completion percentage
Closed	The process is complete as a result of either of the following actions: ■ A knowledge base article was created. ■ The knowledge base article was removed.	100%
Create Article	The creation of the knowledge base article is underway. This status appears only if your Knowledge Management workflow is customized to skip the approval step.	80%

Table 24-2 Knowledge base statuses *(continued)*

Status	Description	Completion percentage
Review Proposed KB Article	A request for a knowledge base article was submitted and is ready to be worked.	20%
Review Request to Remove the KB Submittal	The knowledge base request was rejected and is in a waiting state for the knowledge base approver to remove it.	60%
Review Request to Create KB Entry	The knowledge base request was accepted and edited and is ready for the final review, or the review is underway.	60%

Email notifications from Knowledge Management

ServiceDesk sends email notifications at various stages of the Knowledge Management process. In this context, a knowledge base event is any action that is taken to request or create a knowledge base article. The type of event and the ServiceDesk configurations determine the recipients of the email notifications.

When you create an item in the knowledge base, you can specify whether notifications should be sent for that item.

Table 24-3 Default knowledge base events that trigger email notifications

Event	Email recipient
A knowledge base request is submitted.	The submitter
A knowledge base request is approved or rejected.	The submitter or the user on whose behalf someone submitted the request
A knowledge base article is changed.	Any user A user can set up an automatic email notification to be informed of changes to a specific article.
The Bulletin Board is cleared.	Any user A user can set up an automatic email notification to be informed when the Bulletin Board is cleared.

About permissions in the knowledge base

Access to knowledge base items is controlled through permissions. Permissions can be set on the knowledge base categories and on the individual knowledge base items. Permissions can be granted to users, groups, and organizational units.

The knowledge base items that are created through the Knowledge Management process contain default group permissions. Those default permissions can be edited from the **Knowledge Base** page. The knowledge base items that are created outside the process do not have default permissions. The permissions must be assigned during or after the item creation.

Typically, only the administrator or other user with the appropriate permissions can set permissions on knowledge base items and categories. For example, the knowledge base editors and approvers cannot set permissions for the items that are in the default categories. However, they can set permissions on the items that are in the categories that they created.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

See "Adding a knowledge base category or subcategory" on page 268.

See "Setting permissions" on page 95.

Chapter 25

Processing requests for knowledge base entries

This chapter includes the following topics:

Processing requests for knowledge base entries

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.

See "Roles in Knowledge Management" on page 256.

Table 25-1 Process for submitting and reviewing requests for knowledge base entries

Step	Action	Description
Step 1	A request for a knowledge base entry is submitted.	Requests for a knowledge base entry can originate from the Service Catalog, incidents, or problems. See "Submitting a request for a knowledge base entry" on page 259. See "Sources of knowledge base requests and entries" on page 257. When the request is submitted, a task to review the knowledge base request is assigned to the knowledge base editor.
Step 2	The knowledge base editor reviews the request.	After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. When the request is accepted, the editor can categorize the entry and edit it to improve usability. See "Accepting or rejecting a knowledge base request" on page 260. When the knowledge base editor finishes working with the request, a task is assigned to the knowledge base approver.
Step 3	The knowledge base approver reviews the request and determines how to handle it.	The knowledge base approver makes the final decision to post or remove a proposed knowledge base item. The approver can also return the request to the knowledge base editor for further editing or reconsideration.
Step 4	The knowledge base approver posts the entry to the knowledge base.	After the knowledge base entry is posted, it is available to all users.
Step 5	(Optional) The knowledge base approver sets additional restrictions on the entry.	The knowledge base items that are created through the Knowledge Management process contain default group permissions. If access to the entry needs to be restricted further, the knowledge base approver can edit the entry and its permissions from the **Knowledge Base** page. See "About permissions in the knowledge base" on page 254.

An administrator or other user with the appropriate permissions can create knowledge base items outside the Knowledge Management process.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

Roles in Knowledge Management

ServiceDesk employs roles to define responsibilities for and assign owners to the tasks and other activities within the ITIL processes.

The roles in the Knowledge Management process are tasked with editing, approving, and categorizing knowledge base entries.

See "Processing requests for knowledge base entries" on page 255.

Table 25-2 Roles in Knowledge Management

Role	Description
KB editor	Reviews a knowledge base request and approves or rejects it. The editor can categorize the entry and edit the title or content to improve usability.
KB approver	Reviews the proposed entry and provides a final approval for posting the entry to the knowledge base.

Sources of knowledge base requests and entries

The creation of a knowledge base request triggers the Knowledge Management process for approving and creating knowledge base items. A knowledge base request can originate from several sources.

See Table 25-3.

The administrator or other user with the appropriate permissions can also create knowledge base entries outside the approval process.

See Table 25-4.

Table 25-3 Sources of knowledge base requests for the Knowledge Management process

Source	Description
ServiceDesk portal	A user requests the creation of a knowledge base entry by creating a knowledge base request in the ServiceDesk portal. See "Submitting a request for a knowledge base entry" on page 259.

Table 25-3 Sources of knowledge base requests for the Knowledge Management process *(continued)*

Source	Description
Incident resolution	During the incident resolution process, on the **Create Incident Details** page, the support technician selects the option to create a knowledge base entry. See "Resolving an incident from the advanced incident form" on page 149. This option lets the support technician request an entry that can provide help for the same kind of issue in the future. For example, if the issue was resolved by training the user, the technician can request a knowledge base article that contains the same information. Users who encounter that issue in the future can find and read the knowledge base article instead of creating an incident.
Problem Management	During the problem review, on the **Review Proposal** page, the problem manager selects the option to create a knowledge base entry. See "Reviewing a proposed fix or workaround " on page 223. Creating a knowledge base entry is one way to resolve a problem. For example, if the problem cannot be fixed but a workaround exists, the workaround can be documented in a knowledge base article.

See "Processing requests for knowledge base entries" on page 255.

Table 25-4 Sources of knowledge base items outside the process

Source	Description
Knowledge Base page	On the **Knowledge Base** page, the administrator or other user with the appropriate permissions selects any of the following options: ■ **Add Article** ■ **Add Bulletin Board** ■ **Add FAQ** ■ **Add Wiki** See "Creating a knowledge base item from the Knowledge Base page" on page 269.

Table 25-4 Sources of knowledge base items outside the process *(continued)*

Source	Description
Process View page of an incident, change request, or problem ticket	A process worker Bulletin Board messages can be created by using the **Add/Manage Bulletin Boards** action that appears on the **Process View** page of these tickets. On the **Process View** page of an incident, change request, or problem ticket, a process worker creates a Bulletin Board messages by using the **Add/Manage Bulletin Boards** action.

Submitting a request for a knowledge base entry

Before it can be added to the knowledge base, most new content must go through the knowledge base approval and review process.

This task is a step in the process for creating a knowledge base entry.

See "Processing requests for knowledge base entries" on page 255.

The knowledge base article request is created, and a confirmation screen displays the process ID for the entry request. The proposed knowledge base entry now goes to a knowledge base editor, who approves or denies the request. Click **Close** to close the dialog.

To submit a request for a knowledge base entry

1. In the ServiceDesk portal, click **Submit Request**.
2. On the **Requests** page, under **New Requests** and under **Service Catalog**, click **Knowledge Base**.
3. On the right side of the page, click the **Submit KB entry** link.
4. In the **Entry Request** dialog box, define the entry as follows:

Title	Type a title to identify this entry in any article lists or search results in the ServiceDesk portal. When you type the title, make it as specific as possible so that it quickly conveys the purpose of the entry. For example, instead of "printer jam," you might type "Clearing a printer jam".
Content	Type and format the content for the proposed entry.

5. In the **Entry Request** dialog box, click **Submit**.
6. In the **Thank You** dialog box, click **Close**.

Accepting or rejecting a knowledge base request

After a knowledge base request is submitted, a knowledge base editor reviews the request and accepts or rejects it. The editor can categorize the entry and edit it to improve usability.

To prevent the addition of duplicate entries, ServiceDesk can determine if similar entries already exist and display the duplicates to the editor.

This task is a step in the process for creating a knowledge base entry.

See "Processing requests for knowledge base entries" on page 255.

Whether the request is accepted or rejected, a task is created for the knowledge base reviewer to review it and take final action.

See "Reviewing a knowledge base entry for final resolution" on page 263.

To review a knowledge base request

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Tasks Viewer**, under **Project Name**, expand **SD.KnowledgeBase Submission**.
3. In the list of tasks, find and open a request that needs to be reviewed.
4. On the ticket's **Process View** page, under **My Actions**, click **Review KB Request**.
5. If the request's title or content matches that of an existing entry, in the **Possible Duplicate Entries** dialog box, click the **View** link. Take one of the following actions:

If the request is a duplicate	Follow the steps in To designate a duplicate knowledge base entry.
If the request is not a duplicate	Take the following actions: ■ On the article's view page, click **Close**. ■ In the **Possible Duplicate Entries** dialog box, click **Continue**. ■ Go to step 6.

6. In the **Create KB Article** dialog box, review the entry submission, and then take one of the following actions:

To reject the request	Follow the steps in To reject a knowledge base request.
To accept the request	Follow the steps in To accept a knowledge base request.

To designate a duplicate knowledge base entry

1. Follow the initial steps in To review a knowledge base request.
2. On the duplicate article's view page, click **Close**.
3. In the **Possible Duplicate Entries** dialog box, click **Duplicate**.
4. In the **Reason for Closing this Request** dialog box, provide a reason for rejecting the entry, and then click **Submit**
5. In the **Thank You** dialog box, click **Close**.
6. When you are returned to the task's **Process View** page, you can close it.

To reject a knowledge base request

1. Follow the initial steps in To review a knowledge base request.
2. In the ServiceDesk portal, on the **My Task List** or **Tickets** tabs, open a ticket requesting that you review a proposed knowledge base article.
3. Under **Actions**, click **Respond**.
4. In the **Create KB Article** dialog box, click **Reject Submission**.
5. In the **Close Request** dialog box, provide a reason for rejecting the entry, and then click **Submit**.
6. In the **Thank You** dialog box, click **Close**.
7. When you are returned to the task's **Process View** page, you can close it.

To accept a knowledge base request

1. Follow the initial steps in To review a knowledge base request.
2. In the **Create KB Article** dialog box, categorize and enter additional information about the knowledge base entry.

   See "Create KB Article dialog box" on page 262.
3. When you are satisfied with the information, click **Preview**.
4. In the **Preview Post** dialog box, review the entry in its final format, and then click **Submit**.
5. In the **Thank You** dialog box, click **Close**.
6. When you are returned to the task's **Process View** page, you can close it.

Create KB Article dialog box

This dialog box lets you review a request for a knowledge base entry, edit it, categorize it, and accept or reject it. It appears when a knowledge base editor clicks **Review KB Request** on the request's **Process View** page.

See "Accepting or rejecting a knowledge base request" on page 260.

Table 25-5 Options in the **Create KB Article** dialog box

Option	Description
Knowledge Type	Lets you select the type of knowledge base item that the submission should be created as. The knowledge base item types are as follows: ■ Article ■ Wiki ■ FAQ ■ Bulletin Board
Category	Lets you select the category in which to place the knowledge base entry. You can also create a new category by clicking **New Category**. See "Adding a knowledge base category or subcategory" on page 268.
Parent Entry	(Optional) Lets you link entry articles by selecting a parent entry. You can choose from the other entries that are in the same category as the new entry. When a user searches the knowledge base, child entries are also displayed as links.
Description/Explanation of Question	Lets you provide a description of the article or a more detailed explanation of the question. This description appears under the title of the knowledge base item on the **Knowledge Base** page.
Edit Title/Question	(Optional) Lets you edit the title of the entry question to improve its usability. Depending on the entry type and category, you might use a question format. Examples of possible titles and questions are as follows: ■ If the entry describes how to reset a password, you might type **How do I reset a password?**. ■ If the entry explains when a password must be changed, you might type **How often should I change my password?**. ■ If the entry is an article that lists password creation standards, you might type **Guidelines for strong passwords**.
Content/Answer	Lets you edit or add to the content of the entry.

Reviewing a knowledge base entry for final resolution

After a knowledge base editor accepts or rejects a knowledge base request, the knowledge base approver receives a task to make a final decision.

The knowledge base approver can take the following actions:

- Approve and submit the entry.
- Edit the entry before approving it.
- Reject the entry.
- Return the request to the knowledge base editor for further editing or reconsideration.

The knowledge base approver can review the tasks that have the following statuses:

Review Request to Create KB Entry	This status represents a request that the knowledge base editor accepted. You can return it for further editing, reject it, edit it, or approve it. See Reviewing a request to create a knowledge base entry.
Review Request to Remove the KB Submittal	This status represents a request that the knowledge base editor rejected. You can agree to remove the request or you can decide to return the request to the editor for further editing or consideration. See Reviewing a knowledge base entry rejection.

Reviewing a request to create a knowledge base entry

1. In the ServiceDesk portal, click **My Task List**.
2. Under **Task Viewer**, under **Project Name**, expand **SD.KnowledgeBase Submission**.
3. In the list of tasks, find and open a request that has the status Review Request to Create KB Entry.

4 On the ticket's **Process View** page, under **My Actions**, click **Approve KB Request**.

5 In the **Approve Post** dialog box, select one of the following options:

Return to Editors	Select this option if the entry needs further review or edits. In the **Return Request** dialog box, enter a reason for returning the request, and then click **Return**. When you enter the reason for the return, you might also provide suggestions for changing the entry.
Remove Submission	Select this option to reject the entry and remove the request. In the **Close Request** dialog box, enter a reason for removing the request, and then click **Submit**.
Edit Request	Select this option to edit the request before you take further action. In the **Edit KB Details** dialog box, review and edit the entry as needed, and then click **Preview**. Step through the remaining dialog boxes to submit the entry and close the process. See "Create KB Article dialog box" on page 262.
Approve	Select this option to close the request and create the entry in the knowledge base.

Reviewing a knowledge base entry rejection

1 In the ServiceDesk portal, click **My Task List**.

2 Under **Task Viewer**, under **Project Name**, expand **SD.KnowledgeBase Submission**.

3 In the list of tasks, find and open a request that has the status Review Request to Remove the KB Submittal.

4 On the ticket's **Process View** page, under **My Actions**, click **Approve KB Removal Request**.

5 In the **Review Rejection** dialog box, select one of the following options:

Reject	Select this option to overturn the original decision to reject the request. The request is returned to the queue for the knowledge base editor to reconsider the decision and possibly make changes. In the **Return Request** dialog box, enter the reason for your decision, and then click **Return**. Step through the remaining dialog boxes and close the process.
Approved	Select this option when you agree that the original request should be rejected. Step through the remaining dialog boxes and close the process.

Chapter 26

Managing the knowledge base

This chapter includes the following topics:

About knowledge base categories

ServiceDesk uses categories to classify its knowledge base items. The knowledge base categories help the ServiceDesk workers and users find the information that they need. You can use additional levels of categories to group the items further. A knowledge base category can have multiple subcategories, and you can nest the subcategories.

ServiceDesk contains a hierarchy of predefined knowledge base categories. You can add categories and manage the existing ones on the **Knowledge Base** page in the ServiceDesk portal.

See "Adding a knowledge base category or subcategory" on page 268.

You can set permissions for the knowledge base categories and subcategories. The permissions determine who can access a knowledge base category and all the items that it contains.

Adding a knowledge base category or subcategory

Knowledge base categories and subcategories help you organize all the knowledge base items in ServiceDesk. Organizing the items in categories helps users find the items they need more easily.

You can grant category permissions to users, groups, and organizational units. The category permissions provide or deny access to a category and all the knowledge base items within it. Permissions also determine who can create subcategories for a specific category.

To add a knowledge base category

1. In the ServiceDesk portal, click **Knowledge Base**.
2. On the **Knowledge Base** page, under **Article Category List**, click the **Add Category** symbol (file folder with green plus sign), and then click **Add Root Category**.
3. On the **Knowledge Base** page, under **Categories**, take one of the following actions:

To add a root category	Click the **Add Category** symbol (file folder with green plus sign), and then click **Add Root Category**.
To add a subcategory	Select the category to add the subcategory to, click the **Add Category** symbol (file folder with green plus sign), and then click **Add Sub Category**.

4. In the **Add Root Category** or **Add Sub Category** dialog box, on the **Main Information** tab, provide a title and description for the category.

   The title identifies the category in any list or display of knowledge base categories in the ServiceDesk portal.

5. Click the **Permissions** tab, and then specify the permissions for one or more users, groups, permissions, or organizational units.

   See "Setting permissions" on page 95.

6. When you finish defining the category or subcategory, click **Save**.

Moving a knowledge base item to a different category

You can reorganize the items in the knowledge base by assigning them to different categories or subcategories.

For example, you might have assigned all your FAQ articles to the How To category. Over time, that category becomes full and its contents become harder to find. You can create subcategories for the How To category, and then move items to the subcategories.

See "Adding a knowledge base category or subcategory" on page 268.

When you move a knowledge base item, it inherits the permissions of its new category.

To move a knowledge base item to a different category

1. In the ServiceDesk portal, click **Knowledge Base**.
2. Find or navigate to the item to move.
3. Under **All Articles**, to the right of the item, click the **Actions** symbol (orange lightning), and then click **Move to Category**
4. In the **Move Article** dialog box, click **Pick**.
5. In the dialog box that appears, expand the categories if necessary, and then select the category to move the item to.
6. In the **Move Article** dialog box, click **Move**.

Creating a knowledge base item from the Knowledge Base page

An administrator or other user who has the appropriate permissions can create knowledge base items outside the Knowledge Management process.

To create a knowledge base item from the Knowledge Base page

1. In the **ServiceDesk** portal, click **Knowledge Base**.
2. On the **Knowledge Base** page, under **Categories**, select the category to add the item to.

   If the appropriate category is not listed, you can add a new one.

   See “Adding a knowledge base category or subcategory” on page 268.
3. On the **Knowledge Base** page, in the right pane, click one of the following options:
   - **Add Article**
   - **Add Bulletin Board**
   - **Add FAQ**
   - **Add Wiki**
4. In the dialog box that appears, define the content, set permissions on the item, and specify whether to send email notifications of the item’s events.

   The dialog box that appears depends on the type of item that you chose to add, as follows:
   - **Add Article**
     See “Add Article dialog box” on page 270.
   - **Add Bulletin**
     See “Add Bulletin dialog box” on page 272.
   - **Add FAQ**
     See “Add FAQ dialog box” on page 274.
   - **Add Wiki**
     See “Add Wiki dialog box” on page 275.
5. When you finish entering the information, click **Save**.

Add Article dialog box

This dialog box lets you create knowledge base articles outside the Knowledge Management process.

See “Creating a knowledge base item from the Knowledge Base page” on page 269.

When you edit an article or an article entry, the **Edit Article** and **Edit Entry Information To Article** dialog boxes contain similar options.

When an article is first created, it consists of one entry. More entries can be added later. For example, instead of editing the original entry, you can add an entry that contains updates or corrections.

In Table 26-2, the options that are marked as entry-specific apply to each entry. The other options apply to the entire article. You cannot edit the entry-specific options directly from the **Knowledge Base** page. Instead, you must open the article and select the option to edit an entry.

Table 26-1 Tabs in the **Add Article** dialog box

Tab	Description
Article Information	Lets you define the contents of the article. See Table 26-2.
Description	Appears beneath the article title in any list or display of knowledge base items in the ServiceDesk portal. The description helps the users decide whether to view the article in more detail. When you edit an existing article, the **Description** box appears on the **Article Information** tab.
Attachment	Lets you add an attachment to the article. For example, you can add an attachment as a source to an article's premise.
Notifications	Contains the **Process Notifications** option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.
Permissions	Lets you set the permissions for the item. See "Setting permissions" on page 95.
Profiles	(Optional) Lets you apply profiles to the item.
Key Words	Lets you apply key words to the item.
Tags	Lets you apply tags to the item.

Table 26-2 Options on the **Article Information** tab

Option	Description
Category Name	(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See "Moving a knowledge base item to a different category" on page 269.
Article Title	Identifies the item in any list or display of knowledge base items in the ServiceDesk portal.
Entry Title	(Entry-specific) Appears on the page that opens when a user views the article.
Text	(Entry-specific) Lets you provide the more extensive information that appears when a user views the article. This information is associated with the entry title.

Add Bulletin dialog box

This dialog box lets you create bulletin board messages outside the Knowledge Management process.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

When you edit a bulletin board message or a message entry, the **Edit Bulletin** and **Edit Entry Information To Article** dialog boxes contain similar options.

When a bulletin board message is first created, it consists of one entry. More entries can be added later. For example, instead of editing the original entry, you can add an entry that contains updates or corrections. The entries appear separately on the Bulletin Board.

In Table 26-3, the options that are marked as entry-specific apply to each entry. The other options apply to the entire message. You cannot edit the entry-specific options directly from the **Knowledge Base** page. Instead, you must open the message and select the option to edit an entry.

Table 26-3 Tabs in the **Add Bulletin** dialog box

Tab	Description
Bulletin Information	Lets you define the contents of the bulletin board message. See Table 26-4.

Table 26-3 Tabs in the **Add Bulletin** dialog box *(continued)*

Tab	Description
Description	Appears beneath the bulletin board title on the **Knowledge Base** page. Because of space limitations, it does not appear on the Bulletin Board. When you edit an existing bulletin board message, the **Description** box appears on the **Bulletin Information** tab.
Notifications	Contains the **Process Notifications** option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.
Permissions	Lets you set the permissions for the item. See "Setting permissions" on page 95.
Profiles	(Optional) Lets you apply profiles to the item.
Key Words	Lets you apply key words to the item.
Tags	Lets you apply tags to the item.

Table 26-4 Options on the **Bulletin Information** tab

Option	Description
Category Name	(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See "Moving a knowledge base item to a different category" on page 269.
Bulletin Board Title	Appears at the left of the message on the Bulletin Board. It also appears on the page that opens when a user views the bulletin board message.
Mark as Obsolete	Indicates that the item is no longer current. By default, obsolete items do not appear on the **Knowledge Base** page. Obsolete items can be viewed if the **Show Obsolete Articles** option is selected.
Entry Title	(Entry-specific) Appears on the Bulletin Board as the message heading. It also appears on the page that opens when a user views the bulletin board message. The priority determines the color of the entry title when it appears on the Bulletin Board.

