Symantec™ ServiceDesk 7.5 MP1 Release Notes

Symantec™ ServiceDesk 7.5 MP1 Release Notes

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™ ServiceDesk 7.5 MP1 Release Notes

This document includes the following topics:

- About ServiceDesk 7.5 MP1

- What's new in ServiceDesk 7.5 MP1

- ServiceDesk 7.5 MP1 support matrix

- System requirements for ServiceDesk

- Server configuration options for ServiceDesk

- Installing ServiceDesk 7.5 MP1

- Upgrading from ServiceDesk 7.5 to ServiceDesk 7.5 MP1

- Migrating to ServiceDesk 7.5 MP1

- Migrating data to ServiceDesk 7.5 MP1

- Known issues

- Fixed issues

- Other things to know

- Documentation that is installed

- Other information

About ServiceDesk 7.5 MP1

Symantec ServiceDesk improves your infrastructure's service management.

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

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

You can configure ServiceDesk to meet your organization's specific requirements. These configurations include setting up business hours, routing rules for incidents and changes, and email templates and notification rules. You can implement advanced customizations. These customizations may include creating data types, modifying feeder forms, modifying the Process View page, and adding fields to reports.

For more information, see the following:

Symantec™ ServiceDesk 7.5 MP1 Implementation Guide

Symantec™ ServiceDesk 7.5 MP1 User Guide

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

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

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

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

What's new in ServiceDesk 7.5 MP1

In the 7.5 MP1 release of ServiceDesk, the following new features are introduced:

Table 1-1   List of new features in ServiceDesk 7.5 MP1

Feature	Description
Ability to authenticate an SMTP server that requires authentication to send emails.	■ You can authenticate an SMTP server during installation or upgrade when you configure the outbound and the inbound email settings. ■ You can authenticate an SMTP server in the Process Manager portal from the **Application Properties** page and in **Master Settings**.
Ability to specify times when you schedule changes.	The Change Management process lets you specify the dates and times when you schedule your changes.
Ability to assign subtasks to groups.	The Incident Management process lets you assign subtasks to users and groups.
Ability to set the incident resolution timeout.	The Incident Management incident resolution timeout can be configured from the **Application Properties** page in the Process Manager portal. By default, the incident resolution timeout is set to three days.
Ability to set the level of classification that is required to resolve an incident.	The level of classification to resolve an incident can be configured from the **Application Properties** page in the Process Manager portal. By default, the Incident Management process only requires a partial classification to resolve an incident. Classifications requirements can be set to full or partial.
Process Messages and Comments display first and last names in addition to email address.	Technicians can view the first and last names and email addresses in the **Comments** and the **Process History** sections on the Incident ticket's **Process View** page.
Active Directory auto-authentication is supported in Chrome and Firefox.	Active Directory auto-authentication is supported in Chrome and Firefox in addition to Internet Explorer. For any additional configurations that may be required, see the knowledge base article, Pass-thru Authentication with Chrome & Firefox on ServiceDesk & Workflow at: http://www.symantec.com/docs/TECH204270

Table 1-1 List of new features in ServiceDesk 7.5 MP1 *(continued)*

Feature	Description
New Incident Management automation ruleset conditions	■ The **Incident Type** condition was added to the Incident Management Process Automation Rulesets. ■ The **Incident Is In Queue** condition was added to the Incident Management Process Automation Rulesets.

See "Installing ServiceDesk 7.5 MP1" on page 16.

See "Upgrading from ServiceDesk 7.5 to ServiceDesk 7.5 MP1" on page 17.

See "Migrating to ServiceDesk 7.5 MP1" on page 18.

ServiceDesk 7.5 MP1 support matrix

The support matrix provides an overview of the primary ServiceDesk components and their supported operating systems. It displays the versions of the operating systems that are supported and the versions that are not supported in ServiceDesk 7.5 MP1.

See "System requirements for ServiceDesk" on page 8.

Table 1-2 ServiceDesk support matrix

Component	Supported in ServiceDesk 7.5 MP1	Support new to ServiceDesk 7.5 MP1	Not Supported in ServiceDesk 7.5 MP1
Symantec Management Platform (for ServiceDesk)	■ 7.1 SP2	N/A	■ 7.1 ■ 7.1 SP1
ServiceDesk Server/Process Manager portal operating system (OS)	■ Windows Server 2008 R2 SP1	N/A	■ Windows Server 2003 (all versions) ■ Windows Server 2008 (pre-R2) ■ Windows Server 2008 R2

Table 1-2 ServiceDesk support matrix *(continued)*

Component	Supported in ServiceDesk 7.5 MP1	Support new to ServiceDesk 7.5 MP1	Not Supported in ServiceDesk 7.5 MP1
Microsoft SQL Server	- Microsoft SQL Server 2005 SP4 - Microsoft SQL Server 2008 SP2 - Microsoft SQL Server 2008 SP3 - Microsoft SQL Server 2008 R2 - Microsoft SQL Server 2008 R2 SP1 - Microsoft SQL Server 2008 R2 SP2 - Microsoft SQL Server 2012	- Microsoft SQL Server 2008 SP3 - Microsoft SQL Server 2008 R2 SP2 - Microsoft SQL Server 2012	- Microsoft SQL Server 2005 SP2 - Microsoft SQL Server 2005 SP3 - Microsoft SQL Server 2008 - Microsoft SQL Server 2008 SP1
Workflow Designer operating system (OS)	- Windows 7 x86 and x64 - Windows 7 SP1 x86 and x64 - All ServiceDesk Server supported OS versions	N/A	- Windows XP SP2 - Windows XP SP3 x86 - Windows Vista SP1 - Windows Vista SP2 x86 and x64
Process Manager portal browsers	- Microsoft Internet Explorer versions 7, 8, and 9 - Firefox version 13 and later - Google Chrome version 17 and later - Safari version 5 and later **Note:** Active Directory auto-authentication is supported in Internet Explorer, Google Chrome, and Firefox. For any additional configurations that may be required, see the knowledge base article, Pass-thru Authentication with Chrome & Firefox on ServiceDesk & Workflow at http://www.symantec.com/docs/TECH204270	N/A	N/A

System requirements for ServiceDesk

ServiceDesk requires that you dedicate certain servers.

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

See "Server configuration options for ServiceDesk" on page 14.

Table 1-3   The dedicated servers that ServiceDesk requires

Server	Description
Symantec Management Platform	ServiceDesk requires a 7.1 SP2 instance of the Symantec Management Platform.
	See "ServiceDesk requirements for the Symantec Management Platform" on page 9.
ServiceDesk server	The ServiceDesk server is a 64-bit server on which you install the Workflow Platform and the ServiceDesk modules.
	This server might also be referred to as the Process Manager server or the Workflow Server.
	This server cannot contain an installation of Helpdesk Solution.
	See "System requirements for the ServiceDesk server" on page 10.
SQL Server	The Process Manager databases must reside on a SQL Server.
	Symantec recommends that ServiceDesk has its own dedicated off-box SQL Server.
	See "System requirements for the SQL Server" on page 12.
	See "About supported SQL Server collations for the Process Manager database" on page 13.

See "Requirements for the ServiceDesk client computers" on page 14.

ServiceDesk requirements for the Symantec Management Platform

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

Table 1-4   ServiceDesk requirements for the Symantec Management Platform

Item	Requirement
Hardware and base software	For information about the Symantec Management Platform 7.1 SP2 hardware and the software requirements, see the chapter *Performance and scalability recommendations for IT Management Suite* in the Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide.
Symantec Management Platform	A 7.1 SP2 instance of the Symantec Management Platform must be installed and running.
	The installation of your instance of the Symantec Management Platform is managed through the Symantec Installation Manager.

| Table 1-4 | ServiceDesk requirements for the Symantec Management Platform *(continued)* |

Item	Requirement
Altiris Configuration Management Database Solution (CMDB Solution)	If the Configuration Management Database Solution is not already installed, it is included in the installation of the ServiceDesk Solution software. You do not need to perform a separate installation.

System requirements for the ServiceDesk server

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

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

- Both servers must be members of the same domain.

- This configuration must be installed in an Active Directory environment.

| Table 1-5 | System requirements for the ServiceDesk server |

Item	Requirement
Server and processor	Multi-core or multiple processors, 64-bit
RAM	■ Minimum: 8 GB (recommended for test servers only) ■ Minimum recommended: 16 GB ■ Preferred: 32 GB
Operating system	Windows Server 2008 R2 SP1, 64 bit
Network configuration	■ IP v4 ■ Static IP address ■ Name resolution services (DNS) ■ Internet connectivity ■ Connectivity to the Symantec Management Platform server ■ Gigabit Network Interface Controller (GB NIC)

Table 1-5   System requirements for the ServiceDesk server *(continued)*

Item	Requirement
Installation account	ServiceDesk requires an installation account: ■ **Windows** (Windows Integrated Security) Use a domain account with the *sysadmin* server role on the target SQL instance. ■ **SQL** (Microsoft SQL Server Security) Use a SQL account with the *sysadmin* server role for that target SQL instance. Note: If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Operation service account	ServiceDesk requires a run-time service account. ■ **Windows** (Windows Integrated Security) Use a domain service account that is set up in that SQL instance. This account is used as the identity under which the ServiceDesk application pool runs in IIS. This account is added to the *db_owner* role on the Process Manager database. Note: This authentication method is the recommended authentication method. Windows authentication allows for easy upgradeability and provides the greatest ease of change. Because connection string information is stored in the Web.config files of Projects, Windows authentication also adds security. ■ **SQL** (Microsoft SQL Server Security) Use an account in the target SQL instance. This account is added to the *db_owner* role on the Process Manager database. Note: If you plan to use this authentication method, the target database server must be configured to support SQL authentication.
Email account	■ Primary email account for the ServiceDesk mailbox for monitoring the system and sending email from the system ■ SMTP server connectivity ■ (Optional) POP or IMAP mailbox for monitoring
SQL Server components	The ServiceDesk server requires the SQL Server ADOMD.NET. This SQL Server component is a Microsoft .NET Framework data provider. It facilitates communication with the Microsoft SQL Server Analysis Services. If SQL Server is installed on a server that is separate from the ServiceDesk server (off-box), the ServiceDesk server requires the following SQL Server components: ■ SQL Management Objects (SMO) site ■ SQL Server Analysis Management Objects (AMO) ■ Microsoft ADOMD.NET ■ SQL Native client This component is a prerequisite for installing the SQL Management Objects.

| Table 1-5 | System requirements for the ServiceDesk server *(continued)* |

Item	Requirement
Microsoft Internet Information Services (IIS)	IIS 7 (IIS 6 Management Compatibility mode)
.NET Framework	.NET 3.5 with ASP.NET
Internet browser	ServiceDesk is intended to work with all of the major Internet browsers. We have tested ServiceDesk with the following browsers: ■ Microsoft Internet Explorer versions 7, 8, and 9 ■ Firefox version 13 and later ■ Google Chrome version 17 and later ■ Safari version 5 and later **Note:** Active Directory auto-authentication is supported in Internet Explorer, Chrome, and Firefox. For any additional configurations that may be required, see the knowledge base article, Pass-thru Authentication with Chrome & Firefox on ServiceDesk & Workflow at http://www.symantec.com/docs/TECH204270.