Table 26-4 Options on the **Bulletin Information** tab *(continued)*

Option	Description
Priority	(Entry-specific) Lets you indicate the importance of a bulletin board entry. You can set the priority to Low, Medium, High, or Emergency.
Display From	(Entry-specific) Indicates the first date on which the entry appears on the Bulletin Board.
Display Until	(Entry-specific) Indicates the last date on which the entry appears on the Bulletin Board.
Text	(Entry-specific) Lets you provide the more extensive information that appears when a user opens the bulletin board message. For example, if the bulletin board message announces a planned outage, the text might describe when the outage is planned and which systems it affects. This information is associated with the entry title.

Add FAQ dialog box

This dialog box lets you create FAQ (frequently asked question) items outside the Knowledge Management process.

See “Creating a knowledge base item from the Knowledge Base page” on page 269.

When you edit a FAQ item, the **Edit FAQ** dialog box contains similar options.

Table 26-5 Tabs in the **Add FAQ** dialog box

Tab	Description
FAQ Information	Lets you define the contents of the FAQ item. See Table 26-6.
Explanation of Question	Lets you type information in **Explanation of the Question** to help the users decide whether they selected a FAQ that meets their needs. Typically, the explanation should explain the situation that the FAQ answers. For example, if the FAQ question is “How do I clear a printer jam?” you might provide the following explanation: **This FAQ describes what to do when paper is stuck in your printer.**
Notifications	Contains the **Process Notifications** option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.

Table 26-5 Tabs in the **Add FAQ** dialog box *(continued)*

Tab	Description
Permissions	Lets you set the permissions for the item. See "Setting permissions" on page 95.
Profiles	(Optional) Lets you apply profiles to the item.
Key Words	Lets you apply keywords to the item.
Tags	Lets you apply tags to the item.

Table 26-6 Options on the **FAQ Information** tab

Option	Description
Category Name	(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See "Moving a knowledge base item to a different category" on page 269.
Question	Lets you type a question that the FAQ item answers. Try to write the question from the user's point of view and in non-technical language. For example: How do I clear a printer jam?
Answer	Lets you provide the solution to the user's question. The answer format depends on the nature of the question. For example, if the question asks how to perform a task, you can format the answer as a series of numbered steps. If the question asks for conceptual or reference information, you can format the answer as a paragraph or a table, respectively.

Add Wiki dialog box

This dialog box lets you create wiki articles outside the Knowledge Management process. When you edit a wiki article or an article entry, the **Edit Wiki** and **Edit Wiki Entry** dialog boxes contain similar options.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

Table 26-7 Tabs in the **Add Wiki** dialog box

Tab	Description
Wiki Information	Lets you define the contents of the wiki article. See Table 26-8.
Wiki Description	Appears beneath the wiki article title in any list or display of knowledge base items in the ServiceDesk portal. The description helps the users decide whether to view the wiki article in more detail. When you edit an existing article, the **Description** box appears on the **Article Information** tab.
Notifications	Contains the **Process Notifications** option, which sends the email notifications when events occur on the item. For example, notifications can be sent when an item is edited or read. The notifications are sent to those who have notify permissions for the item. This option is selected by default.
Permissions	Lets you set the permissions for the item. See "Setting permissions" on page 95.
Profiles	(Optional) Lets you apply profiles to the item.
Key Words	Lets you apply key words to the item.
Tags	Lets you apply key words to the item.

Table 26-8 Options on the **Wiki Information** tab

Option	Description
Category Name	(Read only) Displays the category to which this item belongs. This information might not appear when the item is first created. The only way that the category can be changed is by moving the item to a different category. See "Moving a knowledge base item to a different category" on page 269.
Wiki Title	Identifies the item in any list or display of knowledge base items in the ServiceDesk portal.
Mark as Obsolete	Indicates that the item is no longer current. By default, obsolete items do not appear on the **Knowledge Base** page. Obsolete items can be viewed if the **Show Obsolete Articles** option is selected.

Table 26-8 Options on the **Wiki Information** tab *(continued)*

Option	Description
Text	Lets you provide the more extensive information that appears when a user opens the wiki article. You can add links in the text area to provide access to related information. See "Adding entries and links to a wiki article" on page 277. See "Links in wiki articles" on page 278.

Adding entries and links to a wiki article

When you create a wiki article and its subentries, you can add links to the text area to provide access to related information. For example, you can link to another subentry, a knowledge base article, a document, or an image file.

See "Creating a knowledge base item from the Knowledge Base page" on page 269.

To add entries and links to a wiki article

1. In the ServiceDesk portal, click **Knowledge Base**.
2. On the **Knowledge Base** page, open an existing wiki article.

   You can also add a link at the same time that you create a new wiki article. However, you must save the article and then open it to connect the link to its target.
3. On the article view page, click the **Actions** symbol (orange lightning), and then click **Edit Entry**.
4. In the **Edit Wiki Entry** dialog box, in **Text**, type a link in the appropriate format.

   See "Links in wiki articles" on page 278.
5. Enter any additional information as needed, and then click **Save**.
6. On the article view page reappears, click the link.

   The link appears in the following format:

   ??_*link*_??
7. Depending on the type of link that you entered, you might be required to type text or select a file or document to add.
8. When you finish creating the new entry, click **Save**.
9. Close the article view page.

Links in wiki articles

When you create a wiki article and its subentries, you can add links to the text area to provide access to related information. Several types of links are available.

See "Adding entries and links to a wiki article" on page 277.

Table 26-9 Types of links in wiki articles

Link syntax	Description
`[[article]]`	Links to any type of knowledge base item. The title of the knowledge base item becomes the link text. When you click this link during the entry creation, a small version of the **Knowledge Base** page appears, where you select the item to link to.
`[[file]]`	Links to any type of document file. The document title or file name becomes the link text. When you click this link during the entry creation, a small version of the **Documents** page appears, where you select the file to link to. If the file is not listed, you can add it. See "Adding a document to the Document Management system" on page 297.
`[[home]]`	Links to the main entry for the wiki article.
`[[image]]`	Links to an image file that is stored in the ServiceDesk document management system. When you click this link during the entry creation, a small version of the **Documents** page appears, where you select the image to link to. If the image is not listed, you can add it. See "Adding a document to the Document Management system" on page 297.
[[*new entry title*]]	Links to a new entry. The text that you type within the brackets becomes the title of the new entry and the name of the link that the user sees. When you click this link during the entry creation, a new entry page appears, where you can type information for the new entry.
`[[owner]]`	Links to the entry that is the parent of the current entry.

Table 26-9 Types of links in wiki articles *(continued)*

Link syntax	Description
`[[`***`text to link`***`|`***`Title To Show`***`]]`	Links to another entry. The link that the user sees is not the same as the entry title. The *text to link* segment is the name of the link. You can specify any of the wiki links. The contents of the *text to link* segment becomes the name of the link that the user sees in the wiki article. Examples of how you can use this link format are as follows: ■ `[[`***`article|Click here to open an article.`***`]]` The link text becomes "Click here to open an article." ■ `[[`***`About Wikis|Learn more about wikis.`***`]]` The title of the new entry becomes "About Wikis" and the link text becomes "Learn more about wikis."

Chapter 27

Using the knowledge base

This chapter includes the following topics:

Searching the knowledge base

You can search for knowledge base items on the **Knowledge Base** page.

The knowledge base searches are performed as follows:

- The search is performed on the item name.
- The search evaluates the items in all the knowledge base categories.
- Your permissions determine the categories and items that you can access, which in turn influences the results of your searches.

When you find a knowledge base item, you can open and view it or perform other actions.

See "What you can do with a knowledge base item" on page 282.

To search the knowledge base

1. In the ServiceDesk portal, click **Knowledge Base**.
2. Under **Search Articles**, enter the text to search for, and then click the **Search** symbol.

Viewing an item in the knowledge base

To view an item in the knowledge base

1. In the ServiceDesk portal, click **Knowledge Base**.
2. On the **Knowledge Base** page, take one of the following actions:
   - Under **Search Articles**, enter the text to search for, and then click the **Search** symbol.
   - Under **Article Category List**, select a category that is likely to contain the item.
3. Under **All Articles**, scroll through the list of knowledge base items to find one that might provide the information you need.

   If you cannot find what you need, you can repeat step 2.
4. To open an item, click its article name or click the **Open** symbol (a magnifying glass) that appears at the far right of its name.
5. If the item contains multiple entries, you can expand and collapse them to view their information.
6. (Optional) Take any other actions that you need.

   Your permissions determine what you can do with a knowledge base item. For example, typical actions are to view the item's history, print it, or export it.

   See "What you can do with a knowledge base item" on page 282.

What you can do with a knowledge base item

When you open and view a knowledge base item, you might have additional options for interacting with that item.

See "Viewing an item in the knowledge base" on page 282.

All the options except **Add New Entry** are available on the drop-down list that appears when you click the **Actions** symbol (orange lightning) for an item.

Your permissions determine the options that are available to you. For example, typical actions are to view the item's history, print it, or export it.

Table 27-1 Options for working with a knowledge base item

Options	Description
Add Comment	Lets you comment on the knowledge base item.

Table 27-1 Options for working with a knowledge base item *(continued)*

Options	Description
Add New Entry	Lets you add an entry to the knowledge base item. For example, a knowledge base article can consist of several entries.
Delete Entry	Lets you delete the selected entry.
Edit Entry **Edit FAQ**	Lets you edit the entries of a knowledge base item. FAQ items do not contain additional entries.
Export	Lets you save the knowledge base item to a file.
Send Entry	Lets you specify one or more email addresses to send the entry to.
Print	Lets you print the knowledge base item.
Rating	Displays five stars and lets you rate the item by selecting one of the stars. The first star is the lowest rating, and the last star is the highest rating.
View History	Displays the events that have occurred for the knowledge base item. For example, the list includes the additions and edits that were made to the item.

Section 8

Managing the documents in ServiceDesk

Chapter 28

Adding and managing documents

This chapter includes the following topics:

About Document Management

The Document Management system in ServiceDesk lets you store, track, and use, the documents and files that are associated with ServiceDesk processes. The ServiceDesk documents include the files and the screen images that are attached to process tickets and any plans that are created during a process.

See "About Document Management in the ServiceDesk processes" on page 289.

Document Management lets you take the following actions:

- Set permissions at both the category level and the individual document level.
- Add documents with or without version information or keywords.
- Add messages to the **Documents** page to inform a set of users that a document is expected from them by a certain date.
- Add any type of document or file. Documents are not restricted to a set of defined file types.
- Find documents by performing a name search or an advanced keyword search.
- Set up a nested category hierarchy to organize documents and make them easier for users to find.
- Email documents.
- Edit the information data for existing documents.
- Add new versions of documents and display version and document history.
- Download documents in their native file formats or as compressed (.zip) files.

About Document Management in the ServiceDesk processes

Certain of the core ServiceDesk processes contain built-in Document Management functionality. By default, ServiceDesk stores some of the documents that are created in the processes and displays them on the **Documents** page.

The Knowledge Management processes does not integrate with Document Management by default. However, you can edit the processes in Workflow Designer to add Document Management integration.

For more information about editing workflow processes, see the *Workflow Solution User Guide*.

Table 28-1 Default Document Management functionality in ServiceDesk processes

Process	Process documents in Document Management
Incident Management	File attachments and screen shots
Change Management	Risk assessments, implementation plans, test plans, backout plans, and any other planning documents
Problem Management	Documents that you attach as part of the Problem Management process
Any process ticket	Documents that are attached to a process ticket ServiceDesk creates a Process category, adds a subcategory for each process, and adds a subcategory for each process ticket. All the documents that are associated with a specific process ticket are assigned to that ticket's category. The process ticket categories are hidden categories. The **Hidden** check box on the **Documents** page lets users show or hide the hidden categories.

About document categories

ServiceDesk uses categories to classify its documents. The document categories help the ServiceDesk workers find the documents that they need. You can use additional levels of categories to group the documents further. A document category can have multiple subcategories, and you can nest the subcategories.

ServiceDesk contains a hierarchy of predefined document categories. ServiceDesk also creates subcategories when it adds the documents that are attached to or created within a process. You can add categories and manage the existing ones on the **Documents** page in the ServiceDesk portal.

See "Adding a document category" on page 290.

You can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains.

See "Setting permissions for a document category" on page 293.

Adding a document category

Document categories help you organize all the documents in ServiceDesk. The document categories help the ServiceDesk workers find the documents that they need.

See "About document categories" on page 289.

You can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create categories.

See "Setting permissions for a document category" on page 293.

To add a document category

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, at the upper right of the **Browse** section, click the **Add Root Category** symbol (a file folder with a green plus sign).
3. In the **Add Category** dialog box, on the **Category Information** tab, define the new category, and then click **Save**.

   See "Category and Sub Category dialog boxes" on page 291.
4. (Optional) On the

Adding a document subcategory

You can create document subcategories to subdivide the contents of document categories and provide another level of document organization. You can add subcategories to any category.

See "About document categories" on page 289.

You can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create subcategories for a specific category.

See "Setting permissions for a document category" on page 293.

To add a document subcategory

1. In the ServiceDesk portal, click **Documents**.
2. On the **Documents** page, under **Browse**, select the category to add a subcategory to.
3. In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Add Sub Category**.
4. In the **Add Sub Category** dialog box, on the **Category Information** tab, define the new subcategory, and then click **Save**.

   See "Category and Sub Category dialog boxes" on page 291.

Category and Sub Category dialog boxes

These dialog boxes let you add a document category, add a document sub category, or edit any document category. The action that you take in ServiceDesk determines which dialog box appears.

See "Adding a document category" on page 290.

See "Adding a document subcategory" on page 290.

See "Editing a document category" on page 292.

Some of the options differ depending on which dialog box appears.

These dialog boxes contain the following tabs:

Category Information	Lets you define the category. See Table 28-2 on page 292.
Profiles	Lets you assign a profile to the category.
Advanced	Displays the category ID for informational purposes only. No user actions are located on this tab. This tab appears in the **Edit Category** dialog box only.

Table 28-2 Options on the **Category Information** tab

Option	Description
Name	Identifies the category in any list or display of document categories in the ServiceDesk portal.
Header Text	Lets you type additional information to describe the category. The description appears beneath the category title in the right pane of the **Documents** page.
Category Type	Lets you select a document category type. The document category types provide 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. The use of document category types is optional. They are available only if the administrator added them.
Hidden	Lets you hide the category from all other users.
Process Notifications	Sends the email notifications when events occur on the documents that belong to the category. For example, notifications can be sent when a new version of a document is added. The notifications are sent to those who have notify permissions for the item. This option is selected by default.
Parent Category	(Lets you specify a parent category. This option appears in the **Edit Category** dialog box only.

Editing a document category

You can edit the existing document categories and document subcategories in ServiceDesk.

See "About document categories" on page 289.

To edit a document category

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the category or subcategory to edit.

3 In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Edit**.

4 In the **Edit Category** dialog box, edit the information as needed, and then click **Save**.

See "Category and Sub Category dialog boxes" on page 291.

Setting permissions for a document category

Document categories help you organize all the documents in ServiceDesk. The document categories help the ServiceDesk workers find the documents that they need.

See "About document categories" on page 289.

An administrator or other user who has the appropriate permissions can set permissions for the document categories and subcategories. The permissions determine who can access a document category and all the documents that it contains. Permissions also determine who can create categories and subcategories.

To set permissions for a document category

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the category.

3 In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Permissions**.

4 In the **Permissions** dialog box, add or edit the permissions as needed.

See "Setting permissions" on page 95.

5 Click **Close**.

Deleting a document category

An administrator or other user who has the appropriate permissions can delete document categories. The selections that you make during the deletion process determine what happens to the subcategories and the documents that are contained in the document categories.

See "About document categories" on page 289.

To delete a document category

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the category to delete.

3 In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Delete**.

4 In the **Delete Category** dialog box, under **SubCategories Delete Option**, select one of the following options for handling any subcategories that are contained in the category:

Don't delete SubCategories	Retain all the subcategories and move them up to the next-highest level.
Delete SubCategories	Delete all the subcategories. Any documents in the subcategory that also belong to another category are retained in the other category. Any documents that do not belong to other categories are moved to the Orphan category.
Delete SubCategories and all files in them	Delete all the subcategories and the documents that they contain.

5 In the **Delete Category** dialog box, under **Documents Delete Option**, select one of the following options for handling any documents that are contained in the category:

Don't delete documents	Retains all the documents that belong to the category.
Delete documents (that are linked only to the deleted category)	Delete all the documents that belong to the category but that do not belong to another category. Any documents that belong to other categories are retained.
Delete documents even if linked to multiple categories	Delete all the documents that belong to the category, even if they also belong to categories.

6 Click **Delete**.

Displaying the history of a document category

The document category history displays the creation history and change history for a document category.

See "About document categories" on page 289.

To display the history of a document category

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the category.
3. In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **History**.

Creating expected document messages

You can use expected document messages to remind certain ServiceDesk users to provide a document by a certain date. The messages appear on the **Documents** page. You can display a message to a user, group, or organizational unit.

See "About document categories" on page 289.

To create an expected document message

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the expected document's category.
3. In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Add Expected Document**.
4. In the **Expected Documents** dialog box, define the message and specify its recipients.

   See "Expected Documents dialog box" on page 296.
5. In **Select Source**, select the entity to show the message to: a user, group, permission, or organizational unit.
6. In **User**, **Group**, **Permission**, or **Organization**, type the name of the entity to display the message to.

   You can also click **Pick** to select the appropriate entity.

7 If you clicked **Pick**, in the **Picker** dialog box, select a specific entity as follows:

User Picker dialog box	Select a user. See "Picking a user" on page 96.
Group Picker dialog box	Click the **select** link to the right of the appropriate group.
Permission Picker dialog box	Click the **select** link to the right of the appropriate permission.
Organisation Picker dialog box	Expand the organizations if necessary, and then select an organization.

8 In the **Expected Documents** dialog box, click **Add Source**.

9 To add more sources, repeat step 5 through step 8.

10 When you finish defining the message and selecting the recipients, click **Save**.

Expected Documents dialog box

This dialog box lets you define a message to remind certain ServiceDesk users to provide a document by a certain date. This dialog box is available from the **Documents** page.

See "Creating expected document messages" on page 295.

Table 28-3 Options on the **Expected Documents** dialog box

Option	Description
Document Name	Lets you provide the name of the document that is expected.
Group Name	Lets you provide a name for the collected recipients of the message. For example, if you select three users, you can use this name to address them collectively, regardless of any actual groups that they belong to.
Expected Date	Lets you specify the date on which the document is needed.
Document Type	Lets you select from a list of document types, which lets the recipient know what type of document is expected.

Table 28-3 Options on the **Expected Documents** dialog box *(continued)*

Option	Description
Description	Lets you describe the document that is expected. For example, you can specify the document contents and explain the data that is required. The description is included in the message display.
Select Source	Lets you select the entity to show the message to: a user, group, permission, or organizational unit.
User **Croup** **Permission** **Organization**	Lets you type or pick the specific entity to display the message to.
Add Source	Adds the selected recipient to the message.

Adding a document to the Document Management system

You can add any type of document to the Document Management system in ServiceDesk. The information that you provide when you add the document determines whether the document is considered simple or advanced.

Advanced documents contain version information and search keywords in addition to the standard document information. Simple documents do not contain the version information or search keywords.

See “About Document Management” on page 288.

To add a document to the Document Management system

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the category to add a document to.
3. In the right pane, at the far right of the category’s title bar, click the **Edit Folder** symbol (orange lightning). Select one of the following options:
   - **Add Simple**

- **Add Advanced**

4 In the **Add Documents** or **Add Advanced Document** dialog box, define the new document, and then click **Save**.

See "Add Documents dialog box" on page 298.

See "Add Advanced Document dialog box" on page 299.

Add Documents dialog box

This dialog box appears when you add a simple document to the Document Management system. Simple documents do not contain the version information or search keywords.

See "Adding a document to the Document Management system" on page 297.

Table 28-4 Options in the **Add Documents** dialog box

Tab	Description
Documents Information	Lets you specify the location of the document file.
Optional	Lets you apply attributes to the document to make it easier to identify. See Table 28-5.
Expected Documents	Lets you indicate that the new document represents a response to an expected document request. This tab appears only if at least one expected document exists. See Table 28-6.
Profiles	Lets you apply a profile value to the document.

Table 28-5 Options on the **Optional** tab

Option	Description
Document Type	Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can add any type of document to the Document Management system even if it is not listed.

Table 28-5 Options on the **Optional** tab *(continued)*

Option	Description
Override Name	Identifies this document in any list of documents in the ServiceDesk portal. Make the name descriptive enough for you and others to easily understand the purpose of the document. If you do not provide a name, the document's file name is used.
Description	Appears beneath the document name in any list or display of documents in the ServiceDesk portal. The description helps the users decide whether to view the document.

Table 28-6 Options on the **Expected Documents** tab

Option	Description
Expected Document	Lets you select the expected document that the new document represents. When the new document is saved and added, the associated expected document message is removed.
Document Name	Lets you name the new document. The options are as follows: ■ **Missing document name** ■ **Uploaded document name** ■ **User specified name**

Add Advanced Document dialog box

This dialog box appears when you add an advanced document to the Document Management system. Advanced documents contain version information and search keywords in addition to the standard document information.

See "Adding a document to the Document Management system" on page 297.

Table 28-7 Tabs in the **Advanced Document** dialog box

Tab	Description
Document Information	Defines the document. See Table 28-8 on page 300.

Table 28-7 Tabs in the **Advanced Document** dialog box *(continued)*

Tab	Description
Versions to Keep	Determines the number of versions of the document to keep. See Table 28-9 on page 301.
Version Information	Specifies the document's version. See Table 28-10 on page 301.
Expected Documents	Lets you indicate that the new document represents a response to an expected document request. This tab appears only if at least one expected document exists. See Table 28-11 on page 301.
Profiles	(Optional) Lets you apply a profile value to the document.

Table 28-8 Options on the **Document Information** tab

Option	Description
File	Lets you specify the location of the document file.
Name	Identifies this document in any list of documents in the ServiceDesk portal. Make the name descriptive enough for you and others to easily understand the purpose of the document. If you do not provide a name, the document's file name is used.
Category	(Read only) Displays the category to which this document belongs.
Document Type	Lets you identify the document format or type. The ServiceDesk administrator creates the types that appear in the list. However, you can add any type of document to the Document Management system even if it is not listed.
Description	Appears beneath the document name in any list or display of documents in the ServiceDesk portal. The description helps the users decide whether to view the document.
Keywords	(Optional) Lets you associate keywords with the document. The keywords appear during a document search. When you type multiple keywords, separate them with a comma.

Table 28-9 Options on the **Versions to Keep** tab

Option	Description
Release **Major** **Minor**	Lets you specify the number of each version type that ServiceDesk keeps. Any versions beyond the specified numbers are removed.
Keep major versions of prior release versions	Lets you specify whether to keep major versions of previous release versions.
Keep minor versions of prior major versions	Lets you specify whether to keep minor versions of previous major versions.

Table 28-10 Options on the **Version Information** tab

Option	Description
Release version **Major version** **Minor version**	Lets you define the document's version. The numbers of the different version levels are combined when the version number is displayed. For example, in the version number 2.1.0, the release version is 2, the major version is 1, and the minor version is 0.
Notes	(Optional) Lets you type additional information to display with the document.

Table 28-11 Options on the **Expected Documents** tab

Option	Description
Expected Document	Lets you select the expected document that the new document represents. When the new document is saved and added, the associated expected document message is removed.
Document Name	Lets you name the new document. The options are as follows: ■ **Missing document name** ■ **Uploaded document name** ■ **User specified name**

Setting permissions for a document

An administrator or other user who has the appropriate permissions can set permissions for a document in ServiceDesk. The permissions determine who can access and use a document. For example, you can specify which users or groups can view, edit, delete, or email a document.

See "About Document Management" on page 288.

To set permissions for a document

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.

3 In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Edit > Permissions**.

4 In the **Permissions List** dialog box, add or edit permissions as needed.

   See "Setting permissions" on page 95.

5 Click **Close**.

Editing document data

You can edit a document's descriptive information, versions, and profiles.

You cannot edit the document itself from the ServiceDesk portal. However, you can import a new version of the document and associate it with the existing document.

See "Adding a new document version" on page 303.

To edit document data

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.

3 In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Edit > Document Data**.

4 In the **Document Data** dialog box, edit the data as needed, and then click **Save**.

Adding a new document version

You can update a document by importing a new version of the file. You specify the updated document and then specify whether the document represents a new release, major version, or minor version. When the document is added, the version number is incremented.

To add a new document version

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Edit > Add New Version**.
4. In the **Document Versions** dialog box, click the **Add New Version** tab.
5. On the **Add New Version** tab, provide the following information:

Version Type	Specify which of the version types the document represents, as follows: ■ **Minor** ■ **Release** ■ **Major**
Notes	Provide additional information about the nature of the new version.
File	Specify the location of the updated document file.

6. Click **Add**.

Promoting a document version

You can promote a document's most recent version to the next version level. Promoting the version means incrementing the number of the next-highest version type. For example, if the original version of a document is 2.0.0 and you add a minor version, the new version number is 2.0.1. If you promote the version, the new version number becomes 2.1.0.

To promote a document version

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Edit > Promote Document Version**.
4. In the **Promote Documents Version** dialog box, click the **Promote This Document Version** tab.
5. (Optional) In **Notes**, provide an explanation or other additional information about the version promotion.
6. Click **Promote This Version**.

Adding a document to additional categories

When a document is first added to the Document Management system, it is assigned to a single category. You can assign a document to any number of additional categories.

To add documents to additional categories

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Edit > Add to Category**.
4. In the **Add to Category** dialog box, click the **Add New Category** tab.
5. In **Category**, type the name of the category to add the document to or click **Pick** to select from a list of categories.
6. Click **Add**.
7. To confirm the new category, click the **Category List** tab to view the category, and then close the dialog box.

Deleting a document

You can delete a document that is obsolete or no longer useful.

To delete a document

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Delete**.
4. In the confirmation dialog box, click **OK**.

Chapter 29

Viewing documents

This chapter includes the following topics:

What you can do with ServiceDesk documents

When you open and view a document, you might have additional options for interacting with it.

All of the options are available on the drop-down list that appears when you click the **Actions** symbol (orange lightning) for a document.

Your permissions determine the options that are available to you. For example, typical actions are to download a document, view its history, or send it by email.

Table 29-1 Options for working with a document

Option	Description
Add New Version	Lets you update a document by importing a new version of the file and choosing how to increment the version number. See “Adding a new document version” on page 303.
Add to Category	Lets you assign a document to other categories in addition to its original category. See “Adding a document to additional categories” on page 304.
Delete	Lets you delete a document that is obsolete or no longer useful. See “Deleting a document” on page 305.
Document Data	Lets you edit a document’s descriptive information, versions, and profiles. See “Editing document data” on page 302.
Download	Lets you download a document. See “Downloading a document” on page 310.
Download Zip	Lets you download a document as a compressed file. See “Downloading a document in .zip format” on page 311.
Edit	Lets you select the following options: ■ **Document Data** ■ **Add New Version** ■ **Promote Document Version** ■ **Permissions** ■ **Add to Category**
History	Lets you view the history of a document’s creation and updates in the Document Management system. See “Viewing a document’s history” on page 312.
Open Document	Lets you open a document so that you can view its contents. See “Viewing a document” on page 310.
Permissions	Lets you set permissions for other users to access a document. See “Setting permissions for a document” on page 302.
Promote Document Version	Lets you promote a document’s most recent version to the next version level, which increments the number of the next-highest version type. See “Promoting a document version” on page 303.

Table 29-1 Options for working with a document *(continued)*

Option	Description
Send	Lets you attach a document to an email message or provide a link for the email recipient to download the document. See "Emailing a document" on page 311.
Show Versions	Lets you view or download any existing version of a document. See "Viewing a document's versions" on page 312.
View	Lets you select the following options: ■ **Open Document** ■ **Show Versions** ■ **History**

Searching for documents

You can search for documents on the **Documents** page.

The document searches are performed as follows:

- You can search on the document name or on keywords.
  Only the documents that have keywords (advanced documents) are included in a keyword search.
- The search evaluates the documents in all the document categories.
- Your permissions determine the categories and documents that you can access, which in turn influences the results of your searches.

You can preview the search results to decide whether to open it.

See "Previewing documents" on page 310.

When you find a document, you can open and view it or perform other actions.

See "What you can do with ServiceDesk documents" on page 307.

To search for documents

1. In the ServiceDesk portal, click **Documents**.
2. Under **Search Document**, type the text to search for, and then click the **Search** symbol.

Previewing documents

The document viewer lets you quickly scan the documents in a category so you can decide whether to view or download the. The document viewer opens in a new window and lists the documents in the left pane. When you select a document, a preview of the document appears in the right pane.

The document viewer can display Microsoft Office documents and image files.

To preview documents

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, at the far right of the category's title bar, click the **Edit Folder** symbol (orange lightning), and then click **Document Viewer**.
4. When you finish previewing the documents, close the document viewer window.

Viewing a document

You can open a document from the **Documents** page to view it in a new window.

See "What you can do with ServiceDesk documents" on page 307.

To view a document

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **View > Open Document**.
4. When you finish viewing the document, you can close the document window.

Downloading a document

You can download a document so that you can use it outside of the ServiceDesk portal.

To download a document

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Download** symbol (blue diskette).
4. In the **File Download** dialog box, click **Open** or **Save** and follow the prompts.

Downloading a document in .zip format

You can download a document as a compressed (.zip) file so that you can use it outside of the ServiceDesk portal. Compressing the file reduces the download time.

To download a document in .zip format

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Download Zip**.
4. In the **File Download** dialog box, click **Open** or **Save** and follow the prompts.

Emailing a document

You can email a document by attaching it to an email message or by adding a link to the document's location.

To email a document

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **Send**.

4 In the **Send Document** dialog box, type the following information:
   - **Send To**
   - **CC**
   - **Subject**
   - **Message**

5 In **Send Method**, select one of the following options:

Send as attachment	Attach the document to the email message.
Send download link	Add a link to the body of the email for downloading the document.

6 Click **Send Document**.

Viewing a document’s versions

You can view all of the available versions of a document. You can also download any of the available versions.

To view document version and history

1 In the ServiceDesk portal, click **Documents**.

2 On the **Category View** page, under **Browse**, select the document’s category.

   If you cannot find the document, you can perform a search.

   See “Searching for documents” on page 309.

3 In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **View > Show Versions**.

4 In the **Document Versions** dialog box, for any of the displayed versions, you can take the following actions:
   - Download the document as a compressed (.zip) file.
   - Download the document.

Viewing a document’s history

You can view the history of a document in the Document Management system.

The document history consists of the following information:

- Actions

- Action by user
- Date and Time
- Version
- Notes

To view a document's history

1. In the ServiceDesk portal, click **Documents**.
2. On the **Category View** page, under **Browse**, select the document's category.

   If you cannot find the document, you can perform a search.

   See "Searching for documents" on page 309.
3. In the right pane, to the far right of the document name, click the **Action** symbol (orange lightning), and then click **View > History**.
4. When you finish viewing the history, in the **Documents History** dialog box, click **Cancel**.

Section 9

Communicating in the ServiceDesk portal

Chapter 30

Emailing in the ServiceDesk portal

This chapter includes the following topics:

Sending an email from a process ticket

When you work in a process ticket, you can send an email to one or more users about the ticket. The email is created from a predefined template that you select. You can also edit the email message.

To send an email from a process ticket

1. In the ServiceDesk portal, open an existing ticket or create a new one.
2. On the ticket's **Process View** page, under **My Actions**, click **Send Email**.

3 In the **Email Template Setup** dialog box, take any of the following actions:

To add a group	Under **Add a Group**, click the **Add** link to the right of each group to add.
To add a user	Under **Add a Contact**, click the **Add** link to the right of each user to add.
To search for a group or user that is not listed	Click the **Search for Specific User or Group** link. On the **Select User** dialog box, perform a search, and then click the **Select** link to the right of each user or group to add.

See "Email Template Setup dialog box" on page 318.

4 In **Email Template**, select a template to use.

The templates that appear in the list are associated with the specific ticket type. For example, if you send an email from a change ticket, the templates that you can select are change-related templates.

5 Select one of the following options:

Quick Send	Opens the **Email Preview** dialog box, where you can review and send the message.
Modify and Send	Opens the **Create an Email Message** dialog box, where you can edit the message, add attachments, and send the message. See "Create an Email Message dialog box" on page 319.

6 When the ticket's **Process View** page reappears, you can continue to work the ticket or close it.

Email Template Setup dialog box

This dialog box lets you select the recipients and content of an email message that you send from ServiceDesk. It appears when you click **Send Email** on a ticket's **Process View** page.

See "Sending an email from a process ticket" on page 317.

Most email content is obtained from templates. An email template is a message that contains the predefined content, format, and structure that is used to create individual emails from a ServiceDesk process.

ServiceDesk contains default templates for the core ServiceDesk processes. When an email is triggered within a process, the process selects a template that corresponds to the process ID. For example, if the process ID is IM-000001, then an Incident Management template is selected.

The email templates can be customized in the SD.EmailServices project in Workflow Designer.

For more information about customizing ServiceDesk email, see the *ServiceDesk Customization Guide*.

Table 30-1 Options in the **Email Template Setup** dialog box

Option	Description
Add a Group	Lets you select one or more groups to send the message to. The groups that appear are associated with the ticket type. For example, if you created the email message from an incident, this list includes the support groups.
Add a Contact	Lets you select one or more users or groups to send the message to. The users and groups that appear are associated with the specific ticket.
Search for Specific User or Group	If you do not see a group or user that you need to add, you can perform a search.
Mail to List	Displays the groups and users that you added as the email recipients. You can remove a group or user from this list if necessary.
Email Template	Lets you select the template to use for the email.
Quick Send	Opens the **Email Preview** dialog box, where you can review and send the message. You can use this option when you do not need to change or add to the default content of the email message.
Modify and Send	Opens the **Create an Email Message** dialog box, where you can edit the message, add attachments, and send the message. See "Create an Email Message dialog box" on page 319.

Create an Email Message dialog box

This dialog box lets you create or edit an email message that you send from ServiceDesk. It appears when you create an email message from a process ticket.

See "Sending an email from a process ticket" on page 317.

Table 30-2 Options in the **Create an Email Message** dialog box

Option	Description
To	When the email message is crated from within a process ticket, the contacts that you selected appear here. You can also type the email address for any other recipient. Use a comma to separate multiple addresses.
CC	Lets you type any additional recipients. Use a comma to separate multiple addresses.
Subject	If you created the email from within a process ticket, the subject line contains the ticket ID. It also contains the title from the email template that you selected.
Attachments	Opens the **Add Attachments** page, which lets you attach files to the email message. You can attach any files that are attached to the process ticket, and you can select additional files to attach.
Email Body	Contains the text and the process ticket information that is defined in the email template. You can type additional text.
Include the Reply Code	Generates a reply code that causes any replies to this message to be linked to the process ticket. This option is selected by default.
Preview	Opens the **Email Preview** dialog box, where you can review and send the message.

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.

For example, when a technician resolves an incident, an email that contains information about the resolution is sent to the person who submitted the incident.

ServiceDesk contains default notifications for the following core processes:

- Incident Management
  See "Email notifications from Incident Management" on page 112.
- Problem Management
  See "Email notifications from Problem Management" on page 213.
- Knowledge Management

See “Email notifications from Knowledge Management” on page 253.

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 *Workflow Solution 7.1 SP2 User Guide* at the following URL:

http://www.symantec.com/docs/DOC4824

and see the *ServiceDesk 7.1 SP2 Customization Guide* at the following URL:

http://www.symantec.com/docs/DOC2150

You can also change the default contents of the automatic email notifications.

See “About the contents of email notifications” on page 442.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the ServiceDesk portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted.

See “About process notifications” on page 321.

About process notifications

ServiceDesk can send email notifications as a result of events that occur within the ServiceDesk portal. These notifications are known as process notifications.

For example, notifications can be sent for the events that can occur on documents, discussions, and knowledge base entries. Examples of events are when an item is added, edited, deleted, or accessed.

Process notifications are sent based on the following settings:

The item’s permissions	When you create or edit an item that has process notification capability, it includes notification permissions for the events that can occur on the item. You can set the permissions on the **Permissions** tab that appears when you create or edit the item.
The **Process Notification** option	When you create or edit an item that has process notification capability, this option appears in the editing dialog box. It typically appears on the **Notifications** tab. This option is selected by default.

The process notifications are different from the automatic email notifications that ServiceDesk can send at various stages of a core process.

See "About automatic email notifications" on page 320.

Chapter 31

Chatting in the ServiceDesk portal

This chapter includes the following topics:

About chatting in the ServiceDesk portal

You can chat with other users within the ServiceDesk portal. Use the chat feature to communicate with others in real time by engaging in an instant message-style conversation.

The **Chat** Web part, which lets you participate in a chat session, appears by default on the **Process View** pages for process tickets. An administrator can add the **Chat** Web part and other chat-related Web parts to any place in the ServiceDesk portal.

You can join a chat session in the following ways:

From a chat invitation email	You can click the link in the invitation or paste the URL into a browser window to open the ServiceDesk portal to the chat window. If you are not logged on to the ServiceDesk portal, you are prompted to log on.

From the **Chat** Web part in a process ticket	By default, the **Chat** Web part appears on the **Process View** pages. It can also be added to other areas of the ServiceDesk portal. See "Chatting in the ServiceDesk portal" on page 324.
From the **Chat** Web part in other areas of the ServiceDesk portal	This Web part does not appear by default in areas other than process tickets. The administrator or other user with the appropriate permissions must add it. For example, the **Chat** Web part can be added to the **Home** page. See "Adding a Web part to a ServiceDesk portal page" on page 81.

The portal master settings contain settings for monitoring and saving ServiceDesk chat sessions.

Chatting in the ServiceDesk portal

You can chat with other users about a specific process ticket within the ServiceDesk portal. Use the chat feature to communicate with others in real time by engaging in an instant message-style conversation.

You can start a chat or join an existing one.

Users who are invited to join a chat receive an email notification. If the chat is conducted within a process ticket, the email message refers to the process ID.

See "About chatting in the ServiceDesk portal" on page 323.

To chat about a process ticket

1. Open the chat session as follows:
   - In a chat invitation email, click the link in the invitation or paste the URL into a browser window.
     If you are not logged on to the ServiceDesk portal, you are prompted to log on.
   - In the ServiceDesk portal, open the ticket that is associated with the chat. On the ticket's **Process View** page, expand the **Chat** section, and then click **Open Chat**.

- In the ServiceDesk portal, open any page that contains the **Chat** section (Web part).

2 If you need to invite participants, in the **Process Manager Chat** window, click **Invite New Participant**.

Other participants can be added later. The ability to invite chat participants depends on your permissions.

See "Inviting participants to a chat session" on page 325.

3 (Optional) In the **Process Manager Chat** window, you can select any of the options that appear.

For example, you can capture a screen image and add it to the chat session. The options that are available depend on the type of ticket and your permissions.

See "Process Manager Chat window" on page 326.

4 In the **Process Manager Chat** window, in the text box at the lower right of the page, type the chat message, and then click **Send**.

5 At any time during the chat session, you can click **Save**.

This option opens the **Process Messages** dialog box, where you can save some or all of the chat messages to the process ticket's history.

By default, chat messages are not saved.

6 You can leave the **Process Manager Chat** window open for the duration of the chat session or you can close it and reopen it later.

Inviting participants to a chat session

When you start a chat session, you must invite one or more participants. Other participants can be added later. The ability to invite chat participants depends on your permissions.

See "About chatting in the ServiceDesk portal" on page 323.

To invite participants to a chat session

1 Access the **Process Manager Chat** window.

See "Chatting in the ServiceDesk portal" on page 324.

2 Click **Invite New Participants**.

3 In the **Invite Participants** dialog box, take any or all of the following actions:

- Expand the permissions folders and check the check box to the left of each user to invite.
- Click **Pick** and use the **User Picker** dialog box to search for and select a user.
  You can continue to pick as many users as necessary.
  See "Picking a user" on page 96.

4 When you finish the user selection, in the **Invite Participants** dialog box, click **Invite**.

5 When the **Process Manager Chat** window reappears, you can start or resume the chat.

Process Manager Chat window

This window lets you start and participate in a chat session with other ServiceDesk users. The main section of the window displays the chat messages are they are added. The chat title appears at the top of the window. If the chat session is associated with a process ticket, the chat title is the same as the process name.

See "Chatting in the ServiceDesk portal" on page 324.

Table 31-1 Options in the **Process Manager Chat** window

Option	Description
PARTICIPANTS	Lists the workers who have been invited to participate in the chat session. A blue circle symbol to the left of a participant's name indicates that the participant is active in the chat.
Invite New Participant	Lets you invite one or more participants to the chat session. Participants can be added when the chat session is started and at any time thereafter. The ability to invite chat participants depends on your permissions. See "Inviting participants to a chat session" on page 325.
Process Actions	Lets you perform the actions that are associated with the process task. For example, a support technician who participates in a chat about an incident can resolve the incident or request a change. You can use this option only if you are assigned to perform one or more tasks in the process.
Screen Capture	Opens the Screen Capture utility, which lets you capture screen shots and attach them to the chat. The screen shot files remain available during the chat session. Unless you save the screen shot files, they are lost when the chat session ends. See "Capturing a screen image" on page 97.

Table 31-1 Options in the **Process Manager Chat** window *(continued)*

Option	Description
View/Save Files	Lets you view any files that are associated with the chat session and attach them to the process ticket. The options on the **Send Files** dialog box are as follows: ■ **view** Lets you open a file in a **Preview Page** dialog box. This link appears to the right of each file. ■ **Save** Lets you save and attach any files whose check box you check. The check box appears to the left of each file. Any files that you do not save are lost when the chat session is closed.
Open Process	Opens the **Process View** page for the process that associated wchat session.
Save	Opens the **Process Messages** dialog box, where you can save some or all of the chat messages to the process ticket's history. If you do not save the chat contents, you cannot see them in the process ticket after the chat session is closed. An option in the portal master settings determines whether chat messages for are saved automatically for a specified number of days. The default is zero.
Send	Sends the message that you type to the chat session so that the other participants can read it.

Chapter 32

Holding discussions in the ServiceDesk portal

This chapter includes the following topics:

About discussions in the ServiceDesk portal

You can participate in discussions with other users within the ServiceDesk portal. Use the discussion feature to communicate with others in an open forum environment. Users can post comments and messages to offer insight or answer questions.

Discussions can be created from the **Discussions** page in the ServiceDesk portal. For example, a support technician can start a discussion thread about an incident to get information and feedback on resolving the incident from other technicians.

See "Adding a discussion in the ServiceDesk portal" on page 330.

See "Discussions page" on page 58.

Discussions can also be created from a problem ticket. When a user creates a new problem ticket, a new discussion is created. The name and description of the problem ticket become the title and description of the new discussion. The problem ticket's process ID is added to the discussion title. Problem workers can access the discussion from the problem's **Process View** page. A problem-related discussion can be a valuable tool for finding a resolution to the problem.

See "Creating a new problem ticket" on page 216.

A discussion is displayed as a hierarchy of information, as follows:

Discussion	The highest level in the hierarchy. Typically, a discussion encompasses a single subject or problem.
Thread	A subtopic of a discussion. You can use threads to better organize the **Discussions** page.
Post	A subtopic of a thread or of another post. You can create a new post for a thread, or you can reply to an existing post. Replies become the children of the original post. A single post can have multiple layers of replies.

Permissions can be set at the discussion level. The permissions determine who can create, edit, view, and participate in a discussion.