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

System requirements for the SQL Server

ServiceDesk requires an installation of Microsoft SQL Server.

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

■ Both servers must be members of the same domain.

■ This configuration must be installed in an Active Directory environment.

| Table 1-6 | System requirements for the SQL Server |

Item	Requirement
Processor	32-bit or 64-bit Symantec recommends that you use a 64-bit.
Operating system	Windows Server 2008 R2 SP1

Table 1-6   System requirements for the SQL Server *(continued)*

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

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

About supported SQL Server collations for the Process Manager database

The Process Manager database supports the following SQL Server collations:

■ SQL_Latin1_General_CP1_CI_AS - Latin alphabet, case insensitive, accent sensitive
  By default, the Process Manager database is created with this collation.

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

Requirements for the ServiceDesk client computers

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

Note: Active Directory auto-authentication is supported in Internet Explorer, Chrome, and Firefox.For any additional configurations that may be required, see the knowledge base article, Pass-thru Authentication with Chrome & Firefox on ServiceDesk & Workflow at http://www.symantec.com/docs/TECH204270.

We have tested ServiceDesk with the following browsers:

- Microsoft Internet Explorer versions 7, 8, and 9

- Firefox version 13 and later

- Google Chrome version 17 and later

- Safari version 5 and later

See "System requirements for ServiceDesk" on page 8.

Server configuration options for ServiceDesk

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

See "System requirements for ServiceDesk" on page 8.

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

Requirements for server configurations	A server configuration is valid if it meets the following requirements:
	■ Microsoft SQL Server is installed on either a 32-bit server or a 64-bit server. Symantec recommends that you use a 64-bit server. ■ The Symantec Management Platform and the ServiceDesk Solution software are installed on a 64-bit server. ■ ServiceDesk is installed on a 64-bit server. Separate from the Symantec Management Platform

Typical server configurations	The most commonly-used configurations are as follows:
■ SQL Server is installed off-box for both the Symantec Management Platform and ServiceDesk.
See Figure 1-1.
■ The Symantec Management Platform and ServiceDesk share an off-box SQL Server installation.
See Figure 1-2.
Additional server configurations	Examples of additional configurations are as follows:
■ SQL Server is installed off-box for either the Symantec Management Platform or ServiceDesk.
■ SQL Server is installed on-box for either the Symantec Management Platform or ServiceDesk, or both.
■ One of the applications uses an on-box installation of SQL Server and shares it with the other application.
■ One of the applications uses an on-box installation of SQL Server and the other application uses an off-box installation of SQL Server.
Unsupported server configurations	Symantec does not support the following server configuration:
■ Symantec Management Platform with ServiceDesk Solution software installed on the same server as the ServiceDesk application software.
Note: The Symantec Management Platform with ServiceDesk Solution must be installed to a separate server than the actual ServiceDesk application server.

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

Notification Server (Symantec Management Platform)

SQL Server

ServiceDesk Server
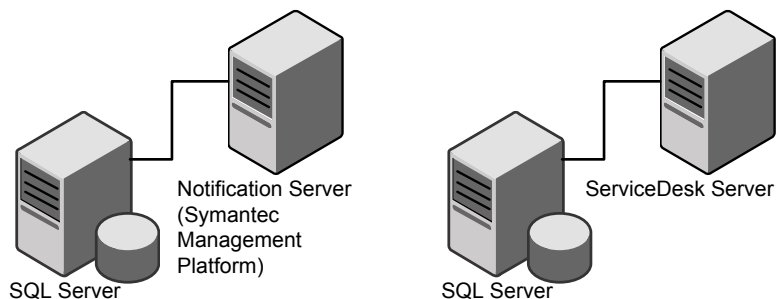
SQL Server

Figure 1-2   Symantec Management Platform and ServiceDesk share an off-box
SQL Server

Notification Server
(Symantec
Management
Platform)

SQL Server

ServiceDesk Server
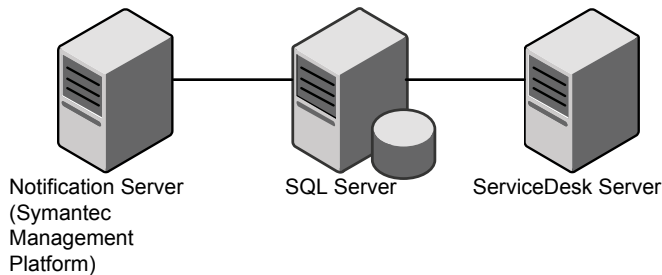
Installing ServiceDesk 7.5 MP1

You can install ServiceDesk as a standalone product. You can also install
ServiceDesk and use it along with the other products in the IT Management Suite.

Before you install ServiceDesk on the ServiceDesk server, see the topic
"ServiceDesk scalability" in the *Symantec™ ServiceDesk 7.5 MP1 Implementation
Guide* at:

http://www.symantec.com/docs/DOC6513

Things to know about the ServiceDesk installation process:

■ ServiceDesk 7.5 MP1 is compatible with Symantec Management Platform
versions 7.1 SP2 and 7.1 SP2 MP1. It is also compatible with IT Management
Suite versions 7.1 SP2 and 7.1 SP2 MP1.

■ You use the Symantec Installation Manager (SIM) to install the ServiceDesk
Solution software.
The ServiceDesk Solution software grants you access to the ServiceDesk Server
installer.

■ You use the ServiceDesk server installer to install the ServiceDesk application
on your new designated server.

For information about installing ServiceDesk, see the *Symantec™ ServiceDesk 7.5
MP1 Implementation Guide* at:

http://www.symantec.com/docs/DOC6513.

For information about installing the IT Management Suite, see the *Altiris™ IT
Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide*
at:

http://www.symantec.com/docs/DOC4827

See "About ServiceDesk 7.5 MP1" on page 4.

See "Upgrading from ServiceDesk 7.5 to ServiceDesk 7.5 MP1" on page 17.

See "Migrating to ServiceDesk 7.5 MP1" on page 18.

Upgrading from ServiceDesk 7.5 to ServiceDesk 7.5 MP1

Existing ServiceDesk 7.5 customers can perform an in-place same-server upgrade to ServiceDesk 7.5 MP1, which involves using the same server hardware.

Things to know about the ServiceDesk upgrade process

- ServiceDesk 7.5 MP1 is compatible with the Symantec Management Platform versions 7.1 SP2 and 7.1 SP2 MP1. It is also compatible with the IT Management Suite versions 7.1 SP2 and 7.1 SP2 MP1

- You use the Symantec Installation Manager (SIM) to upgrade the ServiceDesk Solution software on the Symantec Management Platform.
  The ServiceDesk Solution software grants you access to the ServiceDesk server installer.

- You use the ServiceDesk server installer to upgrade the ServiceDesk application on your ServiceDesk server.

Warning: Upgrading Workflow that shipped with ServiceDesk 7.5 or ServiceDesk 7.5 MP1 will break ServiceDesk.

Workflow Solution 7.5 is not compatible with ServiceDesk 7.5 or ServiceDesk 7.5 MP1. Do not upgrade the version of Workflow that shipped with ServiceDesk 7.5 or ServiceDesk 7.5 MP1 and is installed on the ServiceDesk Server to Workflow Solution 7.5. This will break ServiceDesk.

For information about upgrading to ServiceDesk 7.5 MP1, see the topic "Process for upgrading from ServiceDesk 7.5 to ServiceDesk 7.5 MP1" in the *Symantec™ ServiceDesk 7.5 MP1 Implementation Guide* at:

http://www.symantec.com/docs/DOC6513

See "What's new in ServiceDesk 7.5 MP1" on page 5.

See "Migrating to ServiceDesk 7.5 MP1" on page 18.

Migrating to ServiceDesk 7.5 MP1

Existing ServiceDesk 7.0, 7.1, 7.1 SP1, and 7.1 SP2 customers must migrate to ServiceDesk 7.5 MP1, which involves migrating to new hardware. This migration includes both the ServiceDesk server and a new Process Manager database instance. You should plan to install ServiceDesk in a new environment, separate from your existing ServiceDesk server. An in-place upgrade path is not available for pre- 7.5 versions of ServiceDesk. Symantec does not support attempts to install 7.5 MP1 over a pre- 7.5 version of ServiceDesk. You must run both systems in parallel until your previous tickets are closed and necessary data is migrated to your ServiceDesk 7.5 MP1 environment.

Things to know about the ServiceDesk migration process:

- You must first upgrade or migrate your instance of the Symantec Management Platform (and IT Management Suite if installed) to version 7.1 SP2.

- ServiceDesk 7.5 MP1 is compatible with Symantec Management Platform versions 7.1 SP2 and 7.1 SP2 MP1.

- You use the Symantec Installation Manager (SIM) to install or upgrade the ServiceDesk Solution software on the Symantec Management Platform. The ServiceDesk Solution software grants you access to the ServiceDesk server installer.

- You use the ServiceDesk server installer to install the ServiceDesk application on your new designated server.

For information about migrating to ServiceDesk 7.5 MP1, see the topic "Migrating to ServiceDesk 7.5 MP1" in the *Symantec™ ServiceDesk 7.5 MP1 Implementation Guide* at:

http://www.symantec.com/docs/DOC6513

For more information about upgrading or migrating to Symantec Management Platform 7.1 SP2, see the topic "About upgrading from IT Management Suite 7.1 to 7.1 SP2" in the *Symantec™ Management Platform 7.1 SP2 Installation Guide* at:

http://www.symantec.com/docs/DOC4798

Migrating data to ServiceDesk 7.5 MP1

You can leverage some of the data from ServiceDesk 7.0 MR2, 7.1 SP1, and 7.1 SP2 in ServiceDesk 7.5 MP1. You can migrate incidents, change requests, problems,

and other data. You can access this historical ticket data from ServiceDesk 7.5 MP1 for reporting purposes.

You can also leverage some data from Helpdesk Solution 6.x. You can migrate incidents, categories, and some knowledge base content.

For more information about migrating data to ServiceDesk 7.5 MP1, see the topic "About migrating data to ServiceDesk 7.5 MP1" in the *Symantec™ ServiceDesk 7.5 MP1 Implementation Guide* at:

http://www.symantec.com/docs/DOC6513

See "Migrating to ServiceDesk 7.5 MP1" on page 18.

Known issues

The following are known issues for this release. If additional information about an issue is available, the issue has a corresponding Article link.

For the most up-to-date information, latest workarounds, and other technical support information about this solution, see the Technical Support knowledge base.