The participants in a discussion can rate the discussion's posts. The participant ratings are accumulated and displayed on the **Discussions** page.

The discussion ratings are as follows:

- Poor(1)
- Average(2)
- Good(3)
- Very Good(4)
- Excellent(5)

Adding a discussion in the ServiceDesk portal

A discussion is the highest level in the discussion hierarchy. You can create a discussion in the ServiceDesk portal.

Typically, a discussion encompasses a single subject or problem.

Discussions can also be added through the Product Management process.

See "About discussions in the Problem Management process" on page 215.

To add a discussion

1. In the ServiceDesk portal, click **Knowledge Base > Discussions**.
2. On the **Discussions** page, click **Add Discussion**.

3 On the **Add Discussions** dialog box, click the **Edit Discussion Info** tab and provide a title and a description for the discussion.

   This information identifies the discussion on the **Discussions** page.

4 (Optional) To enable email notifications of the events that occur on this discussion, click the **Notifications** tab, and then verify that **Process Notifications** is selected.

   See "About process notifications" on page 321.

5 In the **Add Discussions** dialog box, click the **Permissions** tab, and then specify the permissions for one or more users, groups, permissions, or organizational units.

   See "Setting permissions" on page 95.

6 When you finish defining the discussion, on the **Add Discussions** page, click **Save**.

Adding a thread to a discussion

A thread is a subtopic of a discussion. You can use threads to better organize the **Discussions** page.

See "About discussions in the ServiceDesk portal" on page 329.

Users cannot post messages at the discussion level. Instead, they can post to threads.

See "Participating in a discussion in the ServiceDesk portal" on page 332.

To add a thread to a discussion

1. In the ServiceDesk portal, click **Knowledge Base > Discussions**.
2. If the discussion does not appear in the list, in **Search**, type the text to search for, and then click the **Search** symbol.
3. At the right of the discussion's header bar, click the **Add Thread** symbol (a white page with a green plus sign).
4. In the **Add Thread** dialog box, on the **Thread Information** tab, type the title and the body text for the thread.
5. (Optional) In the **Add Thread** dialog box, on the **Thread Description** tab, type a description to further identify the thread.
6. When you finish defining the thread, click **Save**.

Participating in a discussion in the ServiceDesk portal

You can participate in discussions with other users within the ServiceDesk portal. Use the discussion feature to communicate with others in an open forum environment.

When you participate in a discussion, you can add threads, add posts, and reply to existing posts. Your ServiceDesk permissions determine which discussions you can edit, view, and participate in.

See "About discussions in the ServiceDesk portal" on page 329.

To participate in a discussion in the ServiceDesk portal

1 In the ServiceDesk portal, access the discussion in any of the following ways:

From the portal	Click **Knowledge Base > Discussions**. If the discussion does not appear in the list, in **Search**, type the text to search for, and then click the **Search** symbol.
From a problem ticket	On the problem's **Process View** page, under **Smart Tasks**, click **Go to Discussion**.

2 Expand the discussion section to view the posting history.

3 If a series of five stars appears under the post's text, you can rate the post by selecting one of the stars.

The first star is the lowest rating, and the last star is the highest rating.

The stars do not appear for the posts that you created.

4 If you plan to post any information that is not related to the discussion's existing threads, create a new thread.

See "Adding a thread to a discussion" on page 331.

5 You can add to the existing discussion in the following ways:

Post to a thread.	At the right of the thread's title bar, click the **Add Post** symbol (a white page with a green plus sign). In the **Add Post** dialog box, type and post the message text.
Reply to a post.	At the right of the post's title bar, click the **Reply** symbol (a white text balloon). In the **Reply** dialog box, type and save a reply to the selected post.

Section 10

Managing reports

Chapter 33

Viewing and organizing reports

This chapter includes the following topics:

About ServiceDesk reporting

ServiceDesk includes a large number of predefined reports that provide easy access to the ServiceDesk data. The predefined reports meet the ITIL need of many organizations. However, reports can be customized and new reports can be created to meet your organization's specific requirements.

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 eliminates the need to use SQL for report creation.
- You can add a report to any ServiceDesk portal page or dashboard, and you can define the size and placement of the report.
- During report creation, you can add run-time filters to the report definition. Run-time filters let users scope the reports based on the data that they want to see.

You can view and customize reports on the **Reports** page.

See "Reports page" on page 64.

Viewing a report

You can view reports in the ServiceDesk portal on the **Reports** page or on any portal page that includes reports. For example, the **My Task List** page and the **Tickets** pages include reports.

Your permissions determine the reports that you can view.

To view a report on the Reports page

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report to view.
3. In the right pane, under **Reports**, take any of the following actions:
   - Click the report name.

- Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **View**.

4 (Optional) To take action on the report, click the **Actions** symbol (orange lightning), and then select the appropriate option.

See "What you can do with a report" on page 337.

What you can do with a report

When you view a report in ServiceDesk, you might have additional options for interacting with that report.

See "Viewing a report" on page 336.

All the options are available on the drop-down list that appears when you click the **Actions** symbol (orange lightning) on the **Reports** page.

Your permissions determine the options that are available to you. For example, typical actions are to print the report or export it

Table 33-1 Options for working with reports

Option	Description
Add Child Report	Lets you create a child report. See "About child reports" on page 346.
Categories	Lets you view the categories that the report belongs to and add the report to additional categories. See "Adding reports to additional categories" on page 345.
Copy	Lets you make a copy of the report so that you can create a new report based on the current report. You can customize the copy of the report without having to recreate the report settings. See "Copying a report" on page 339.
Delete	Lets you delete the report. See "Deleting reports" on page 341.
Edit	Lets you edit the report. See "Modifying standard reports" on page 355.

Table 33-1 Options for working with reports *(continued)*

Option	Description
Export Report	Lets you export the report definition to an XML schema file, which lets you or another user run the report from another ServiceDesk instance. See “Exporting a report definition” on page 340.
Permissions	Lets you set the permissions for the report. See “Setting permissions for a report” on page 338.
Print View	Displays the report in Print View, which shows you how the report appears when it is printed. See “Displaying reports in print view” on page 338.
Schedules	Lets you view the reports that contain the report or create a new schedule for the report. See “Creating a report schedule” on page 358.
View	Opens the report.

Displaying reports in print view

You can display any report in Print View, which shows you how the report appears when it is printed.

To display a report in print view

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Print View**.

Setting permissions for a report

An administrator or other user who has the appropriate permissions can set permissions for a report. The report permissions control the access to and use of that report. For example, you can specify which users or groups can view, edit, delete, or create subreports for a report.

To set permissions for a report

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Permissions**.
4. In the **Report Permissions** dialog box, add or edit permissions as needed.

   See "Setting permissions" on page 95.
5. When you finish setting permissions, click **Close**.

Copying a report

Copying an existing report lets you create a new report that is customized to your needs, without having to recreate the report settings. You can copy a report that has almost all of the information you need, and then add, remove, and edit the report. Modifying the copied report lets you get what you are want in the report. Administrators, and the users with the appropriate permissions can copy reports. By default, Administrators can copy a report that is located in any category. Other users cannot copy a report that is in a category for which they do not have permission to create reports.

To copy a report

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Copy**.
4. In the **Report Information** dialog, enter a new name for the report in the **Report Name** field.
5. Optionally, enter a description for the report in the Report Description field. The description text you enter appears under the report name on the **Reports** tab, when you expand a report entry.
6. Click **Save**.

Exporting a report definition

Any report definition can be exported to an XML schema file. When you export a report definition, the report settings are exported so that the report can be run from another ServiceDesk system. The actual report data is not exported when you use the export report feature. You have the option of saving or viewing the XML file. Any user that has access to view a report has permission to export it.

To export a report

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Export Report**.
4. In the **File Download** dialog box, click either of the following options:

Open	Opens the XML file for viewing.
Save	Saves the file on your computer.

Importing reports

You can import reports from another instance of ServiceDesk.

To import reports

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category to import reports to.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Import Reports**.
4. In the **Import** dialog box, click **Browse** and select the report file that you want to import.
5. Select one of the following options to determine whether ServiceDesk overwrites or copies existing reports:
   - Overwrite existing reports - ServiceDesk overwrites reports with the same report ID.
   - Create new copy - ServiceDesk creates new copies of all the reports.
6. Click **Import**.

Adding reports to a portal page

Any ServiceDesk reports can be added to a portal page. Administrators and users with the appropriate permissions to modify portal pages can add reports.

To add a report to a portal page

1. In the ServiceDesk portal, select the portal page you want to add the report to.
2. Select **Site Actions > Modify Page**.
3. Select **Site Actions > Add Web Part**.
4. Select **Reports** in the **Catalog List.**.
5. Select the **Standard Report Viewer** check box to add a standard report.
6. In **Add to**, select the zone to add the report to.
7. Click **Add**. The Report Viewer web part is added to the portal page.
8. Click **Close**.
9. Click the **Report Selection** icon and select the report that you want to display in the **Report Viewer** web part.

Deleting reports

You can delete any report that you have delete permissions for from the Reports tab.

To delete a report

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category that contains the report.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Delete**.
4. Click **OK** in the confirmation dialog box.

About report categories

ServiceDesk uses categories to classify its reports. The report categories help the ServiceDesk workers find the reports that they need. You can use additional levels of categories to group the reports further. A report category can have multiple subcategories, and you can nest the subcategories.

ServiceDesk contains a hierarchy of predefined report categories, which organize the default ServiceDesk reports. You can add categories and manage the existing ones on the **Reports** page in the ServiceDesk portal.

See "Adding report categories" on page 342.

You can set permissions for the report categories and subcategories. The permissions determine who can access a report category and all the reports that it contains.

See "Setting permissions for a report category" on page 344.

Adding report categories

Report categories assist you in organizing all of the reports that are located on the Reports page. Organizing the reports in categories helps users find the reports they need more easily. You can also apply permissions to categories, which deny or grant access to that category and all the reports within it.

See "Setting permissions for a report category" on page 344.

To add a report category

1. In the ServiceDesk portal, click **Reports**.
2. On the Documents page, under **Report Categories**, click **Add Report Category**.
3. In the **Category Information** dialog box, in the **Name** text box, type a name for the category.
4. (Optional) In the **Header Text** text box, type descriptive text. The text is displayed under the category name on the right-hand side of the Reports page when a user selects the category.
5. Click **Save**.

Adding report subcategories

Report subcategories can assist with further organizing the categories and reports that are located on the Reports page. You can add subcategories to any category if you have the necessary permissions to do so.

To add a report subcategory

1. In the ServiceDesk portal, click **Reports**.
2. On the Reports page, under **Report Categories**, select the category that you want to add a subcategory to.

3 On the right side of the page, click the orange lightning symbol, and then click **New Sub Category**.

4 In the **Category Information** dialog box, in the **Name** text box, type a name for the subcategory.

5 (Optional) In the **Header Text** text box, type some descriptive text. The text is displayed under the category name on the right-hand side of the **Reports** page when a user selects the category.

6 Click **Save**.

Deleting report categories

Users with the appropriate permissions can delete report categories. When you delete report categories, the subcategories and the reports that are contained in that category are not necessarily deleted. You can make selections during the deletion process, which determines what happens to the subcategories and the reports that are contained in a report category.

To delete a report category

1 In the ServiceDesk portal, click **Reports**.

2 On the **Reports** page, under **Report Categories**, select the category to delete.

3 On the right side of the page, click the **Actions** symbol (orange lightning), and then click **Delete**.

4 In the **Delete Category** dialog box, select one of the following options for handling any subcategories that are contained in the category:

Don't delete SubCategories	Retains all subcategories that are contained in the parent category. The subcategories are moved up to the root level.
Delete SubCategories	Deletes all subcategories that are contained in the parent category. If reports in that category also belong to another category, they remain in the other categories. If reports do not belong to other categories, they are moved to the Orphan category.
Delete SubCategories and all reports in them	Deletes all subcategories and the reports they contain.

Select one of the following options for handling any reports that are contained in the category:

Don't delete reports	Retains all reports that are contained in the category.
Delete reports (that are linked only to the deleted category)	Deletes all the reports that are contained in the category, as long as they are linked only to the deleted category. If the reports are linked to additional categories, they are retained.
Delete reports even if linked to multiple categories	Deletes all reports that are contained in the category, even if they are linked categories other than the one being deleted.

5 Click **Delete**.

Setting permissions for a report category

Report categories help you organize all of the reports that are located on the Reports page. Organizing the reports in categories helps users find the reports they need more easily. You can apply permissions to categories, which deny or grant access to that category and all the reports within it. By default, the category inherits the permissions of the user who created it. If you want the permissions to be different for other users of the category, you need to modify the category permissions.

An administrator or other user who has the appropriate permissions can set permissions on a report. The report permissions control the access to and use of that report. For example, you can specify what users or groups can view, edit, delete, or create subreports for a report.

To set permissions for a report category

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, select the category.
3. In the right pane, at the far right of the category's title bar, click the **Actions** symbol (orange lightning), and then click **Permissions**.
4. In the **Category Permissions** dialog box, add or edit permissions as needed.

   See "Setting permissions" on page 95.
5. When you finish setting permissions, click **Close**.

Adding reports to additional categories

When a report is first added to ServiceDesk, it is assigned to a single category. You can add a report to any number of additional categories.

To add a report to additional categories

1. In the ServiceDesk portal, click **Reports**.
2. On the Reports page, under **Report Categories**, select the report's category.
3. In the right pane, at the far right of the category's title bar, click the **Actions** symbol (orange lightning), and then click **Categories**.
4. In the **Report Category Management** dialog box, click the **Add New Category** tab.
5. Select the category that you want to add the report to and click **Add**.
6. Click **Close**.

Importing a report category

You can import report categories from another instance of ServiceDesk.

To import a report category

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, under **Report Categories**, click **Import Category**.
3. In the **Import** dialog box, click **Browse** and select the report file.

4 Select one of the following options:

Overwrite existing reports	Overwrites any reports that have the same report ID as an imported report.
Create new copy	Creates new copies of all the reports.

5 Click **Import**.

About child reports

The use of child reports in ServiceDesk lets you create and edit a copy of a report. If you need to add custom information to a report, you can make the changes without affecting the original report definition. When you create a child report, you can add data but not subtract it.

Child reports are created from the **Reports** page, using the **Child Reports** option that appears when you click the **Actions** symbol (orange lightning).

Chapter 34

Creating and customizing standard reports

This chapter includes the following topics:

Creating a standard report

Administrators and users with the appropriate permissions can create reports.

To create a new report

1. In the ServiceDesk portal, select **Reports**.
2. In the **Report Categories** area, select the category that you want the report to reside in. The report that you create is added to the category that you select.
3. Click the **Add Report** icon, and select **Add Standard Report**.
4. In the **Name** field, enter a name for the report. Report names must be unique. The **Name** field has a 100 character limit.

5 In the **Report Designer** tab, specify the data that you want included in the report and the display of that data.

See "Setting up or modifying the data in standard reports" on page 348.

6 (Optional) In the **Description** tab, enter a description for the report which appears on the Reports portal page underneath the report. The description should make it easy for users to quickly understand the information that the report contains. The description text is also searched when users search for reports. The description has no character limit.

7 On the **Permissions** tab, add or edit the permissions as needed.

See "Setting permissions" on page 95.

8 (Optional) On the **Web Services** tab, set up Web Service access for the report.

See "Setting up or modifying Web Service access for standard reports" on page 351.

9 Click **Save**.

Setting up or modifying the data in standard reports

The data that is included and displayed in reports is completely customizable. On the **Report Designer** tab, you can specify the information that should be included in a report, as well as criteria to narrow the report results. The information that you specify in this tab can both add to and restrict the data that appears in the report.

Selecting a check box for a type of data to add to the report includes all of the fields available for that section in the report. The available fields are displayed in the **Data** section. Selecting the check box for one of the fields lets you apply filters to the data that is returned in that field.

For example, if you wanted information about Incident Management in the report, you would select the checkbox to expand the Incident Management section. Selecting that checkbox adds all of the fields in the Incident Management table to the report. If you want to display the data from a particular field, you need to add the particular column to the report.

However, you may only be interested in seeing the incidents that have an SLA status of "late". When you select the "SLA Status" checkbox, the SLA Status dialog opens. This dialog lets you narrow the results of the report, by checking the "Late" checkbox and clicking OK. Selecting this checkbox narrows the report results so that only incidents with an SLA status of "late" are shown.

As you work in the **Preview** pane, it displays the results of the report as you build it. After every change that you make, the display refreshes. If the constant refreshing becomes cumbersome, you can uncheck the **Auto Preview** option as you work. You can reselect the option whenever you need to see an updated preview of the report.

To set up or modify the data and display of standard reports

1. In the ServiceDesk portal, select **Reports**.
2. On the **Reports** page, do one of the following:
   - Create a new report.
     See "Creating a standard report" on page 347.
   - Modify an existing report.
     See "Modifying standard reports" on page 355.
3. In the **Add/Edit Standard Report** dialog box, select the **Report Designer** tab.

   See "Add/Edit Standard Report dialog box" on page 352.
4. On the **Data** tab, select the check box for the type of data that you want to include in the report.

   When you select a data type, all of the data fields of that type are added to the report. All of the data fields are available for display in the report. Data types that are included in the report have a green check mark next to them. Repeat this step for all of the data types that you want to include in the report.
5. (Optional) To filter the data that is included in the report, select the check box next to the field that you want to filter.

   The fields to which you have applied filtering have a green check mark next to them. For example, you may want to filter incidents so that only those with a priority of high are shown in the report. In the dialog that appears, set the parameters for the filter, and click **OK**.
6. In the **Columns** area, select the check box for the columns that you want to display in the report. Repeat this step for all of the columns that you want to include in the report. Columns that are included in the report have a green check mark next to them, and are displayed at the top of the columns area.
7. (Optional) Customize the layout of the report.

   See "Customizing the layout of grid standard reports" on page 350.
8. (Optional) Customize the filtering and sorting of the report.

   See "Customizing the filtering and sorting for standard reports" on page 350.
9. Click **Save**.

Customizing the layout of grid standard reports

You can view the layout of a report as you work on it. The report preview pane, in the center of the **Report Designer** tab, shows you how the report currently looks.

See "Add/Edit Standard Report dialog box" on page 352.

When **Auto Preview** is selected, the changes you make to your report are shown as you make them. If you make a lot of changes, you may want to turn off Auto Preview. When Auto Preview is turned off, you do not have to wait for each change to be reflected in the preview pane. If you have turned off Auto Preview, you can click **Generate** to see the current report with all of your changes.

When **Limit Results** is selected, the report results are limited to the top 50 results. When you limit results, you can see how the report looks without showing a large amount of data in the report preview pane.

You can customize the layout of grid standard reports in the following ways:

- Move columns in the report by selecting the left arrow or right arrow for the column in the report preview pane.
- Delete a column by selecting the red x for the column in the report preview pane.
- Change the name of a column by moving your mouse over the column name in the **Columns** section, and clicking the **Edit** option. Edit the title of the column and click **OK**.
- Adjust column width by placing the mouse arrow over the column and dragging to get the desired width.
- Apply special formatting to columns in the report by adding renderers. For example, you can set up your report so that high priority incidents appear in red. To apply the formatting, you would move your mouse over the column name in the **Columns** section, and click the **Edit** option. Select the type of renderer to apply, click **Add Renderer**, enter the text to search for, select a fore color of red, and click **OK**.

Customizing the filtering and sorting for standard reports

You can specify the grouping, sorting, and paging options for a report.

To customize the filtering and sorting for a report

1. In the ServiceDesk portal, select **Reports**.
2. On the Reports page, do one of the following:
   - Create a new report.
     See "Creating a standard report" on page 347.
   - Modify an existing report.
     See "Modifying standard reports" on page 355.
3. In the **Add/Edit Standard Report** dialog box, select the **Report Designer** tab.

   See "Add/Edit Standard Report dialog box" on page 352.
4. (Optional) In the **Report Designer** tab, select **Options**.
5. Select the **Limit Rows** check box to limit the number of rows that are returned with the report. The default number of rows that are returned is 50. When you select this option, the user is able to configure the number of rows that are returned at run time.
6. Select the **Use Paging** check box, and specify the number of rows per page for the report.
7. Select a column in the **Sort By** drop-down list to sort the report by that column, and select ascending or descending sort order.
8. Select up to three columns to group the report by in the **Group By** drop-down lists.
9. To add aggregations to your groups, under **Group Aggregations**, select a column to aggregate a group by and the type of aggregation, and then click **Add Aggregation**. Aggregations summarize mathematical data at the group level. For example, you can set up an aggregation that displays the average age of a ticket per location.
10. Click **Display SQL** to display the SQL statement that the report executes against the database.
11. Click **Save**.

Setting up or modifying Web Service access for standard reports

Setting up web service access for a report allows programmatic access to that report.

The Web service access is required if you plan to configure schedules automatically execute and email reports.

See "Scheduling automatic report emails" on page 357.

To set up or modify Web Service access for standard reports

1. In the ServiceDesk portal, click **Reports**.
2. On the **Reports** page, do one of the following:
   - Create a new report.
     See "Creating a standard report" on page 347.
   - Modify an existing report.
     See "Modifying standard reports" on page 355.
3. In the **Add/Edit Standard Report** dialog box, click the **Web Services** tab.

   See "Add/Edit Standard Report dialog box" on page 352.
4. On the **WebService** tab, click the check box to enable programmatic access to the report. To enable WebService Access, enter the following information:

Namespace	The namespace for the WebService and the objects that are used in the web service.
Namespace URL	The URL for the namespace.
WebService Name	A name that describes the service, such as "OpenIncidentsThisMonthReport".
Class Name	The results of the report are an array of the class name that is supplied here. The class name has public properties for each of the columns in the report.

   Click **Generate** to compile the WebService and deploy it to a URL.

   The URL is displayed on the screen and can be used to access the WebService. When report data changes, you need to generate the WebService again to update the class.
5. Click **Save**.

Add/Edit Standard Report dialog box

This dialog box appears when you create or edit a standard report.

The **Add/Edit Standard Report** dialog box has four tabs.