Table 1-7 Known issues

Issue	Description	Article link
Clean and upgrade installations of ServiceDesk 7.5 MP1 are blocked when an Admin email address with a top-level domain longer than four characters is used.	The **Admin Account Name** check on the **Workflow Installation Options** page in the ServiceDesk installer does not let you continue with clean or upgrade installations if you use an email address with a top-level domain longer than four characters For example, the Admin email address check lets you use *admin@symantec.test*, but blocks installations if you use *admin@symantec.local*. **Workaround:** See the *KNOWN ISSUE: ServiceDesk 7.5 MP1 upgrade will not pass the Workflow admin account verification* knowledge base article.	TECH206746
A new ServiceDesk installation fails if you do not close the ServiceDesk installation wizard after you run an uninstall.	Using the ServiceDesk installer to uninstall ServiceDesk and/or Workflow and then to reinstall ServiceDesk without closing the installer after the uninstall causes error during reinstallation. **Workaround:** After using the ServiceDesk installer to uninstall ServiceDesk and/or Workflow, close the ServiceDesk installer before using it to reinstall ServiceDesk.	

Table 1-7	Known issues *(continued)*

Issue	Description	Article link
No default report is provided to display the incidents that are on hold.	After an incident is placed on hold, it disappears from reports and task lists. No default report is provided to display the incidents that are on hold. See the *Incidents on Hold do Not Disappear from Open Ticket Reports* knowledge base article.	TECH199688
Adding groups to and removing groups from Service Queues does not affect currently assigned incidents.	The group-to-service queue relationship is only used during ticket assignment. Adding groups to and removing groups from Service Queues only affects future assignments and does not affect currently assigned incidents. **Workaround:** Individual ticket assignments can be reset when you reassign them to the queue to which they are currently assigned.	
Deleting a Service Queue can cause routing rules to fail.	If you delete a service queue before you modify the routing rules that route incidents to that queue, the routing rules error out. **Workaround:** Before you delete a service queue, modify all the rules that route incidents to the queue and route them to another queue.	
Deleting a Service Queue does not affect existing ticket assignments.	If a service queue is deleted, all existing tickets stay assigned to the service queue's groups. **Workaround:** Individual ticket assignments can be reset when you reassign them to a different queue.	
Service Queues do not detect newly created groups.	Opening the **Create/Edit Service Queue** page caches the existing ServiceDesk groups. The Service Queues do not detect newly created groups. **Workaround:** See the *New Queue and Group does Not Show Up after Creation* knowledge base article.	TECH198039
The **Send Email** action is displayed twice in the **Add Action** drop-down list for rules in the **DocumentAdded** ruleset.	When you create rules for the **DocumentAdded** data event ruleset, the **Send Email** action appears twice in the **Add Actions** drop-down list. You can use both **Send Email** actions; both actions produce the same results.	

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
Change managers cannot add a category or a bulletin board when adding a bulletin board entry.	Members of the Change Manager group receive an error when they click **Add Category** or **Add Bulletin Board** on the **Add Bulletin Board Entry** page. Change Manager group does not have the **Articles.CanAddCategory** and the **Articles.CanAddArticle** permissions. **Workaround:** Grant the **Articles.CanAddCategory** and the **Articles.CanAddArticle** permissions to the Change Manager group.	
Change request ticket's **Process History** does not display the execution of the automation rules.	When you open a change request ticket's **Process View** page, the execution of the automation rules is not displayed in the **Process History** section. By default, the **Process Messages** filter is turned off. **Workaround:** ■ Open a change request ticket. ■ On the ticket's **Process View** page, in the **Process History** section, click **Filter**. ■ In the **Filter Options** dialog box, in the **Messages** section, check **Process Messages** and then click **Apply**. ■ The **Process History** section on your change tickets' **Process View** page displays the automation rules execution.	
False failure can be reported on knowledge base article creation.	When you create a knowledge base article from a problem, a failure is reported even though the article was created successfully. To verify that the article was created successfully, navigate to the **Knowledge Base** page and search for the article.	
False failure may be reported on a submitted incident, a change request, or a problem.	After a new install of ServiceDesk 7.5 MP1 or an IISRESET, the first submitted incident, change request, or problem reports an error even though the incident, the change request, or problem was submitted successfully.	
In Problem Management, all **List Open Problems...** reports and all **Problems Closed...** reports do not display ticket data.	The Problem Management **List Open Problems...** reports and **Problems Closed...** reports do not extract the correct data. **Workaround:** See the *When trying to run any of the Problem Management reports the result is No Data* knowledge base article.	TECH200490

Table 1-7   Known issues *(continued)*

Issue	Description	Article link
Manually setting the Workflow Platform server to a non-default port causes the ServiceDesk installation to fail.	If you manually set the Workflow Platform to a non-default HTTP port or HTTPS port, your ServiceDesk prerequisite check and ServiceDesk installation fail.	
The **Manage Related Configuration Items** process type action lets you add multiple references of the same asset to the same incident or change request.	When you use the **Manage Related Configuration Items**, **Process Action** to associate assets to an incident or a change request, you can associate the same asset to the same incident or change request multiple times.	TECH204841
Fields in the **Submit Incident (Advanced)** form are not reset to default values when you use the **Start Another Ticket** option.	When you use the **Submit Incident (Advanced)** form to submit an incident and then use the **Start Another Ticket** option on the **Thank You** page to submit another incident, several fields in the form are not reset to their default values. **Workaround:** See the *KNOWN ISSUE: Several fields on the Advanced Form don't reset to defaults when you choose the option to start another incident* knowledge base article.	TECH204898
More than one person working on the **Process Automation Rulesets** at the same time can cause errors or incorrect data to be saved.	When more than one person works on the Incident Management and/or Change Management **Process Automation Rulesets** at the same time, errors may be reported and incorrect data may be saved in the rulesets.	
When an end user's email response to an incident contains multiple attachments, only one of the attachments is saved to the incident ticket.	When the **Email Monitor Project** processes a reply email to an incident that contains multiple attachments, only one of those attachments is saved to and available on the incident ticket. **Workaround:** See the *KNOWN ISSUE: Email monitor project only doesn't add all attachments when a reply email is processed containing multiple attachments* knowledge base article.	TECH204563

Table 1-7 Known issues *(continued)*

Issue	Description	Article link
When an end user submits an incident by email with an attachment, the attachment is not saved to the incident ticket that is created.	When the **Email Inbound Management Project** creates an incident from an email that contains an attachment, the attachment is not saved to and available on the incident ticket. **Workaround:** See the *After Creating an IM Ticket From an EM Ticket That Has an Attachment, the Attachment is not Transferred to the IM ticket* knowledge base article.	TECH206004
If you edit an incident ticket and use the **Clear existing assignments** option, all assignments may be removed from the incident when you save your changes.	If the owner of the incident edits the ticket and uses the **Clear existing assignments** option, all assignments (queue and owner) are removed from the incident when the changes are saved. The ticket is orphaned. **Workaround:** See the *Using the Edit Incident Process Action to Change Ticket Assignment Sometimes Causes Assignment to be Empty* knowledge base article.	TECH206100
After installing a Workflow rollup for ServiceDesk 7.5 MP1, you cannot use the ServiceDesk installer to repair or uninstall ServiceDesk.	After installing or upgrading to ServiceDesk 7.5 MP1, if you install a Workflow rollup, the ServiceDesk installer's **Install, Repair, Upgrade or Remove ServiceDesk** option fails to execute. The instructions that are provided in the **Prerequisite Not Met** dialog box message, do not fix the problem. **Workaround:** See the *ServiceDesk 7.5 Repair does not work after Workflow Rollup Installation* knowledge base article.	TECH206345
The Change Management **Process View** page's **Ticket Overview** section may only display dates instead of dates and times.	This issue only occurs when you upgrade from 7.5 to 7.5 MP1. In Change Management, you can specify times for **Needed By**, **Planned Start**, and **Planned Completion**. When you open the change request ticket's **Process View** page, the dates are displayed but not the times. **Workaround:** See the *Change Management ticket page only shows dates and not times for Planned Start and Planned Completion fields* knowledge base article.	TECH206735

| | **Table 1-7** | Known issues *(continued)* |

Issue	Description	Article link
If you use the **Resolve/Close Multiple Incidents** action to close an Incident ticket and its associate subtasks, the open subtasks may not get closed.	When you use the **Resolve/Close Multiple Incidents** action to close an Incident ticket and its subtasks, and you check **Skip the 'resolved' step for these tickets**, the open subtasks do not get closed.	
If you use the **Resolve/Close Multiple Incidents** action to resolve an Incident ticket, the **Resolution** SLA milestone may not get resolved.	When you use the **Resolve/Close Multiple Incidents** action to close an Incident ticket, and you check **Skip the 'resolved' step for these tickets**, the **Resolution** SLA milestone does not get resolved.	

Fixed issues

The following are the previous issues that were fixed in this release.

| | **Table 1-8** | Fixed issues |

Issue	Description
Pass-thru authentication when using HTTPS communication	Pass-thru authentication now works when using HTTPS communication to access the ServiceDesk 7.5 MP1 Servers. For more information, see the following knowledge base article: http://www.symantec.com/docs/TECH209860
Not all subtasks are closed on resolving incidents with multiple subtasks	An updated `SD.IncidentManagementSimple` installer and `SD.IncidentManagementSimple.Subtask` installer is available to resolve this issue. **Note:** This fix must be applied on ServiceDesk 7.5 MP1 Servers only. For more information, see the following knowledge base article: http://www.symantec.com/docs/TECH209213
You cannot use a rule to set an incident's SLA if the incident's **Priority** was set on the **Submit Incident (Advanced)** form.	Previously, if you set an incident's **Priority** on the **Submit Incident (Advanced)** form, you could not use a routing rule to set that incident's SLA.
Incident' SLA's are not set correctly.	Previously, the SLA on all incident tickets was set to **Normal**, rather than being set to an SLA based on their **ProcessPriority**.

| Table 1-8 | Fixed issues *(continued)* |

Issue	Description
Users without administration privileges cannot view the private comments that they added to tickets.	Previously users were unable view the private comments that they added to a ticket unless they had **admin privileges**. Now, users can only select a comment level that corresponds with their view permissions. For example if a user does not have permission to view private comments on a ticket, the user is unable to add a private comment.
You cannot use the **LocationRequiredToResolveIncident** option to set the location requirement for incident resolution.	Previously, you were unable to use the **LocationRequiredToResolveIncident** option in **ServiceDesk Settings** section, on the **Application Properties** page, to set the location requirement for incident resolution.
You cannot use SQL 2008 R2 Datacenter edition to build your SQL Server.	Previously, if you attempted to install ServiceDesk to SQL Server 2008 R2 Datacenter edition, the prerequisite check failed and you could not continue.
ServiceDesk installer does not set the Email SMTP server Master Setting.	Previously, the ServiceDesk installer did not set the settings to support the send email actions. For the **Send Email** action to work, you had to manually set the Master Setting for the SMTP server.
ServiceDesk installer does not consistently capture the underscores that are used as part of server or service account names.	Previously, the ServiceDesk installer did not consistently capture and render the underscores (_) when they were used in the names of servers or service accounts.
Running a repair on ServiceDesk reverts the **OnIncidentReceived** ruleset to its default state.	Previously, using the ServiceDesk installer to repair ServiceDesk reverted the **OnIncidentReceived** ruleset to its default or out-of-the-box state. The repair reinstalled the single default rule in the **OnIncidentReceived** ruleset.
The Change Request form's **Location Search** does not find locations and can cause an **application error**.	Previously, the Change Request form's **Location Search** functionality did not discover locations. The search functionality also populated the **Search the CMDB** field with your location search criteria.
	When you cleared the **Search the CMDB** field and tried to search the CMDB for the equipment and services that the change affected, an **application error** was thrown. Your change request was canceled.
Change Implementers cannot assign implementation tasks when using the **Manage Implementation Task** action.	Previously, members of the Change Implementer group received an error when they used **Manage Implementation Task** on the change request ticket's **Process View** page to assign implementation tasks.
	Task assignment does not grant permissions. Task assignment uses the actual user's permissions.