Table 34-1 Tabs in the **Add/Edit Standard Report** dialog box

Tab	Description
Report Designer	Lets you specify what data is included in the report and specify options for that data. You can also specify the sorting and grouping of the resulting data, and specify columns for the resulting data set. Table 34-2
Description	Lets you specify a description of the report which is displayed on the Reports page.
Permissions	Lets you specify the permissions for the report. Table 34-3
Web Services	Lets you enable Web Service access to the report. Table 34-4

Table 34-2 Options on the **Report Designer** tab

Option	Description
Data tab	Lets you specify the type of data that is included in the report.
Grid	Displays the current report in grid view in the report preview pane. Whichever pane is displayed when you save the report is the type of report that anyone viewing the report sees.
Chart	Displays the current report in chart view in the report preview pane. Whichever pane is displayed when you save the report is the type of report that anyone viewing the report sees.
Auto Preview	Displays a preview of the current report as you build it. Auto Preview is selected by default.
Limit Results	Limits the result set of the report that is shown in the report preview pane to 50. The Limit Results option is selected by default.
Generate	When Auto Preview is not selected, clicking Generate lets you view the report in the report preview pane with all the changes you have made.
Columns	Lets you specify the columns that are displayed in the report.
Options tab	Lets you specify the grouping and sorting of the data in the report.

Table 34-2 Options on the **Report Designer** tab *(continued)*

Option	Description
Limit Rows	Lets you specify the maximum number of rows that are included in the report. The default number of rows is 50, and users can configure the number of rows they want to see in the report at run time.
Use Paging	Lets you specify the number of rows per page in the report.
Sort By	Lets you specify the columns to sort by and whether the data in those columns should be sorted in ascending or descending order.
Group By	Lets you specify the columns to group by.
Group Aggregations	Lets you add group aggregations. Group aggregations summarize mathematical data at the group level. For example, you might want to add an aggregation to a report that shows the average age of a ticket per location.
Add Aggregation	Lets you add aggregations to the report. Any number of aggregations are allowed.
Display SQL	Displays the SQL statement for the report.

Table 34-3 Options on the **Permissions** tab

Option	Description
Rows in the tab	Lists the current permissions that are assigned to the report.
Edit icon	Lets you edit the permissions for that user, group, permission, or organization.
Delete icon	Lets you delete that permission.
Add New Permission	Lets you add a new permission.

Table 34-4 Options on the **Web Services** tab

Option	Description
Enabled for programmatic access	Lets you enable the report for programmatic access. Selecting this check box displays the fields that you need to specify to set up Web Service access.
Namespace	The namespace for the WebService and the objects that are used in the webservice.

Table 34-4 Options on the **Web Services** tab *(continued)*

Option	Description
Namespace URI	The URI for the namespace.
WebService Name	A name that describes the service, such as "OpenIncidentsThisMonthReport".
Class Name	The results of the report are an array of the class name that is supplied here. The class name has public properties for each of the columns in the report.
Generate	Compiles the Web Service and deploys it to a URL. The URL is displayed on the screen and can be used to access the WebService. When report data changes, you need to generate the WebService again to update the class.

Modifying standard reports

You can modify any report for which you have the appropriate permissions. You are more likely to spend time modifying existing reports than creating new reports. ServiceDesk includes many predefined reports that meet most of your reporting needs. When you want to make a small change to an existing report, copy the existing report and make your changes in the new report. By copying the report instead of making modifications directly to a predefined report, you can always go back to the original report.

To modify a standard report

1. In the ServiceDesk portal, select **Reports**.
2. On the Reports page, under **Report Categories**, select the category that contains the report that you want to modify.
3. Under **Reports**, at the far right of the report name, click the **Actions** symbol (orange lightning), and then click **Edit**.
4. In the **Edit Standard Report** dialog box, edit the report.

   The dialog and tabs for editing and adding standard reports are the same.

   See "Creating a standard report" on page 347.

   See "Add/Edit Standard Report dialog box" on page 352.
5. Click **Save**.

Chapter 35

Scheduling reports

This chapter includes the following topics:

Scheduling automatic report emails

You can automatically execute and email reports on one or more schedules that you define. You can send the reports in Excel, CSV, or HTML format.

Before a report schedule can run, you must set up Web service access.

See "Setting up or modifying Web Service access for standard reports" on page 351.

Table 35-1 Process for scheduling automatic report emails

Step	Action	Description
Step 1	Create a report schedule.	The schedule defines when the report emails are sent. See "Creating a report schedule" on page 358.
Step 2	Add reports to the schedule.	You can specify one or more reports to include in the scheduled email message. See "Adding a report to a report schedule" on page 359.

Creating a report schedule

You can create a schedule for emailing reports in several formats.

After you create the schedule, you must select the reports to send.

See "Adding a report to a report schedule" on page 359.

To create a report schedule

1. In the ServiceDesk portal, click **Admin > Reports > Report Schedule List**.
2. In the upper right of the **Report Schedules** section, click the **Add Report Schedule** symbol (a white page with a green plus sign).
3. In the **New Report Schedule** dialog box, name and configure the schedule.

   The type of schedule that you select determines the schedule settings that appear.
4. When you finish configuring the schedule, in the **New Report Schedule** dialog box, click **Save**.

New Report Schedule dialog box

This dialog box lets you configure schedules for sending report emails.

Table 35-2 Options in the **New Report Schedule** dialog box

Option	Description
Name	Lets you provide a unique, descriptive name for the schedule so that it can be easily recognized in the **Report Schedules** section.
Active	Makes the schedule active so that the report runs at the scheduled times. You can uncheck this check box at any time to disable this schedule temporarily.
Select type of schedule	Lets you schedule the report to run in one of the following intervals: ■ **Daily (number of days)** ■ **Weekly** ■ **Monthly** ■ **One time only** The type of schedule that you select determines the remaining schedule options that appear in this dialog box. These schedule options are the same for several other types of schedules. See "Options for scheduling reports and events" on page 359.

Table 35-2 Options in the **New Report Schedule** dialog box *(continued)*

Option	Description
Advanced	Opens the **Advanced** dialog box, which lets you set the report task to repeat after a specified number of minutes or hours, until a specified time. For example, you can set a report to run every four hours on the scheduled days. This option is not available for a one-time-only schedule.

Adding a report to a report schedule

After you create a schedule for emailing one or more reports, you must select the reports to send.

See "Creating a report schedule" on page 358.

To add a report to a report schedule

1. In the ServiceDesk portal, click **Admin > Reports > Report Schedule List**.
2. Under **Report Schedules**, find the schedule, click the **Actions** symbol (orange lightning) at the far right of the schedule name, and then click **Reports**.
3. In the **Reports** dialog box, click **Add Report**.
4. Under **Reports List**, specify the report to run, the addresses to send it to, and the format to send, and then click **Add**.
5. To add more reports, repeat step 3 through step 4.
6. When you finish adding reports, in the **Reports** dialog box, click **Close**.

Options for scheduling reports and events

In ServiceDesk, you can schedule the following types of reports and events:

Report emails	You can create schedules to email reports. See "Scheduling automatic report emails" on page 357. You schedule the report emails in the **New Report Schedule** dialog box. See "New Report Schedule dialog box" on page 358.

Database replication	You can create schedules for replicating the Process Manager database. See "Scheduling the database replication" on page 379. You schedule the database replication in the **New Replication Schedule** dialog box. See "New Replication Schedule dialog box" on page 380.

These schedule dialog boxes let you schedule the event to run in one of the following intervals:

- **Daily (number of days)**
  See Table 35-3.
- **Weekly**
  See Table 35-4.
- **Monthly**
  See Table 35-5.
- **One time only**
  See Table 35-6.

The options that appear for each of these intervals are the same regardless of the type of schedule you define.

Table 35-3 Daily scheduling options in the schedule dialog boxes

Option	Description
Start date & time	The date and time at which the event begins.
End Date	The date on which the event ends.
Perform this task	Lets you specify the days on which the event should occur, as follows: ■ **Every Day** ■ **Weekdays** ■ **Every** (number of days) The interval of days between the event occurrences.

Table 35-4 Weekly scheduling options in the schedule dialog boxes

Option	Description
Start time	The time at which the event begins.
End Date	The date on which the event ends.

Table 35-4 Weekly scheduling options in the schedule dialog boxes *(continued)*

Option	Description
Every (number of weeks)	Lets you specify an interval of weeks between the event occurrences.
Select the day(s) of the week below	Lets you specify one or more days on which the event occurs every week. For example, you can run a report on Tuesday and Friday of the scheduled week.

Table 35-5 Monthly scheduling options in the schedule dialog boxes

Option	Description
Start time	The time at which the event begins.
End Date	The date on which the event ends.
Perform this task	Lets you specify the days of the month on which the event should occur, as follows: ■ **Day** The **Days** link that appears to the right of this option lets you select the days of the month on which the event should occur. ■ **The** The **Weeks** and **Weekdays** links that appear to the right of this option let you select the weeks of the month and the days of the week on which the event should occur.
Of the month(s)	Lets you select the months in which the event should occur.

Table 35-6 One-time-only scheduling options in the schedule dialog boxes

Option	Description
Start date & time	The date and time at which the event occurs.

Section 11

Setting up and managing ServiceDesk

Chapter 36

Configuring the ServiceDesk application

This chapter includes the following topics:

- Migrating categories from Helpdesk Solution

About configuring the ServiceDesk application software

The installation of the ServiceDesk application software includes an initial configuration of the ServiceDesk portal. The initial configuration lets you select the parts of ServiceDesk to install, configure communication settings, and install sample data.

Because ServiceDesk contains predefined, ITIL-compliant settings, it is ready to use as soon as you set up the ServiceDesk users. However, most organizations prefer to perform some level of customization to incorporate their specific procedures and processes. Your organization can decide how much customization it needs.

Before you begin to configure the ServiceDesk application software, you must install it and perform additional setup tasks.

See “Before you configure the ServiceDesk application software” on page 366.

See “Configuring the ServiceDesk application software” on page 367.

Before you configure the ServiceDesk application software

Before you begin to configure the ServiceDesk application software, you must install it and perform additional setup tasks.

See “Configuring the ServiceDesk application software” on page 367.

Table 36-1 Tasks to perform before you configure the ServiceDesk application software

Task	Description
Install ServiceDesk and perform the initial configuration.	The initial configuration task continues the installation of the ServiceDesk application software.
(Optional) Migrate data from a previous version of Helpdesk Solution, if necessary.	You can also migrate the data from within the ServiceDesk portal.

Table 36-1 Tasks to perform before you configure the ServiceDesk application software *(continued)*

Task	Description
Verify or create groups, permissions, and users.	If you use Active Directory authentication for ServiceDesk, you must set up AD server connections and Active Directory sync profiles. Once you add the sync profiles, you can import the users and groups from Active Directory. See "About Active Directory synchronization" on page 404. See "Managing Active Directory server connections" on page 407. See "Managing Active Directory sync profiles" on page 418. During the creation of the sync profiles, you also had the ability to map the default ServiceDesk groups to the Active Directory group names. Review the imported information to verify its accuracy and edit it if necessary. You can view the group, permission, and user information in the ServiceDesk portal by clicking the **Admin** tab and then clicking **Users**. If you use native authentication for ServiceDesk, you must add the users in the ServiceDesk portal. ServiceDesk contains predefined groups and permissions, which you can use or modify. Assign the new users to the appropriate groups. See "Default ServiceDesk user groups" on page 473.

Configuring the ServiceDesk application software

Because ServiceDesk contains predefined, ITIL-compliant settings, it is ready to use as soon as you set up the ServiceDesk users. However, most organizations prefer to perform some level of customization to incorporate their specific procedures and processes.

See "About configuring the ServiceDesk application software" on page 366.

Before you begin to configure the ServiceDesk application software, verify that it is installed and that you have performed the required setup steps.

See "Before you configure the ServiceDesk application software" on page 366.

Table 36-2 lists the configurations that are available. Perform the configuration tasks that are necessary to incorporate your organization's specific procedures and processes into ServiceDesk.

Many of the configuration tasks are performed in Workflow Designer and other tasks are performed in the ServiceDesk portal. Most of the configuration tasks that are performed in the ServiceDesk portal require administrator permissions.

For more information about any of the Workflow Designer tasks, see the *ServiceDesk Customization Guide* and the *Workflow Solution User Guide*.

Table 36-2 Configurations for the ServiceDesk application software

Action	Description
Set up 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 ServiceDesk portal for use in future incidents. Review the existing categories and edit or add to them if necessary. See "About incident categories and the data hierarchy" on page 431.
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 372. 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. However, most ServiceDesk implementations either use the default values or make only minor changes. You can make these changes by editing SD.GeneralIncidentSubmitForm in Workflow Designer.
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 460. See "Adding and deleting incident close codes" on page 461.
Configure the ServiceDesk portal master settings.	The ServiceDesk portal master settings determine the behavior of the ServiceDesk application software and portal. The 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 "About the ServiceDesk portal master settings" on page 462.

Table 36-2 Configurations for the ServiceDesk application software *(continued)*

Action	Description
Customize the appearance of the ServiceDesk portal.	You can customize the appearance of the ServiceDesk portal in the following ways: ■ Customize the general appearance by adding a company logo and selecting a theme, menu style, and other appearance-related features. You can perform this customization in the ServiceDesk portal, in the **Customization** section of the portal master settings. See “Editing the ServiceDesk portal master settings” on page 463. ■ 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 ServiceDesk portal pages” on page 76.
Customize the appearance and content of forms.	In the ServiceDesk 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. You can use Workflow Designer to customize the appearance and behavior of the forms in the ServiceDesk portal. See “About customizing forms” on page 435. Examples of common form customizations are as follows: ■ Setting permissions for forms. See “Setting permissions for a form” on page 438. ■ 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 438.
Establish rules for routing incidents.	Routing rules determine the users or groups that new ServiceDesk incidents are assigned to. The rules also determine how incidents are escalated. ServiceDesk contains predefined routing rules and other settings that are ready to use, but you can customize them to meet your organization’s requirements. Most organizations perform some level of customization. See “About incident routing and escalation” on page 167. You can customize the routing rules by editing the SD.RoutingRules project in Workflow Designer.

Table 36-2 Configurations for the ServiceDesk application software *(continued)*

Action	Description
Establish Service Level Agreement (SLA) times.	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. See "About the Service Level Agreement and Operating Level Agreement" on page 375. See "About the Service Level Agreement (SLA) time frames" on page 376. A default SLA is built in to the Incident Management process in ServiceDesk. You can edit the default SLA time frames and you can set up the SLA in any custom process that you create.
Set business hours and holidays.	Business hours are the hours during which your business is commonly conducted. You can customize your organization's business hours on a global, project, or component basis. See "About business hours and holidays" on page 377. You set the global business hours in the Business TimeSpan Editor, which is installed as a Workflow Designer tool. You set the business hours for a specific project or component by editing it in Workflow Designer.
Set up Follow the Sun routing.	Follow the Sun routing lets you set incidents to be passed to or picked up by another service location when the originating office closes. See "About Follow the Sun routing" on page 378. You set up the Follow the Sun routing by editing the SD.FollowTheSun project in Workflow Designer.
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 130. See "Creating an incident template" on page 137.
Customize email for ServiceDesk processes.	ServiceDesk can send email notifications when various 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 441.

Table 36-2 Configurations for the ServiceDesk application software *(continued)*

Action	Description
Change the timeout period for users to confirm incident resolutions.	After an incident is resolved, it appears in the affected user's task list for confirmation of its resolution. If the user does not respond within a specified number of days, the incident's status is changed from Resolved to Closed. The default timeout period is two days. You can change the timeout period by editing the SD.IncidentManagementProcess project in Workflow Designer.
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.
Change the CAB approval percentage for Change Management	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. By default, when you use the ITIL change type, 100 percent of the participants must approve a change before it can be implemented. You can change this percentage so that a change can proceed after a single person's approval, a specific user's approval, or a majority approval. You change the approval percentage by editing the SD.ChangeManagement project in Workflow Designer.
Set the database replication schedule.	Your organization might want to create a replication database to duplicate the data in the Process Manager database. The replication database is created during or after the installation of the ServiceDesk application software. See "About replicating the Process Manager database" on page 379. You can set up one or more schedules for synchronizing the data between the Process Manager database and the replication database. See "Scheduling the database replication" on page 379.
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. However, most ServiceDesk implementations either use the default values or make only minor changes. You can make these changes by editing the SD.ProblemManagement project in Workflow Designer.

Table 36-2 Configurations for the ServiceDesk application software *(continued)*

Action	Description
(Optional) Make the ServiceDesk documentation available to your users.	We assume that each organization has specific requirements for providing documentation to their process workers and the users of the ServiceDesk portal. Therefore, the ServiceDesk documentation is not installed with the ServiceDesk application software. We recommend that you download these guides and make them available to your users as needed. See "Making the ServiceDesk documentation available to users" on page 447.
(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.

About the incident priority

Every incident that is submitted to the ServiceDesk is assigned a priority, which determines 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 impact. These values are used to calculate the incident's priority 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 374.

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 373.

Most ServiceDesk implementations either use the default values or make only minor changes. 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 SD.GeneralIncidentSubmitForm project in Workflow Designer.

For more information about customizing forms and editing projects, see the *ServiceDesk Customization Guide* and the *Workflow Solution 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. 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.

Most ServiceDesk implementations either use the default values or make only minor changes.

See "About the incident priority" on page 372.

Table 36-3 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 users can select from the following values: ■ **No Immediate Urgency** ■ **Preventing Some Non-Urgent Work** ■ **Blocking Critical Business** The support technicians can select from the following values: ■ **Core Business Service** ■ **Support Service** ■ **Non-urgent Services**

Table 36-3 Default priority, urgency, and impact values *(continued)*

Setting	Default values
Impact	Defines the extent of the issue by specifying how many people are affected. In the **Who is Affected?** option on the **Create a New Incident** page, the users can select from the following values: ■ **Single User** ■ **Entire Team or Group** ■ **Entire Department** ■ **Unsure** In the **Impact** option, the 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 eliminates 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 372.

Table 36-4 lists the priorities that result from combining the default impact and urgency values. You can customize the values and the way that they combine to arrive at the priority.

Table 36-4 How the incident priority is calculated

Urgency	Impact	Calculated priority
No Immediate Urgency	Single User	Low
No Immediate Urgency	Entire Team or Group	Normal
No Immediate Urgency	Entire Department	High
No Immediate Urgency	Unsure	Low
Preventing Some Non-Urgent Work	Single User	Normal
Preventing Some Non-Urgent Work	Entire Team or Group	High
Preventing Some Non-Urgent Work	Entire Department	High
Preventing Some Non-Urgent Work	Unsure	Normal
Blocking Critical Business	Single User	High
Blocking Critical Business	Entire Team or Group	Urgent
Blocking Critical Business	Entire Department	Urgent
Blocking Critical Business	Unsure	High

About the Service Level Agreement and Operating Level Agreement

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 can be between an external customer and your customer support team or between your organization’s employees and your IT department. The SLA formally defines the agreed-upon services, priorities, and responsibilities that are required to support the customers and users.

An Operating Level Agreement (OLA) defines how departments work together to meet the requirements that are documented in an SLA. The OLA describes the responsibilities of each internal support group toward other support groups, including the process and the time frame for delivering their services. The OLA helps ensure that the activities of the multiple support teams are aligned to provide the contracted service.

See "About the Service Level Agreement (SLA) time frames" on page 376.

Typically, corporate policy defines the overall SLA. A default SLA is built in to the Incident Management process. You can edit the default SLA time frames and you can set up the SLA and OLA in any custom process that you create.

For more information about setting up an SLA and OLA in a process and setting time frames in the SLA, see the *ServiceDesk Customization Guide*.

About the Service Level Agreement (SLA) time frames

A Service Level Agreement (SLA) defines the expectations and requirements for delivering a service, including the allowable time frame for the delivery.

See "About the Service Level Agreement and Operating Level Agreement" on page 375.

The SLA time frames that are associated with ServiceDesk processes are as follows:

Overall time frame	The actual time frame that is defined in the SLA.
Internal time frame	Intermediate time frames for completing the process steps. These time frames are shorter than the overall time, to allow the support team to complete the service well within the overall SLA time frame.

Each of these time frames contains the following time definitions:

Late time	The time that can elapse before a service is considered late.
Warn time	The time that elapses before the worker receives a warning about the remaining time that is allowed.

When a ticket's internal SLA level reaches its warn time, an email is sent to the current assignee, if any. The ticket's status is unchanged.

When the internal SLA level reaches its late time, the status is changed to **OUT OF TIME**. The ticket is assigned to Support I, Support II, and Service Managers no matter who it was assigned to. No email is sent because the ticket is now assigned to multiple groups of users rather than one particular user.

When a ticket's overall SLA level reaches its warn time, an email is sent to the current assignee, if any. When the overall SLA level reaches its late time, it is likely that the ticket has been escalated automatically and the notifications have been sent. Therefore, no new action is taken in ServiceDesk.

A default SLA is built in to the Incident Management process. You can edit the default SLA time frames to comply with your organization's SLA.

See "Default SLA time frames" on page 377.

If your organization does not use Service Level Agreements, you can disable an SLA by setting a large number of days for its time frames.

For more information about setting time frames in the SLA, see the *ServiceDesk Customization Guide*.

Default SLA time frames

A Service Level Agreement (SLA) defines the expectations and requirements for delivering a service, including the allowable time frame for the delivery.

See "About the Service Level Agreement (SLA) time frames" on page 376.

A default SLA is built in to the Incident Management process. You can edit the default SLA time frames to comply with your organization's SLA.

Table 36-5 Default SLA time frames

SLA level	Time frames
Basic	The basic time frames are as follows: ■ The overall late time frame is six days, with a warning at three days. ■ The Support I group has eight hours to respond, with a warning at four hours. ■ The second-level support and escalated levels each have eight hours to respond, with a warning at four hours.
Emergency	The overall late time frame is two hours, with a warning at one hour.

For more information about setting time frames in the SLA, see the *ServiceDesk Customization Guide*.

About business hours and holidays

Business hours are the hours during which your business is commonly conducted. Typical business hours can vary by country. For example, business hours in the United States vary by region due to the different time zones.

You can set your organization's business hours and holidays at one of several levels, based on your business locations and SLA policy.

Table 36-6 Levels for setting business hours and holidays

Level	Description
Global	The global business hours become the default settings for every new workflow and monitoring project that is created in Workflow Designer. The global business hours are set with the Business TimeSpan Editor, which is installed as a Workflow Designer tool. You can define the beginning and ending business hours, holidays, and weekend days. For more information about the Business TimeSpan Editor, see the *Workflow Solution 7.1 SP2 User Guide* at the following URL: http://www.symantec.com/docs/DOC4824
Project	The initial business hour settings at the project level are obtained from the global settings. You can use Workflow Designer to change the business hours for specific projects. You might use project-level business hours if a specific department operates through the weekend while the most other departments operate during the business week. For example, the retail industry might require project-level business hours.
Component, within workflow projects only	On their own, the business hour settings do not affect the way a workflow project is executed. But they can be incorporated at the component level to allow or prevent certain actions from occurring based on established business hours. For example, you might need to consider weekends and holidays when establishing timeout and escalation rules.

For more information about setting business hours, see the *ServiceDesk Customization Guide* and the *Workflow Solution User Guide*.

About Follow the Sun routing

In a Follow the Sun management process, a service organization provides 24x7 support by staffing service desks in multiple locations according to time zone. An incident can be submitted and worked in one location and then passed to or picked up by another location when the originating office closes. The incident is then passed from location to location as each one closes, until the incident is resolved.

Follow the Sun routing lets you service your users in a continuous support model. You can also use a Follow the Sun model with overlapping shifts to offset peak call volume times and random call spikes.

The advanced incident form contains a **Follow the Sun** option. When that option is selected, the incident is routed to the groups that you define.

Follow the Sun routing is defined in Workflow Designer in the SD.FollowTheSun project.

For more information about setting up Follow the Sun routing, see the *ServiceDesk Customization Guide* and the *Workflow Solution User Guide*.

About replicating the Process Manager database

You can create a database that replicates certain data from the Process Manager database. You can either copy or move the original data to the replication database or to a file. For example, you can copy data to the replication database for data mining, which might otherwise affect the performance of the Process Manager database. You can move old and unneeded data to purge it from the Process Manager database.

The default name for the actual database is ProcessManagerReplication. It typically resides on the same SQL Server computer as the Process Manager database.

The **ServiceDesk Setup** wizard creates and configures the replication database if you complete the **Database Replication** page. This page is part of the installation's advanced settings. You can configure the replication database after the initial ServiceDesk installation if you did not do so during the installation.

You might not need to replicate data until after you have used ServiceDesk for some time. If you did not configure the replication database during the initial ServiceDesk installation, you can do so at any time thereafter.

After the replication database is created, you configure one or more replication schedules that specify the data to replicate and when to replicate it.

See "Scheduling the database replication" on page 379.

Scheduling the database replication

The replication database replicates certain data from the Process Manager database.

See "About replicating the Process Manager database" on page 379.

The **ServiceDesk Setup** wizard creates and configures the replication database. After the replication database is created, you configure one or more replication schedules that specify the data to replicate and when to replicate it.

Examples of replication schedules are as follows:

- On the first day of every month, move all data that is older than 120 days.
- Every Saturday at 1:00 A.M., copy all data.
- One time, copy the incident data to a file for use in a presentation.

To schedule the database replication

1. In the ServiceDesk portal, click **Admin > Reports > Replication Schedule List**.
2. In the upper right of the **Replication Schedules** section, click the **Add Replication Schedule** symbol (a white page with a green plus sign).
3. In the **New Replication Schedule** dialog box, name and configure the schedule.

   The type of schedule that you select determines the schedule settings that appear.

   See "New Replication Schedule dialog box" on page 380.
4. When you finish configuring the schedule, in the **New Replication Schedule** dialog box, click **Save**.

New Replication Schedule dialog box

This dialog box lets you configure schedules for replicating the Process Manager database. Each schedule specifies the data to replicate and when to replicate it.

See "Scheduling the database replication" on page 379.

Table 36-7 Options in the **New Replication Schedule** dialog box

Option	Description
Name	Lets you provide a unique, descriptive name for the schedule so that it can be easily recognized in the **Replication Schedules** section.
Active	Makes the schedule active so that the replication occurs at the scheduled times. You can uncheck this check box at any time to disable this schedule temporarily.

Table 36-7 Options in the **New Replication Schedule** dialog box *(continued)*

Option	Description
Select type of schedule	Lets you schedule the replication to occur in one of the following intervals: ■ **Daily (number of days)** ■ **Weekly** ■ **Monthly** ■ **One time only** The type of schedule that you select determines the remaining schedule options that appear in this dialog box. These schedule options are the same for several other types of schedules. See "Options for scheduling reports and events" on page 359.
Advanced	Opens the **Advanced** dialog box, which lets you set the replication to repeat after a specified number of minutes or hours, until a specified time. For example, you can set a replication to run every four hours on the scheduled days. This option is not available for a one-time-only schedule.
Add Table Set	Opens the **Add Table Set** dialog box, which lets you specify the data to replicate, the data destination, and whether to copy or move the data. You can add multiple table sets to a single replication schedule. See "Add Table Set dialog box" on page 381.

Add Table Set dialog box

This dialog box lets you specify the Process Manager data to replicate, the data destination, and whether to copy or move the data. This information is added to a database replication schedule. You can add multiple table sets to a single replication schedule.

This dialog box appears when you click **Add Table Set** in the **New Replication Schedule** dialog box.

See "New Replication Schedule dialog box" on page 380.

Table 36-8 Options in the **Add Table Set** dialog box

Option	Description
Table Set	Lets you select the data tables to replicate. The options are as follows: ■ **Report process tables** ■ **Report snapshots**
Older than	Lets you specify the age in days of the data to replicate.
Destination Type	Lets you specify whether to replicate the data to a file or to the replication database.
Destination	If you replicate the data to a file, you can specify the path in which to save the file. If you do not specify a path, the file is saved to a default location. If you replicate the data to a database, you can select the database. Typically, your only choice is the replication database.
Operation Type	Lets you copy or move the data from the Process Manager database. Any data that you move is not available for reporting or other processing in ServiceDesk.
Add	Adds the current table set to the **New Replication Schedule** dialog box.

About the Service Catalog and service items

The Service Catalog is a Web part that appears on several ServiceDesk 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 all 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.

You can also add customized service items to the Service Catalog. For example, you can add service items for self-service activities such an as automated password reset or an automated software request. 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.

The customization of the Service Catalog requires a full Workflow Solution license. Examples of the custom service items are: automated password reset, automated software request.

Migrating categories from Helpdesk Solution

You can migrate the categories from Helpdesk Solution 6.5 so that you can use them in ServiceDesk. If you did not migrate categories at the end of the ServiceDesk installation, you can perform the migration in the ServiceDesk portal.

Category migration can be run multiple times.

To migrate categories from Helpdesk Solution

1. In the ServiceDesk portal, click **Submit Request**.
2. On the **Submit Request** page, under **Service Catalog**, click **ServiceDesk**.
3. Under **New Requests**, click **Migrate Helpdesk Categories**.
4. In the **Migrate Categories** wizard, on the **Welcome** page, enter the Symantec Management Platform computer credentials for the Helpdesk Solution whose data you want to migrate.
5. Click **Next**.
6. On the **Choose Categories** page, select the categories to migrate, and then click **Migrate**.
7. When the migration finishes, click **Close**.

Chapter 37

Managing security, users, roles, groups, and permissions

This chapter includes the following topics:

- Creating a new user
- Add User dialog box: Clone User tab
- Adding new ServiceDesk users from Active Directory manually
- Editing a user account
- Disabling and enabling a user

About ServiceDesk security and permissions

ServiceDesk manages access to the ServiceDesk portal through native authentication or Active Directory authentication.

See "About ServiceDesk authentication" on page 388.

ServiceDesk provides a high level of security within the ServiceDesk portal through the use of users, groups, organizational units, and permissions. The ServiceDesk permissions control all the views and possible actions in the ServiceDesk 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 37-1 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.

Table 37-1 ServiceDesk permissions hierarchy *(continued)*

Permissions level	Description
Group	A collection of users. For example, the Support I group might contain all the level 1 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 387. See "Default ServiceDesk user groups" on page 473.
Permission	Permissions control the access to and use of the ServiceDesk 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 *ServiceDesk User Guide*.

See "Default ServiceDesk permissions by category" on page 467.

See "Default ServiceDesk user groups" on page 473.

See "Creating a group" on page 391.

About ServiceDesk authentication

The authentication method can be defined in the **Process Manager Active Directory Settings** section in the ServiceDesk Portal on the **Master Settings** page. Your organization can use native authentication or Active Directory (AD) authentication.

See "Master Settings: Process Manager Active Directory Settings section" on page 463.

Table 37-2 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.
Active Directory authentication	With Active Directory authentication, a mixed mode authentication is used. AD 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 AD users and groups are imported to ServiceDesk during synchronizations. The imported users and groups are stored in the Process Manager database. However, AD passwords and other sensitive information are not stored in the Process Manager database. See "About Active Directory synchronization" on page 404. 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 407. 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 AD 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 418.

About adding users from Active Directory

When your organization uses Active Directory (AD) authentication, the AD 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 388.

Table 37-3 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 404.
Manually	If a new user needs to access ServiceDesk between synchronization, you can add the user manually from Active Directory. See "Adding new ServiceDesk users from Active Directory manually" on page 399.
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 who are in Active Directory but have not been added to ServiceDesk are added to ServiceDesk when they log on to the ServiceDesk 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 "About adding groups from Active Directory" on page 389.

About adding groups from Active Directory

When your organization uses Active Directory (AD) authentication, the AD users and groups are imported to ServiceDesk during sync profile synchronizations. When AD 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 388.

Table 37-4 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 426.
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 404.

During the creation of your Active Directory sync profiles, your Active Directory groups can be mapped to the default ServiceDesk groups. This option lets the AD groups take the permissions of the default ServiceDesk groups. By mapping the groups, you can benefit from the predefined permissions in the default ServiceDesk groups while using your organization’s preferred group names.

See “Managing Active Directory sync profiles” on page 418.

When Active Directory groups are added or updated in ServiceDesk, the ServiceDesk permissions are assigned as follows:

- The Active Directory groups that are mapped to Process Manager groups take the permissions of the groups that they are mapped to.
  For example, your Active Directory contains a group named Technician and you map it to the default group Support 1. The Technician group is imported to ServiceDesk with the permissions of the Support 1 group. A group named Support 1 is not created.
- Any Active Directory groups that are not mapped to Process Manager groups are added without permissions.
  You must assign permissions to those groups after the installation.
  See “Copying permissions between groups” on page 394.

See “About adding users from Active Directory” on page 389.

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 387.

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 389.

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 394.

See "Copying permissions between groups" on page 394.

To create a group

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, at the upper right of the **All Groups** section, click the **Add Groups** symbol (green plus sign).
3. In the **Add Group** dialog box, name the new group, copy permissions from another group if desired, and specify the group's home page and email address.

   See "Add Group dialog box" on page 391.
4. Click **Save**.

Add Group dialog box

This dialog box lets you add a user group to the ServiceDesk portal.

See "Creating a group" on page 391.

Table 37-5 Options in the **Add Group** dialog box

Option	Description
Group Name	Lets you enter the name of the new group. You can use special characters but you cannot enter a name that is already assigned to another group.
Copy Permissions From Group	Lets you use another group's permissions for this group. You can type the name of the other group or click **Pick** to select a group from the **Group Picker** dialog box. All the permissions from the group that you specify are replicated for 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 394.
Homepage	Lets you specify the name of the portal page that should appear when users in this group log on to the ServiceDesk portal.
Email Address	Lets you type an email address to be used for group-level communications.

Editing a group

An administrator or other user who has the appropriate permissions can edit ServiceDesk groups.

See "About group-level permissions" on page 387.

See "Creating a group" on page 391.

To edit a group

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, under **All Groups**, select the group.
3. In the right pane, at the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Edit**.
4. In the **Edit Group** dialog box, edit the group as necessary.
5. Click **Save**.

Deleting a group

An administrator or other user who has the appropriate permissions can delete ServiceDesk groups.

Deleting a group does not delete the users who belong to that group.

See "About group-level permissions" on page 387.

See "Creating a group" on page 391.

To delete a group

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, under **All Groups**, select the group.
3. In the right pane, at the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Delete**.
4. Click **OK** to confirm the deletion.

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 387.

See "Creating a group" on page 391.

To add users to a group

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, under **All Groups**, select the group.
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.
     See "Picking a user" on page 96.
   - (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 Repeat step 4 as necessary to add all the users.

6 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 387.

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 ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.

2 On the groups page, under **All Groups**, select the group.

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** or **Unselect All** to add all available permissions to a group, or remove all permissions from a group, respectively.

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 ServiceDesk portal. You can also have the permissions assigned automatically when you import Active Directory groups and map them to the ServiceDesk groups.

See "About adding groups from Active Directory" on page 389.

The ability to copy permissions between existing groups is useful when you import an Active Directory group that is not mapped to a ServiceDesk group. In that case, the imported group is created without any permissions and you must assign the permissions yourself. Copying the permissions from another group eliminates the need to assign the permissions manually.

See "About group-level permissions" on page 387.

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 ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, under **All Groups**, find the group to set permissions for.
3. At the right of the group's title bar, click the **Actions** symbol (orange lightning), and then click **Add Permissions From**.
4. On the **Copy Permissions From Groups** dialog box, in **Group Name**, 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**.

Viewing the list of ServiceDesk permissions

In the ServiceDesk portal, an administrator or other user who has the appropriate permissions can view all the ServiceDesk permissions and their descriptions by category.

See "About group-level permissions" on page 387.

See "Default ServiceDesk permissions by category" on page 467.

To view the list of permissions

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Permissions**.
2. On the permissions page, under **Browse Permissions**, select the category of permissions to view.
3. In the right pane, you can view the permissions that are assigned to the selected category, and you can perform several permission-related actions.
4. When you finish viewing the permissions, you can go to another page.

Viewing the permissions for a group

An administrator or other user who has the appropriate permissions can view the permissions that are associated with a specific ServiceDesk group.

A group's permissions determine the permissions that are granted to the users who are members of that group. You can view a group's permissions to discover what the users in that group can do.

See "About group-level permissions" on page 387.

See "Default ServiceDesk user groups" on page 473.

To view the permissions for a group

1. In the ServiceDesk portal, click **Admin > Users > Accounts > List Groups**.
2. On the groups page, under **All Groups**, select the group.
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. When you finish viewing the permissions in the **Permissions For Group** dialog box, click **Cancel**.

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 ServiceDesk portal, click **Admin > Users > Accounts > List Organizations**.
2. On the organizations page, at the upper right of the **Browse Organizations** section, click the **Add Root Organization** symbol (a white page with a green plus sign).
3. In the **Add Organization** dialog box, in **Organization Name**, type a descriptive name for the organization.

   You can use special characters in the name. Duplicate names are not allowed.
4. (Optional) In **Description**, 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 389.

Every ServiceDesk user requires permissions to perform any actions in the ServiceDesk 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 387.

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 393.

To create a new user

1. In the ServiceDesk portal, click **Admin > Users**.
2. On the users page, at the right of the **All Users** title bar, click the **Add New 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. See “Add User dialog box: Clone User tab” on page 398.
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**.

Add User dialog box: Clone User tab

This tab lets you clone information from an existing user to a new user, which can speed the creation of the new user. It is especially useful when you need to add several users of the same type.

See “Creating a new user” on page 397.

Table 37-6 Options on the **Clone User** tab

Option	Description
User	Lets you specify the user to clone. You can type the user’s name or click **Pick** to search for a user. See “Picking a user” on page 96.
Clone User’s Groups	Clones the group settings of this user for the new user.
Clone User’s Permissions	Clones the permissions settings of this user for the new user.
Clone User’s Organization Units	Clones the organization unit settings of this user for the new user.

Adding new ServiceDesk users from Active Directory manually

You can manually add new users to ServiceDesk from Active Directory. Normally, ServiceDesk synchronizes its data with Active Directory on a regular schedule. However, you may want to add new users before the next scheduled update.

The ability to add users from Active Directory is available only if your organization chose the option to use Active Directory authentication.

See "About ServiceDesk authentication" on page 388.

The list of users that appears under **Add Active Directory Users** is current as of the last synchronization with Active Directory.

Every ServiceDesk user requires permissions to perform any actions in the ServiceDesk 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 "Adding users to a group" on page 393.

To add new ServiceDesk users from Active Directory manually

1. In the ServiceDesk portal, click **Admin > Users > AD Users**.
2. Under **Add Active Directory Users**, in **Active Directory Server**, select a server.
3. Search for the users to add in one of the following ways:
   - To display all the users in the selected Active Directory, click **Search Users**.
   - To search for specific users or groups, type the search criteria in **Name** or **Department**, and then click **Search Users**.
4. Under **Select Users**, select the check boxes for the users to add, and then click **Add Users** at the bottom of the page.

   If the list of users consists of multiple pages, you must select the users and click **Add Users** one page at a time. For example, if you select users on page 2 of the display, click **Add Users** before you go to page 3 and add users there.
5. When you finish adding users, you can go to another page in the Software Portal.

Editing a user account

An administrator or other user who has the appropriate permissions can edit the data for ServiceDesk users. Any of the user information that can be set during the user creation is available for editing.

See "Creating a new user" on page 397.

To edit a user account

1. In the ServiceDesk portal, click **Admin > Users**.
2. On the users page, under **All Users**, scroll to the user to edit.
3. At the far right of the user name, click the **Actions** symbol (orange lightning), and then click **Manage User**.
4. On the **Manage User** page, edit the account information that appears on any of the following tabs:

Account Info	Lets you edit the information that identifies the user.
Password Settings	Lets you clone groups, permissions, or organizations for this user from an existing user. See "Add User dialog box: Clone User tab" on page 398.
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. When you finish editing the account information, on the **Manage User** page, click **Save**.

Disabling and enabling a user

An administrator or other user who has the appropriate permissions can disable a user so that the user cannot use ServiceDesk. Disabled users can be enabled so that they can access ServiceDesk again.

If you disable a user who is currently logged onto the ServiceDesk portal, the user is not locked out of the session. However, a disabled user cannot save any data or navigate to any other pages. Disabled users continue to be listed under the **All Users** section, but are not indicated as being active.

Before you disable a user who has process ticket assignments, reassign those tickets.

See "Reassigning incidents, problems, or change tickets" on page 235.

To disable or enable a user

1. In the ServiceDesk portal, click **Admin > Users > Accounts > Manage Users**.
2. On the users page, under **All Users**, scroll to the user that you want to edit.
3. At the far right of the user name, click the **Actions** symbol (orange lightning), and then click **Enable/Disable**.
4. In the **Enable/Disable User** dialog box, click **Disable This User** or **Enable This User**, whichever is appropriate.
5. Click **OK** in the confirmation dialog box that appears.

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 an 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

If your organization chooses to use Active Directory authentication as its authentication method for ServiceDesk, ServiceDesk can synchronize with Active Directory. This synchronization lets you add and update Active Directory users and organizational units and groups in the Process Manager database. During synchronization, the user, units, and groups data from Active Directory update the user, units, and group data that are in the Process Manager database. The Process Manager database does not store Active Directory passwords or other sensitive Active Directory information.

After you connect ServiceDesk to an Active Directory server, you can add Active Directory sync profiles. These sync profiles let you import the entire Active Directory domain or specific organizational units and groups to the Process Manager database. 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 388.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

See "About adding users from Active Directory" on page 389.

See "About adding groups from Active Directory" on page 389.

See "Creating a new user" on page 397.

See "Creating an organizational unit" on page 396.

See "Configuring Active Directory sync profiles" on page 405.

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 404.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

See "Managing Active Directory server connections" on page 407.

See "Managing Active Directory sync profile schedules" on page 413.

See "Managing Active Directory sync profiles" on page 418.

Table 38-1 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 408.
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 412. 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	(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 411.
Step 4	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 414. When adding your Active Directory sync profiles, you can use these schedules to schedule the following synchronizations: ■ Update synchronization ■ Full synchronization

Table 38-1 Process for configuring an Active Directory sync profile *(continued)*

Step	Action	Description
Step 5	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 421.
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 427.
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 429.
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 430.

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 413.

See "Managing Active Directory sync profiles" on page 418.

Table 38-2 Process for managing Active Directory server connections

Step	Action	Description
Step 1	Add Active Directory server connections.	In Workflow Explorer, you can add Active Directory server connections. See "Adding Active Directory server connections" on page 408.
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 409.
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 410.
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 411.

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 405.

See "Managing Active Directory server connections" on page 407.

Before you add an Active Directory server connection, you need to collect the following information:

- NETBIOS domain name of the Active Directory server computer
- Credentials for Active Directory
  The user name and password of an account that can connect to the Active Directory and retrieve user information

To add Active Directory server connections

1. On the computer where Workflow Designer is installed, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the **Symantec Workflow Explorer** screen in the toolbar at the top of the screen, 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 under **General**, type the name of the profile.

   See "New AD Connections Profile and Edit AD connection settings dialog boxes" on page 412.
6. If this profile is the default profile, check **Is Default**.
7. Under **Remote Security**, type the NETBIOS name of the domain that you want to authenticate.
8. Type the user name and password.
9. Click **OK**.
10. Repeat steps 4 thru 9 for each additional server connection.
11. Close Workflow Explorer.
12. (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 412.

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 ServiceDesk Portal on the **Master Settings** page.

See “Managing Active Directory server connections” on page 407.

See “Master Settings: Process Manager Active Directory Settings section” on page 463.

To edit the settings of an Active Directory server connection

1. On the computer where Workflow Designer is installed, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the Symantec Workflow Explorer screen in the toolbar at the top of the screen, click **Credentials**.
3. In the left pane, click **Active Directory**.
4. 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 settings as needed.

   See “Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes” on page 425.
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 411.