	Table 1-8	Fixed issues *(continued)*

Issue	Description
Change Managers cannot add a new CAB.	Previously, members of the Change Manager group received an error when they tried to add a new CAB. Change Manager group did not have the **AccountManagement.Access** permission.
Support users cannot post **Time Spent** working on an incident.	Previously, members of the support group did not have permissions to post **Time Spent** working on the incident in the **Start/Stop Process Timing** section on the **Process View** page.
Known Issue article can be populated with *"data name Problem.CreateDate is not valid because piece CreateDate does not exist. This typically happens if the data type changes structure"*.	Previously, when you resolved a problem by creating a known issue, the Known Issue article was created. However, the **Reported Problem** field in the Known Issue article was populated with *"data name Problem.CreateDate is not valid because piece CreateDate does not exist. This typically happens if the data type changes structure"*.
Process Manager portal crashes when an end-user searches for articles in the knowledge base.	Previously, an end user had default access to the **Knowledge Base** page in the Process Manager portal, but did not have rights to any article categories. When the end user used the **Knowledge Base** page's **Search Articles** feature, the Process Manager portal crashed. The end user was forced to restart the session.
You cannot use the **KB Migration Wizard** to migrate user created Helpdesk Solution 6.5 knowledge base articles.	Previously, the **Migrate KB Articles from Helpdesk 6.5** option did not import user-created Helpdesk Solution 6.5 knowledge base articles. The KB Migration Wizard was intended for importing Helpdesk Solution 6.5 knowledge base content that was added through the installation of a KBI solution add-on.
You cannot run the **Migrate KB Articles from Helpdesk 6.5** process.	Previously, using the **Migrate KB Articles from Helpdesk 6.5** option to migrate the Helpdesk Solution 6.5 knowledge base content failed. No knowledge base items were migrated and errors were thrown in the log.
You cannot run the **Migrate Helpdesk 6 Incidents** process.	Previously, using the **Migrate Helpdesk 6 Incidents** option threw an error *Invalid Portal Permissions*. The instructions that were displayed in the error message did not resolve the issue.
ServiceDesk may not correctly connect to the inbound mail server when the POP protocol is used.	Previously, in some email environments, ServiceDesk did not correctly connect to the inbound mail server using the POP protocol.
You cannot use the ServiceDesk installer to use SSL (https://) to configure the Process Manager database.	Previously, in the ServiceDesk Installer on the **Set Server Base URL** page, the **Use SSL (https://)** check box did not work correctly. It did not configure the Process Manager database using SSL (https://).

<div align="center">**Table 1-8** Fixed issues *(continued)*</div>

Issue	Description
Some variables in Incident and Change Management email templates may not work properly.	Previously, when you created an email template and added variables to it, some variables may not have populated correctly and may have contained incorrect information.
The **Task Response Url** variable in Incident Management email templates does not work.	Previously, when you added the **Task Response Url** to an Incident Management email template, an invalid URL to the incident ticket was created in the email.
Using the **Hold Management** Smart Task to place an Incident on hold, may result in an unworkable ticket.	Previously, if you used the **Hold Management Smart Task** to place a ticket on hold after you used the **Edit Incident**, **Process Action** to edit the ticket, the ticket became unworkable and unrecoverable.
Automation Rule "to send an email **To Task Assignees** on Task Creation" may not work properly.	Previously, to send an email **To Task Assignees** on task creation, you added the **TaskCreated** ruleset and configured a rule to send an email **To Task Assignees**. The rule for this ruleset did not send emails for subtask creation and did not consistently send emails for any other type of task creation. Now, you can use the **TaskAssignmentChanged** ruleset to send an email **To Task Assignees**. You do not use the **TaskCreated** ruleset; task assignees do not exist when the **TaskCreated** ruleset runs. The **TaskCreated** and the **TaskAssignmentChanged** rulesets run back to back. See the "Sending an email To Task Assignees" topic in the Symantec ServiceDesk 7.5 MP1 Implementation Guide.
The Automation Rule's **Any group satisfies** option does not produce expected results.	Previously, when you used the **Any group satisfies** option in a rule to include multiple groups, even if all groups were false, the rule executed the action(s).
The Automation Rule's **Any condition satisfies** option does not produce expected results.	Previously, when you used the **Any condition satisfies** option in a rule to include multiple conditions in the same group, even if all conditions were false, the rule executed the action(s).
The Automation Rule's Ruleset Action "to set the priority of an incident using the Impact/Urgency Matrix" fails.	Previously, when you created a rule to set the priority of an incident using the **Impact/Urgency Matrix**, the **Action** failed even if the condition was met.

Other things to know

The following are things to know about this release. If additional information about an issue is available, the issue has a corresponding Article link.