Deleting an Active Directory server connection

After you add your Active Directory server connections, you may need to delete an Active Directory server connection. In Workflow Explorer, you can 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 that server connection.

Note: When you delete an Active Directory server connection in Workflow Explorer, the sync profiles that you added for that connection are not deleted in ServiceDesk. Therefore, when the sync profiles automatically attempt to synchronize, an error occurs. You must either delete these Active Directory sync profiles or switch them to another Active Directory server connection.

See "Managing Active Directory server connections" on page 407.

See "Managing Active Directory sync profiles" on page 418.

To Delete an Active Directory server connection

1. On the computer where Workflow Designer is installed, click **Start > All Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.
2. On the Symantec Workflow Explorer screen in the toolbar at the top of the screen, click **Credentials**.
3. In the left pane, click **Active Directory**.
4. 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**.

Testing an Active Directory server connection

After you add your Active Directory server connections, you can test any of your 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 405.

See "Managing Active Directory server connections" on page 407.

See "Managing Active Directory sync profiles" on page 418.

To test an Active Directory server connection

1. In the ServiceDesk 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 sync profile name, click the **Actions** symbol (orange lightning), and then 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.

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 ServiceDesk 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 405.

See "Adding Active Directory server connections" on page 408.

To select Active Directory as the authentication method

1. In the ServiceDesk 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.

   See "Master Settings: Process Manager Active Directory Settings section" on page 463.
5. Scroll down to the bottom of the **Master Settings** page and click **Save**.

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 408.

See "Editing the settings of an Active Directory server connection" on page 409.

Table 38-3 Options on the **New AD Connection Profile** and **Edit AD connection settings** dialog boxes

Option	Description
Default Timeout	Lets you specify the parameters for the 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.
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.

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 418.

Table 38-4 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 414. 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 416.
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 417.

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 an 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 405.

See "Managing Active Directory sync profiles" on page 418.

See "Managing Active Directory sync profile schedules" on page 413.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

To add Active Directory sync profile schedules

1. In the ServiceDesk portal, click **Admin > Active Directory > Sync Profile Schedule**.
2. On the **Active Directory Sync Profile Schedule** page, at the far right of the Active Directory Sync Profile Schedule 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.
Start time	Lets you select what time you want the synchronization to start.

4. When you are finished, click **Save**.
5. Repeat steps 2 thru 4 to add more Active Directory sync profile schedules.

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 413.

See “Managing Active Directory sync profiles” on page 418.

To edit an Active Directory sync profile schedule

1. In the ServiceDesk portal, click **Admin > Active Directory > Sync Profile Schedule**.
2. On the **Active Directory Sync Profile Schedule** page, at the far right of the sync profile schedule name, click the **Actions** symbol (orange lightning), and then 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.
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. In ServiceDesk, you can delete an Active Directory sync profile schedule. For example, you may need to delete an obsolete schedule.

Note: You cannot delete a sync profile schedule that is currently used in one of your Active Directory sync profiles. Before you can delete that sync profile schedule you must edit that sync profile and select a different update or full synchronization schedule. You can delete a sync profile schedule only after it is no longer used by any of your sync profiles.

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.

See “Managing Active Directory sync profile schedules” on page 413.

See “Managing Active Directory sync profiles” on page 418.

To delete an Active Directory sync profile schedule

1. In the ServiceDesk portal, click **Admin > Active Directory > Sync Profile Schedule**.
2. On the **Active Directory Sync Profile Schedule** page, at the far right of the sync profile schedule name, click the **Actions** symbol (orange lightning), and then click **Delete Schedule**.
3. In the confirmation message dialog box, click **OK**.

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 ServiceDesk 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 407.

See “Managing Active Directory sync profile schedules” on page 413.

See “Methods for synchronizing Active Directory sync profiles” on page 426.

Table 38-5 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 414. 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 connections. See "Adding Active Directory sync profiles" on page 421.
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 416.
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 417.
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 422.
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 424.

Table 38-5 Process for managing Active Directory sync profiles *(continued)*

Step	Action	Description
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 427.
Step 8	(Optional) Manually perform an 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 an update Active Directory sync profile synchronization manually" on page 428.
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 429.
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 430.
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 411.

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 ServiceDesk portal.

See "Configuring Active Directory sync profiles" on page 405.

See "Managing Active Directory sync profiles" on page 418.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

To add Active Directory sync profiles

1. In the ServiceDesk 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 then click **Add AD Sync Profile**.
3. In the **Add Active Directory Sync Profile** dialog box, enter the settings for the new Active Directory server.

   See "Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes" on page 425.
4. In the **Add Active Directory Sync Profile** dialog box, click **Next**.

   Note that if you do not enter critical information or a connection cannot be made, you cannot proceed until you have entered the correct information.

5 In the **Add Active Directory Sync Profile** dialog box 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 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.

7 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. 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 414.

8 In the **Add Schedule for Active Directory Server** dialog box, click **Finish**.

Editing an Active Directory sync profile

After you add your sync profiles, you can edit the sync profiles settings for any sync profile that you added. In ServiceDesk, you can edit your Active Directory sync profiles. You can edit the sync profile settings for an entire domain, organizational units and groups on the Active Directory server, or specific LDAP queries. For example, you may need to remap an Active Directory field to a Process Manager field. You can edit the settings for that sync profile and remap the field.

See "Managing Active Directory sync profiles" on page 418.

To edit an Active Directory sync profile

1. In the ServiceDesk portal, click **Admin > Active Directory > Sync Profiles**.
2. On the **Active Directory Sync Profiles** page, at the far right of the sync profile name, click the **Actions** symbol (orange lightning), and then click **Edit AD Sync Profile**.
3. In the **Edit Active Directory Sync Profiles** dialog box, edit the settings as needed.

   See "Add Active Directory Sync Profiles and Edit Active Directory Sync Profiles dialog boxes" on page 425.
4. Click **Next**.

   Note that if you do not enter critical information, or a connection cannot be made, you cannot proceed until you have entered the correct information.
5. In the **Edit Active Directory Sync Profile** dialog box under **Synchronization Option**, select one of 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 In the **Edit Active Directory Field Mapping** dialog box, 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.

7 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 8. 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 416.

8 In the **Edit Schedule for Active Directory Server** dialog box, select different schedules in the drop-down lists for **Schedule For Full Sync Profile** and **Schedule For Update Sync Profile** as needed.

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. 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 414.

9 In the **Edit Schedule For Active Directory Server** dialog box, 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. In ServiceDesk, you can delete that Active Directory sync profile.

See "Managing Active Directory sync profiles" on page 418.

To delete an Active Directory sync profile from ServiceDesk

1. In the ServiceDesk 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 sync profile name, click the **Actions** symbol (orange lightning), and then click **Delete AD Sync Profile**.
3. In the confirmation message dialog box, click **OK**.

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 421.

See "Editing an Active Directory sync profile" on page 422.

Table 38-6 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.
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 38-6 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 404.

See "Configuring Active Directory sync profiles" on page 405.

See "Managing Active Directory sync profiles" on page 418.

See "Checking the status of an Active Directory sync profile synchronization" on page 430.

Table 38-7 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 414. 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 421.
Manually run a full synchronization.	In ServiceDesk, you can manually run a full Active Directory sync profile synchronization at any time. After you configure your Active Directory sync profiles, 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 427.
Manually run an update synchronization.	In ServiceDesk, you can manually run an 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 an update Active Directory sync profile synchronization manually" on page 428.
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 429.

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 404.

See "Configuring Active Directory sync profiles" on page 405.

See "Managing Active Directory sync profiles" on page 418.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

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 430.

To run a full Active Directory sync profile synchronization manually

1. In the ServiceDesk 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 sync profile name, click the **Actions** symbol (orange lightning), and then click **Run Reset Sync Profile**.
3. When the dialog box that announces the start of the synchronization appears, you can close it.

Running an update Active Directory sync profile synchronization manually

In ServiceDesk, you can manually run an 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 404.

See "Managing Active Directory sync profiles" on page 418.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

See "Checking the status of an Active Directory sync profile synchronization" on page 430.

To run an update Active Directory sync profile synchronization manually

1 In the ServiceDesk 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 sync profile name, click the **Actions** symbol (orange lightning), and then 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 404.

See "Configuring Active Directory sync profiles" on page 405.

See "Managing Active Directory sync profiles" on page 418.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

To synchronize all Active Directory sync profiles

1 In the ServiceDesk 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 then 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 ServiceDesk portal from the **Active Directory Sync Profiles** page.

See "Configuring Active Directory sync profiles" on page 405.

See "Managing Active Directory sync profiles" on page 418.

See "Methods for synchronizing Active Directory sync profiles" on page 426.

To check the status of an Active Directory sync profile synchronization

1. In the ServiceDesk 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 server profile name, click the **Actions** symbol (orange lightning), and then click **Check Sync Status**.
3. If you check the status during the synchronization, in the **Sync Process Status** dialog box, you can update the display by clicking **Refresh**.
4. When you finish viewing the status information, you can close the **Sync Process Status** dialog box.

Chapter 39

Managing categories and the data hierarchy

This chapter includes the following topics:

About incident categories and the data hierarchy

ServiceDesk uses categories to classify incidents. The support technicians assign a category to incidents in the advanced incident form. The incident category helps route the tickets to the appropriate incident technician or queue. The category also helps sort incidents for reports.

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. You can define up to 10 levels of categories in the hierarchy.

When you set up the data hierarchy, try to achieve a complete categorization system without making it too complex. Provide enough nested levels for the support workers to accurately classify the incidents. However, too many categories and classifications make it difficult to select the correct one. When incidents are categorized incorrectly, some steps in the process might be skipped or the incidents might be reported incorrectly.

You can use any of the following categories:

Default categories	ServiceDesk contains predefined incident categories, which you can use immediately or edit to meet your organization's requirements. You can view the default categories in the ServiceDesk portal from **Admin > Data > Hierarchy Data Service**.
New categories	You can create new categories in addition to or in place of the default categories. See "Adding a new incident category to the hierarchy tree" on page 432.
Imported categories	Categories are imported to ServiceDesk when you migrate incidents or categories from a previous version of Helpdesk Solution. Any incidents that you migrate retain their original categorization. The imported categories are available for any new incidents that are created. The imported categories do not correspond to the default categories in ServiceDesk. After you migrate the incidents or categories, some cleanup might be required.

Adding a new incident category to the hierarchy tree

Categories are used to classify ServiceDesk incidents. The support technicians assign a category to incidents in the advanced incident form.

See "About incident categories and the data hierarchy" on page 431.

You can create new categories in addition to or in place of the default categories.

To add a new incident category to the hierarchy tree

1. In the ServiceDesk portal, click **Admin > Data > Hierarchy Data Service**.
2. Under **Hierarchy Tree**, click the **Add New Category** symbol (page with green plus sign).
3. In the **Add Category** dialog box, in **Hierarchy Category Name**, type a name for the category.
4. (Optional) In **Description**, type a description for the category.

   The description appears in the **Hierarchy Data Service** area only.

5 In the **Add Category** dialog box, click the Permissions tab and add or edit permissions as needed.

See "Setting permissions" on page 95.

6 In the **Add Category** dialog box, click **Save**.

Deleting an incident category from the hierarchy tree

Categories are used to classify ServiceDesk incidents. You can delete the categories 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.

See "About incident categories and the data hierarchy" on page 431.

If the category that you delete contains any subcategories, they are also deleted. Any incidents that belong to a deleted category remain unchanged.

Warning: Best practices recommend that you do not delete a category after you start using ServiceDesk. Any incidents that are still assigned to a deleted category do not appear in the reports and searches that are run on new categories.

To delete an incident category from the hierarchy tree

1 In the **ServiceDesk** portal, click **Admin > Data > Hierarchy Data Service**.

2 Under **Hierarchy Tree**, select the category to delete.

3 In the **Hierarchy** section, click the **Actions** symbol (orange lightning), and then click **Delete Category**.

4 In the confirmation message, click **OK**

Adding hierarchy items to an incident category

Categories are used to classify ServiceDesk incidents. The support technicians assign a category to incidents in the advanced incident form.

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 categories and the data hierarchy" on page 431.

This procedure adds hierarchy items but it does not include the details.

To add hierarchy items to an incident category

1. In the **ServiceDesk** portal, click **Admin > Data > Hierarchy Data Service**.
2. Under **Hierarchy Tree**, select the parent of the category to add an item to.
3. At the far right of the **Hierarchy** title bar, click the **Actions** symbol (orange lightning), and then click **Add Hierarchy Items**.

   You can also click the **Add Hierarchy Items** option that appears at the lower right of the **Hierarchy** section.
4. In the **Add Hierarchy Items** dialog box, in **Add New Hierarchy Item**, type one or more hierarchy items.

   To add multiple items, press **Enter** after each item so that it appears on its own line.
5. When you finish typing hierarchy items, click **Add Items**.

Deleting hierarchy items from an incident category

Categories and their associated hierarchy items are used to classify ServiceDesk incidents. You can delete the hierarchy items that are no longer useful.

See "About incident categories and the data hierarchy" on page 431.

Any incidents that belong to a deleted category remain unchanged.

Warning: Best practices recommend that you do not delete a category item after you start using ServiceDesk. Any incidents that are still assigned to a deleted category item do not appear in the reports and searches that are run on new categories.

To delete a hierarchy item from a category

1. In the **ServiceDesk** portal, click **Admin > Data > Hierarchy Data Service**.
2. Under **Hierarchy Tree**, select the category to delete an item from.
3. Under **Hierarchy**, click the **Delete** symbol (red X) that appears at the far right of the item to delete.
4. In the confirmation message, click **OK**.

Chapter 40

Customizing forms

This chapter includes the following topics:

About customizing forms

In the ServiceDesk 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 438.

The form customization can be performed at different levels and from different places.

Table 40-1 Levels of form customization

<table>
<tr><th>Level</th><th>Where to edit</th><th>What you can customize</th></tr>
<tr><td>The form itself</td><td>Workflow Designer

For more information about customizing forms, see the ServiceDesk Customization Guide and the Workflow Solution User Guide.</td><td>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.
</td></tr>
</table>

Table 40-1 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	ServiceDesk portal, on the **Edit Form** page. See "Editing a form in the ServiceDesk portal" on page 437.	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 ServiceDesk 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 438. ■ **Profiles** Lets you assign a default form profile to the form.

Editing a form in the ServiceDesk portal

In the ServiceDesk 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 435.

To edit a form in the ServiceDesk portal

1. In the ServiceDesk 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 435.

To set permissions for a form

1. In the ServiceDesk 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.

   See "Setting permissions" on page 95.
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.

You can customize the forms that control the Customer Satisfaction Survey.

Examples of how you might change the Customer Satisfaction Survey form are as follows:

- Change the frequency with which the survey is sent.
  By default, the Customer Satisfaction Survey is sent for every incident that is resolved and confirmed, except when the incident's close code is Quick Close. However, you can customize the frequency so that the survey is sent for only a certain percentage of the resolved incidents. You also can set the frequency based on the type or priority of the incident.
  You can change the frequency of the Customer Satisfaction Survey by editing the SD.IncidentManagementProcess project in Workflow Designer.
- 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.CustomerServiceSurvey project in Workflow Designer.

For more information about customizing forms and editing the Customer Satisfaction Survey, see the *Workflow Solution User Guide* and the *ServiceDesk Customization Guide*.

See "About customizing forms" on page 435.

Chapter 41

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 a process, based on one or more events that occur within the process.
- 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 Table 41-1 are optional and can be performed in any order.

Table 41-1 Process for customizing the email actions for ServiceDesk processes

Action	Description
Customize the automatic email notifications.	Each process 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 320. For more information about editing the process projects, see the *Workflow Solution 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 442.
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. See "About the creation of incidents from emails" on page 141. 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 443.

About the contents of email notifications

ServiceDesk can send email notifications at various stages of the core processes, based on one or more events that occur within the process.

See "About automatic email notifications" on page 320.

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 41-2 Sources for the contents of the email messages

Source	Description
Templates in the SD.EmailServices project	Most email content is obtained from templates. An email template is a message containing predefined content, format, and structure that is used to create individual emails from a ServiceDesk process. The SD.EmailServices project contains default templates for the core ServiceDesk processes. When an email is triggered within a process, the process selects a template that corresponds to the process ID. For example, if the process ID is IM-000001, then an Incident Management template is selected. You can customize the email templates by adding, editing, or deleting them in the SD.EmailServices project in Workflow Designer. You can customize the email header and footer in the SD.DataServices, in the GetEmailHeaderandFooter model.
In the Send Email component within a process	Certain processes can execute the Send Email component to generate the email messages within the process itself, instead of calling for a template in SD.EmailServices. You can customize the default email messages by editing the Send Email component for the specific process in Workflow Designer.

For more information about configuring the content for email or editing processes and projects, see the *ServiceDesk Customization Guide* and the *Workflow Solution User Guide*.

These automatic email notifications are different from the process notifications that result from the events that occur on specific items within the ServiceDesk portal. For example, the process notifications can be sent when a document or a knowledge base entry is added, edited, or deleted.

See "About process notifications" on page 321.

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.

See "About the creation of incidents from emails" on page 141.

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 455.

The default monitoring process is ready to use. However, you can customize it in several ways to meet your organization's requirements.

Table 41-3 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.
Change the assignee for the incidents that are created automatically.	Edit the SD.Email.InboundManagement 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 *ServiceDesk Customization Guide*. and the *Workflow Solution User Guide*.

Chapter 42

Distributing the ServiceDesk documentation

This chapter includes the following topics:

Making the ServiceDesk documentation available to users

We assume that each organization has specific requirements for providing documentation to their process workers and the users of the ServiceDesk portal. Therefore, the ServiceDesk documentation is not installed with the ServiceDesk application software. 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 42-1 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: ■ *ServiceDesk Implementation Guide* This guide is for the administrator who installs and configures ServiceDesk. ■ *ServiceDesk User Guide* This guide is for the process workers. ■ *ServiceDesk Portal User Guide* This guide is for the internal users and external users who use ServiceDesk to submit incidents and use the knowledge base. You can decide whether to provide this documentation. The ServiceDesk release notes and other documentation resources contain the links to the location for downloading the documentation files.
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 ServiceDesk 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 Web site. See "Configuring the Help link for ServiceDesk documentation" on page 449. ■ 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 452. ■ 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 451. ■ Add the **Links** Web part that provides links to the documents See "Linking to the ServiceDesk documentation from a Links Web part" on page 450. 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.

Table 42-1 Process for making the ServiceDesk documentation available to users *(continued)*

Step	Action	Description
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 ServiceDesk 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 ServiceDesk 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 Web site.

Other options are available for providing access to the documentation from within the ServiceDesk portal.

See "Making the ServiceDesk documentation available to users" on page 447.

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 Server software updates.

To change the destination of the Help link

1. In the ServiceDesk 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 ServiceDesk portal to display links to the location of the documentation files.

You can set permissions on the portal page that you add the Web part to. 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 ServiceDesk portal.

See "Making the ServiceDesk documentation available to users" on page 447.

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 42-2 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. See "Adding a Web part to a ServiceDesk portal page" on page 81.

Table 42-2 Process for linking to the ServiceDesk documentation from a **Links** Web part *(continued)*

Step	Action	Description
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. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.
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 ServiceDesk 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 that you add the Web part to. 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 ServiceDesk portal.

See "Making the ServiceDesk documentation available to users" on page 447.

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 42-3 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. See "Adding a Web part to a ServiceDesk portal page" on page 81.
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. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.
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 ServiceDesk portal.

See "Making the ServiceDesk documentation available to users" on page 447.

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 42-4 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. See "Adding a document category" on page 290. 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. See "Setting permissions for a document category" on page 293. 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. See "Adding a document to the Document Management system" on page 297.
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. See "Setting permissions for a document" on page 302.

Table 42-4 Process for adding the ServiceDesk documentation to Document Management *(continued)*

Step	Action	Description
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. See "Adding a Web part to a ServiceDesk portal page" on page 81.
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. See "Editing or deleting a Web part on a ServiceDesk portal page" on page 82.

Chapter 43

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 ServiceDesk portal.

See "Admin page" on page 55.

Table 43-1 Commands on the **Admin** menu

Command	Subcommand	Description
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	**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 460.
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. See "About Document Management" on page 288.
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. See "About Document Management" on page 288.

Table 43-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
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 categories and the data hierarchy" on page 431.
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 and add actions to process types. Sending an email is a common example of an action that you may want to include in multiple processes. When you create process type actions, ServiceDesk sees x process type running, and adds y action as an option whenever x process is running. Creating process type actions adds an action in multiple places, without having to add the action to each individual workflow.

Table 43-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Portal	**Master Settings**	Lets you configure the master settings for the ServiceDesk portal, which determine the behavior of the ServiceDesk application software and portal. See "About the ServiceDesk portal master settings" on page 462.
Portal	**Manage Pages**	Lets you manage all the pages in the ServiceDesk 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 ServiceDesk 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 ServiceDesk portal" on page 50.
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 ServiceDesk 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 43-1 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 418.
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.
Manage KB Synonyms	Not applicable	Lets you add, edit, and delete knowledge base synonyms
Process Automation	**Automation Rules**	Lets you configure automation rules for any workflow-based application, which includes service automation library.

Table 43-1 Commands on the **Admin** menu *(continued)*

Command	Subcommand	Description
Reports	**Replication Schedule List**	Used with the Process Manager database replication. Lets you configure the replication schedules that specify the Process Manager data to replicate and when to replicate it. See "Scheduling the database replication" on page 379.
Reports	**Report Schedule List**	Lets you configure the schedules that automatically execute and email reports. See "Creating a report schedule" on page 358.

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 II" in a component, you can use the application property for that group instead, as follows:

[ProfileProperties]service_desk_settings_group_support_ii

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 455.

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 following places:

During the ServiceDesk installation	On the **Incident Management Configuration** page that appears during the configuration segment of the **ServiceDesk Setup** wizard
From the ServiceDesk portal	In the **Application Properties** settings that are available from the **Admin** menu See "Adding and deleting incident close codes" on page 461.

Lets you select a code that indicates the nature of the resolution.

The default close codes are as follows:

- **Completed Success**
- **Training Required**
- **Review Documentation**
- **No Fault Found**
- **Monitoring Required**
- **Advice Given**
- **Change Required**
- **Quick Close**
  Sets the incident's status to Closed and sets the Percent Completed to 100%. A customer survey is not sent when this close code is used.
- **Other**

See "Adding and deleting incident close codes" on page 461.

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 460.

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 **ServiceDesk** portal, click **Admin**, and then click **Data > Application Properties**.

2 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 the **Category: Incident Management** section, 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 ServiceDesk portal master settings

The ServiceDesk portal master settings determine the behavior of the ServiceDesk application software and portal.

The ServiceDesk 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 ServiceDesk portal master settings” on page 463.

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 ServiceDesk portal master settings

The ServiceDesk 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 ServiceDesk portal master settings" on page 462.

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 ServiceDesk portal master settings

1. In the **ServiceDesk** portal, click **Admin**, and then click **Portal > Master Settings**.
2. On the **Master Settings** page, expand the section that contains the settings 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**.

Master Settings: Process Manager Active Directory Settings section

This section lets you edit the method for authenticating the users who log on to the ServiceDesk portal. If you use Active Directory authentication, you can also configure the interval for running the AD synchronization and performing other AD-related functions.

See "About ServiceDesk authentication" on page 388.

This section appears on the **Master Settings** page.

See "About the ServiceDesk portal master settings" on page 462.

Table 43-2 Options in the **Process Manager Active Directory Settings** section

Option	Description
Active Directory Authentication	Lets you specify whether to use Active Directory for creating and authenticating the users who log on to the ServiceDesk portal. This option changes the authentication method that was selected during the ServiceDesk installation. For example, if native authentication was selected during the installation, you can enable the Active Directory authentication by selecting this option.
Convert Native Users to Active Directory User	Lets you specify whether to convert native users to Active Directory users for authenticating the users who log on to the ServiceDesk portal.
Process AD Changes Using Workflow	This option is not available from the ServiceDesk Portal because it does not apply to ServiceDesk.
Ignore AD Users (Comma separated)	Lets you specify any Active Directory users that should not be imported to ServiceDesk. You can type one or more user names and separate them with commas.

If you need to add, edit, and maintain the Active Directory server connections, you can do so from Workflow Explorer.

See "Managing Active Directory server connections" on page 407.

After you add and Active Directory server connection, you can add sync profiles. You can use these sync profiles to target the entire domain, organizational units and groups on the AD server, or for specific LDAP queries.

See "Managing Active Directory sync profiles" on page 418.

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 ServiceDesk 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 **Relates To**, select the type of relationship.

The relationship can relate to users, groups, permissions, or organizational units.

5 Click **Save**.

Appendix A

Default permissions in ServiceDesk

This appendix includes the following topics:

Default ServiceDesk permissions by category

ServiceDesk contains the default permissions that determine what screens and actions are available to users.

Administrators and users with the appropriate permissions can view all the default permissions in the ServiceDesk portal. They can also edit the permission information.

See "Viewing the list of ServiceDesk permissions" on page 395.

On the **List Permissions** page, the **Browse Permissions** section lists the permission categories, which organize the permissions by function. When you click a category, the permissions for that category appear at the right of the page.

When you assign a permission to a group or other entity, the permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

Table A-1 Default ServiceDesk permissions by category

Permission category	Permission name	Permission granted
Account	CompanyAdministration	Add or remove users to or from the organizational unit to which the user belongs.
Account	CompanyAdministration.PasswordReset	Reset passwords for users in the organizational unit to which the user belongs.
Account	ManageDelegations	Manage the delegations for others users.
AccountManagement	Access	Access everything in the **Users** area of the **Admin** module.
AccountManagement	Group.Create	Create a new group.
AccountManagement	Group. Modify	Modify an existing group.
AccountManagement	Permission.Create	Create a new permission.
AccountManagement	Permission.Modify	Modify an existing permission.
AccountManagement	Retrieve.Reference.Name	See reference names. This permission is used in a Userman method that is called GetReferenceName which is then used in Components.
AccountManagement	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
AccountManagement	User.CanResetPassword	Reset another user's password.
AccountManagement	User.Create	Create new users.
AccountManagement	User.FetchInfo	Retrieve a user' information.
AccountManagement	User.Modify	Modify an existing user.
Applications		Application permissions are related to the enterprise repository, and any applications permissions can be safely ignored.
Articles	Access	Access the knowledge base.
Articles	CanAddArticle	Add or update knowledge base articles.
Articles	CanAddCategory	Add categories.

Table A-1 Default ServiceDesk permissions by category *(continued)*

Permission category	Permission name	Permission granted
Articles	CanDeleteArticle	Delete knowledge base articles.
Articles	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
Discussions	Access	Access the threaded discussions module.
Discussions	Administrator	Remove and edit posts. The user with this administrative permission is the discussion moderator.
Discussions	Create	Create discussions.
Discussions	GroupManagement	Create and manage discussion threads on the **Discussions** page.
Discussions	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
DocumentManagement	Access	Access the document management module.
DocumentManagement	CanAddRootCategory	Add root categories to the document management module.
DocumentManagement	CanCheckoutDocuments	Check out documents from the document management module.
DocumentManagement	CanEditDocumentTypes	Edit the document types that are allowed in the document management module.
DocumentManagement	CanPostDocumentsForOther	Can add documents on behalf of other users.
DocumentManagement	CanPromoteDocumentVersions	Promote new versions of documents.
DocumentManagement	CanViewCategoryHistory	View the category history in the document management module.
DocumentManagement	CanViewDocumentHistory	View document history in the document management module.the
DocumentManagement	CanViewHiddenCategories	View hidden categories in the document management module.
DocumentManagement	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.

Table A-1 Default ServiceDesk permissions by category *(continued)*

Permission category	Permission name	Permission granted
ProcessManager	User.Interface.Beta	Access pre-release versions of the beta portal pages. Even with this permission, a user might not see beta pages.
Forms	Access	Access the Service Catalog module.
Forms	Create	Create new forms.
Forms	Delete	Delete existing forms.
Forms	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
Hierarchy	Access	Access the Hierarchy Data Service.
Hierarchy	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
Portal	Admin	Perform most portal actions, such as creating portal pages, deleting portal pages, and editing portal pages.
Portal	CanAddPages	Create new portal pages.
Portal	PersonalCustomization	Customize a portal page. Other users cannot see these customizations. Customization is allowed only on the pages for which customization has been enabled.
Portal	SuperAdmin	Access all portal functions. This permission lets the user make any changes necessary to ensure that the portal functions properly for other users. For example, if a user with the Portal.Admin permission accidentally denies their own access to a portal area, the SuperAdmin user can reset that permission.
ProcessData	Access	Access the reports module.

Table A-1 Default ServiceDesk permissions by category *(continued)*

Permission category	Permission name	Permission granted
ProcessData	CanViewFullProcessViewPage	View the entire process view page. This permission does not override other permissions. To see the full process view page, a user needs this permission and permission to view all of the parts on the page.
ProcessData	DefineFilters	Define filters for reports.
ProcessData	Reports	View a particular report.
ProcessData	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
ProcessData	ViewAll	View all the processes. This permission is a super administrator privilege for processes.
ProcessData	WriteReports	Create reports.
Profile	Access	Access the Profiles module.
Profile	CanViewTree	View the profile tree.
Profile	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
Reports	Access	Access the reporting module.
Reports	Access.ReplicationSchedule	Access the replication schedule.
Reports	Access.ReportSchedule	Access the report schedule.
Reports	OLAP.Create	Create OLAP reports.
Reports	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
Reports	ViewRDD	View a report as RSS.
Schedules	Access	Access the schedules module.
Schedules	CanCreate	Create schedules.
Schedules	CanDelete	Delete schedules.

Table A-1 Default ServiceDesk permissions by category *(continued)*

Permission category	Permission name	Permission granted
Schedules	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.
ServiceDesk	CanViewAllIncidents	View all incidents in ServiceDesk.
ServiceDesk	CanViewChangeSchedules	View the change schedules and release schedules.
ServiceDesk	CanViewProblemManagementTickets	View all the problem tickets in ServiceDesk.
ServiceDesk	Incident.CanSelectAssignment	Select a specific person to assign a task to.
UserLicenseLevel	ProcessManager	Access the ServiceDesk portal.
UserLicenseLevel	ServiceDesk	Access ServiceDesk.
WorkflowTasksManagement	Access	Access the Workflow tasks.
WorkflowTasksManagement	Add	Add Workflow tasks.
WorkflowTasksManagement	AllowBreakLeases	Break a leased task.
WorkflowTasksManagement	CanCloseAnyTask	Close any task, including the tasks that are not assigned to the user who has this permission. This permission is generally granted to administrators only.
WorkflowTasksManagement	CanCompleteAnyTask	Complete any task, including the tasks that are not assigned to the user who has this permission.
WorkflowTasksManagement	CanManageAttributes	Maintain task attributes.
WorkflowTasksManagement	CanRemoveTask	Remove any task, including the tasks that are not assigned to the user who has this permission.
WorkflowTasksManagement	CanSetupDefaultProfile	Set up the default profile.
WorkflowTasksManagement	Modify	Modify any task, including the tasks that are not assigned to the user who has this permission.
WorkflowTasksManagement	ShowInMenu	View this module on the tab bar or menu bar in the ServiceDesk portal.

Table A-1 Default ServiceDesk permissions by category *(continued)*

Permission category	Permission name	Permission granted
WorkflowTasksManagement	ViewAllTasks	View all the tasks in ServiceDesk, including the tasks that are not assigned to the user who has this permission.
WorkflowTasksManagement	ViewUnassignedTasks	View all the unassigned tasks in ServiceDesk, including the tasks that are not assigned to the user who has this permission.

Default ServiceDesk user groups

The ServiceDesk installation creates default user groups. Each group has the predefined permissions that determine what permissions are granted to the users who are members of that group.

See "About group-level permissions" on page 387.

Administrators and users with the appropriate permissions can view all the default permissions in the ServiceDesk portal. They can also edit the permission information.

See "Adding or removing permissions for groups" on page 394.

Table A-2 Default ServiceDesk user groups

Group	Description
Administrators	Contains the users who administer ServiceDesk. The Administrators group is granted all available permissions and can access all the tabs in the ServiceDesk portal.
All Users	Contains all ServiceDesk users with valid accounts. All users can create requests, view and confirm their resolved incidents, access the knowledge base, and perform other common tasks. They can also perform other actions, which depend on what other groups the users belongs to. See "Default permissions for the All Users group" on page 476.
Application Users	See "Default permissions for the All Users group" on page 476.

Table A-2 Default ServiceDesk user groups *(continued)*

Group	Description
Change Implementers	Contains the users that can be chosen to implement the individual tasks that are required for a Change. When Change Planners work on a change, they can pick users from the Change Implementers group. Any member of this group is a member of other groups. Any ServiceDesk user can be a member of this group. The change implementers can perform the tasks that are associated with their roles in the change process. They can also perform other actions, which depend on what other groups the users belongs to. See "Default permissions for the Change Implementers group" on page 479.
Change Manager	Contains the users who orchestrate changes by assigning roles to change implementers. Change Managers have the final sign-off on changes. Change managers can create incidents and problems, request changes, approve changes, and view and work tasks, including the tasks that are assigned to others. They can also view all tickets, run reports, and submit knowledge base articles. See "Default permissions for the Change Manager group" on page 480.
Change Notification	Contains the users who always get notifications on all changes, whether they are a member of the change group or not. The change notification group can perform the tasks that are associated with their roles in the change process. They can also perform other actions, which depend on what other groups the users belongs to. See "Default permissions for the Change Notification group" on page 482.
Change Team - Default	The members of this group are customizable groups of the users that the Change Manager chooses to work on a change. The members of a Change Team should be related in some way, such as by location. When a Change Manager configures a change, they can select an existing Change Team to work on the Change or create a new team. Any member of this group is a member of other groups. The change team can perform the tasks that are associated with their roles in the change process. They can also perform other actions, which depend on what other groups the users belongs to. See "Default permissions for the Change Team - Default group" on page 483.
KB Approvers	Contains the users who are assigned to approve knowledge base articles. KB (knowledge base) approvers can create incidents and problems, request changes, and work their assigned tasks. They can also view all tickets and edit the knowledge base entries. See "Default permissions for the KB Approvers group" on page 484.

Table A-2 Default ServiceDesk user groups *(continued)*

Group	Description
KB Editors	Contains the users who are assigned to review and edit knowledge base articles. KB editors can create incidents and problems, request changes, and work their assigned tasks. They can also view all tickets and edit the knowledge base entries. See "Default permissions for the KB Editors group" on page 486.
Problem Analyst	Contains the users who are assigned to work on problems. Problem analysts can create incidents and problems, request changes, and view and work tasks, including the tasks that are assigned to others. They can also view all tickets, run reports, and submit knowledge base articles. See "Default permissions for the Problem Analyst group" on page 487.
Problem Reviewer	Contains the users that are one level higher than Problem Analysts. These users have approval rights for problems, and review and implement problem resolution proposals submitted by Problem Analysts. Problem Reviewers can create incidents and problems, request changes, work tasks (including those assigned to others), view tickets, submit knowledge base articles , and run reports. See "Default permissions for the Problem Reviewer group" on page 489.
Service Managers	Contains the users in the tier that is higher than ServiceDesk Technicians. ServiceManagers manage all of ServiceDesk. They receive emergency escalation and keep ServiceDesk running smoothly. They can also view all tickets, run reports, and submit knowledge base articles. Service managers can create incidents and problems, request changes, approve changes, and view and work tasks, including the tasks that are assigned to others. See "Default permissions for the Service Managers group" on page 491.
Support I	Contains the ServiceDesk technicians on the first tier of customer support. Users in this group view and work incidents, and resolve them if possible. If they cannot resolve the incidents, they can escalate them to Support II or create a problem. Support I users can create incidents and problems, request changes, and view and work incident tasks. They can also view all tickets, run reports, and submit knowledge base articles. See "Default permissions for the Support I group" on page 493.

Table A-2 Default ServiceDesk user groups *(continued)*

Group	Description
Support II	Contains the ServiceDesk technicians on the second tier of customer support. Users in this group can view and work the incidents that Support I users have escalated, or make assignments to other users. Support II users can create incidents and problems, request changes, and view and work incident tasks, including the tasks that are assigned to others. They can also view all tickets, run reports, and submit knowledge base articles. See "Default permissions for the Support II group" on page 494.

Default permissions for the All Users group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the All Users group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Knowledge Base**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the All Users group are as follows:

- AccountManagement.User.FetchInfo
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement

- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- Forms.Access
- ProcessData.Access
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- ProcessManager.ShowNotifications
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Application Users group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Application Users group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Knowledge Base**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Application Users group are as follows:

- AccountManagement.User.FetchInfo
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- Forms.Access
- ProcessData.Access
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- ProcessManager.ShowNotifications
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Change Implementers group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

The ServiceDesk portal tabs that the Change Implementers group can access depends on what other groups the user is a member of.

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Change Implementers group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports

- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Change Manager group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Change Manager group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Change Manager group are as follows:

- AccountManagement.Access
- Articles.Access

- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Reports.ShowInMenu
- Schedules.Access
- Schedules.ShowInMenu
- ServiceDesk.CanViewAllIncidents
- ServiceDesk.CanViewChangeSchedules
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 473.

Default permissions for the Change Notification group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

The ServiceDesk portal tabs that the Change Notification group can access depends on what other groups the user is a member of.

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Change Notification group are as follows:

- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- Forms.Access
- ProcessData.Access
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access

- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Change Team - Default group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

The ServiceDesk portal tabs that the Change Team - Default group can access depends on what other groups the user is a member of.

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Change Team - Default group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage

- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the KB Approvers group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the KB Approvers group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the KB Approvers group are as follows:

- Articles.Access
- Articles.CanAddArticle
- Articles.CanDeleteArticle
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanAddRootCategory
- DocumentManagement.CanCheckoutDocuments
- DocumentManagement.CanEditDocumentTypes
- DocumentManagement.CanPromoteDocumentVersions
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.CanViewHiddenCategories
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access

- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the KB Editors group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the KB Editors group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the KB Editors group are as follows:

- Articles.Access
- Articles.CanAddArticle
- Articles.CanDeleteArticle
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu

- DocumentManagement.Access
- DocumentManagement.CanAddRootCategory
- DocumentManagement.CanCheckoutDocuments
- DocumentManagement.CanEditDocumentTypes
- DocumentManagement.CanPromoteDocumentVersions
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.CanViewHiddenCategories
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Schedules.Access
- Schedules.ShowInMenu
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 473.

Default permissions for the Problem Analyst group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Problem Analyst group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**
- **Reports**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Problem Analyst group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters

- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Reports.ShowInMenu
- Schedules.Access
- Schedules.ShowInMenu
- ServiceDesk.CanViewAllIncidents
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Problem Reviewer group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Problem Reviewer group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**
- **Reports**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Problem Reviewer group are as follows:

- AccountManagement.Access
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create
- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Reports.ShowInMenu
- Schedules.Access
- Schedules.ShowInMenu

- ServiceDesk.CanViewAllIncidents
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Service Managers group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Service Managers group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Supervisor Dashboard**
- **Knowledge Base**
- **Documents**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as Articles.Access.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Service Managers group are as follows:

- AccountManagement.Access
- AccountManagement.User.FetchInfo
- Applications.DirectoryService.DefaultAccess
- Articles.Access
- Articles.ShowInMenu
- Discussions.Access
- Discussions.Create

- Discussions.GroupManagement
- Discussions.ShowInMenu
- DocumentManagement.Access
- DocumentManagement.CanViewCategoryHistory
- DocumentManagement.CanViewDocumentHistory
- DocumentManagement.ShowInMenu
- Forms.Access
- ProcessData.Access
- ProcessData.CanViewFullProcessViewPage
- ProcessData.DefineFilters
- ProcessData.Reports
- ProcessData.ViewAll
- ProcessData.WriteReports
- Profile.Access
- Profile.CanViewTree
- Reports.Access
- Reports.OLAP.Create
- Reports.ShowInMenu
- Schedules.Access
- Schedules.CanCreate
- Schedules.ShowInMenu
- ServiceDesk.CanViewAllIncidents
- ServiceDesk.CanViewChangeSchedules
- ServiceDesk.CanViewProblemManagementTickets
- ServiceDesk.Incident.CanSelectAssignment
- UserLicenseLevel.ServiceDesk
- WorkflowTaskManagement.Access

See “Default ServiceDesk user groups” on page 473.

Default permissions for the Support I group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Support I group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**
- **Tickets**
- **Knowledge Base**
- **Documents**
- **Reports**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as **Articles.Access**.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Support I group are as follows:

- **AccountManagement.Access**
- **AccountManagement.User.CanResetPassword**
- **AccountManagement.User.Create**
- **AccountManagement.User.FetchInfo**
- **AccountManagement.User.Modify**
- **Applications.DirectoryService.DefaultAccess**
- **Articles.Access**
- **Articles.ShowInMenu**
- **Discussions.Access**
- **Discussions.Create**
- **Discussions.GroupManagement**

- **Discussions.ShowInMenu**
- **DocumentManagement.Access**
- **DocumentManagement.CanViewCategoryHistory**
- **DocumentManagement.CanViewDocumentHistory**
- **DocumentManagement.ShowInMenu**
- **Forms.Access**
- **ProcessData.Access**
- **ProcessData.CanViewFullProcessViewPage**
- **ProcessData.DefineFilters**
- **ProcessData.Reports**
- **ProcessData.ViewAll**
- **ProcessData.WriteReports**
- **Profile.Access**
- **Profile.CanViewTree**
- **Reports.Access**
- **Reports.OLAP.Create**
- **Reports.ShowInMenu**
- **Schedules.Access**
- **Schedules.ShowInMenu**
- **UserLicenseLevel.ServiceDesk**
- **WorkflowTaskManagement.Access**

See "Default ServiceDesk user groups" on page 473.

Default permissions for the Support II group

The permissions that are assigned to this group determine what permissions are granted to the ServiceDesk users who are members of this group.

By default, the Support II group can access the following tabs in the ServiceDesk portal:

- **Home**
- **Submit Request**
- **My Task List**

- **Tickets**
- **Knowledge Base**
- **Documents**
- **Reports**

Administrators and users with the appropriate permissions can view and edit the group permissions.

See "Viewing the permissions for a group" on page 396.

The permission name is a combination of the category plus the permission. For example, the Articles category contains a permission named Access. On the screens where you assign that permission, the permission name appears as **Articles.Access**.

See "Default ServiceDesk permissions by category" on page 467.

The default permissions for the Support II group are as follows:

- **AccountManagement.Access**
- **AccountManagement.User.CanResetPassword**
- **AccountManagement.User.Create**
- **AccountManagement.User.FetchInfo**
- **AccountManagement.User.Modify**
- **Applications.DirectoryService.DefaultAccess**
- **Articles.Access**
- **Articles.ShowInMenu**
- **Discussions.Access**
- **Discussions.Create**
- **Discussions.GroupManagement**
- **Discussions.ShowInMenu**
- **DocumentManagement.Access**
- **DocumentManagement.CanViewCategoryHistory**
- **DocumentManagement.CanViewDocumentHistory**
- **DocumentManagement.ShowInMenu**
- **Forms.Access**
- **ProcessData.Access**

- **ProcessData.CanViewFullProcessViewPage**
- **ProcessData.DefineFilters**
- **ProcessData.Reports**
- **ProcessData.ViewAll**
- **ProcessData.WriteReports**
- **Profile.Access**
- **Profile.CanViewTree**
- **Reports.Access**
- **Reports.OLAP.Create**
- **Reports.ShowInMenu**
- **Schedules.Access**
- **Schedules.ShowInMenu**
- **ServiceDesk.CanViewAllIncidents**
- **ServiceDesk.Incident.CanSelectAssignment**
- **UserLicenseLevel.ServiceDesk**
- **WorkflowTaskManagement.Access**

See “Default ServiceDesk user groups” on page 473.

Index

Symbols

A

B