Table 1-9   Things to know

Component	Issue	Article link
The session timeout setting for Process Manager is changed from days to minutes.	The session timeout for Process Manager is changed from number of days to number of minutes. Additionally, the default session timeout is changed from 90 days to 90 minutes. After the configured session timeout in minutes, the user needs to log on to access Process Manager.	N/A
Helpdesk Solution migration support	ServiceDesk 7.5 MP1 is the last ServiceDesk release with Helpdesk Solution 6.x migration support. See the *About migrating data from Helpdesk Solution 6.x* topic.	See the Symantec™ ServiceDesk 7.5 MP1 Implementation Guide.
Symantec™ ServiceDesk Solution 7.5 MP1 may not appear in the **Available Products** list in the Symantec Installation Manager (SIM).	The **Symantec™ ServiceDesk Solution 7.5 MP1** may not appear in the **Available Products** list because the Symantec Installation Manager (SIM) is pointed to a previous release's or a Beta release's product listing (PL). **To point SIM to the current PL:** 1 Open SIM. 2 On the **Install New Products** page, click **Cancel** to change the product listing (PL). 3 In the **Symantec Installation Manager** dialog box, click **Yes**. 4 On the **Install Products** page, click **Settings**. 5 On the **Settings** page, click **Change product listing**. 6 On the **Manage Product Listings** page, select the **(Default)** product listing.	
Incident Management	Incident Management requires setup and is not fully functional out-of-the-box. See the *About configuring ServiceDesk* topic.	See the Symantec™ ServiceDesk 7.5 MP1 Implementation Guide or the Symantec™ ServiceDesk 7.5 MP1 User Guide.
Change Management	Change Management requires setup and is not fully functional out-of-the-box. See the *About configuring ServiceDesk* topic.	See the Symantec™ ServiceDesk 7.5 MP1 Implementation Guide or the Symantec™ ServiceDesk 7.5 MP1 User Guide.

Table 1-9 Things to know *(continued)*

Component	Issue	Article link
Default Workflow reports do not accurately display ServiceDesk data.	The default **Open Process…** reports in **Process Reports** and **Process Admin Reports** require modification to filter out closed ServiceDesk tickets. For an example of how to modify a report, see the *My Open Tickets report in ServiceDesk 7.1 displays Closed and Resolved tickets* knowledge base article.	TECH1598786
Send Email link on the Incident Management **Process View** page	The **Send Email** link on the Incident Management's **Process View** pages is hidden until an email template is created. See the *Creating email templates for Incident Management* topic.	See the Symantec™ ServiceDesk 7.5 MP1 User Guide.
Send Email link on the Change Management **Process View** page	The **Send Email** link on the Change Management's **Process View** page is hidden until an email template is created. See the *Creating email templates for Change Management* topic.	See the Symantec™ ServiceDesk 7.5 MP1 User Guide.
Improved security controls on the Workflow Server	Symantec has improved security controls on the Workflow Server. The improved security can potentially block the ability to deploy from a local Workflow Designer to a remote Workflow Server. If you cannot deploy to a remote Workflow Server, change the following setting on the remote Workflow Server before attempting to deploy. **To allow remote connections:** ■ On the Workflow Server, right-click on the **Task Tray Tool** and click **Settings**. ■ In the **Workflow Server** section next to **Workflow Server Configuration**, click the ellipsis. ■ In the **General** section, check **Allow Remote Connections**. Please note that the Symantec security best practice is to revert this setting after you are finished deploying. For more information on Symantec security best practices, see the article *ServiceDesk/Workflow General Security Best Practices*.	www.symantec.com/docs/DOC6160

Table 1-9   Things to know *(continued)*

Component	Issue	Article link
IT Analytics 7.1 SP2	ServiceDesk 7.5 MP1 is not compatible with IT Analytics 7.1 SP2. If you want to use IT Analytics 7.1 SP2 with ServiceDesk 7.5 MP1, a ServiceDesk Pack 7.5 for IT Analytics 7.1 SP2 is available. For more information, see the *ServiceDesk Pack for Altiris™ IT Analytics 7.1 SP2 from Symantec™ User Guide (ServiceDesk 7.5)*.	www.symantec.com/docs/DOC5639
ServiceDesk Solution Software User Guide	The *ServiceDesk Solution Software User Guide* has been deprecated. The instructions that were in this guide are now in the *ServiceDesk Implementation Guide* and *ServiceDesk User Guide*.	See the Symantec™ ServiceDesk 7.5 MP1 Implementation Guide or the Symantec™ ServiceDesk 7.5 MP1 User Guide.
ServiceDesk Portal User Guide	The *ServiceDesk Portal User Guide* has been deprecated. The instructions that were in this guide are now in the *ServiceDesk User Guide*.	See the Symantec™ ServiceDesk 7.5 MP1 User Guide.
ServiceDesk Customization Guide	The *ServiceDesk Customization Guide* has been deprecated. Because of the changes to ServiceDesk, most of the customizations can be accomplished in the Process Manager portal. Some advance customizations can still be accomplished by editing the workflow processes. See the *Configuring ServiceDesk* and *Advanced ServiceDesk customizations* topics.	See the Symantec™ ServiceDesk 7.5 MP1 Implementation Guide or the Symantec™ ServiceDesk 7.5 MP1 User Guide.

Documentation that is installed

Table 1-10   Documentation that is included into the product installation

Document	Description	Location
Help	Information about how to use this product. 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.
User Guide	Information about how to use this product. This information is available in PDF format.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. The Documentation Library provides a link to the PDF User Guide on the Symantec support Web site. ■ 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**.

Other information

Table 1-11   Information resources that you can use to get more information

Document	Description	Location
Symantec Management Platform User Guide	Information about using the Symantec Management Platform.	Symantec Management Platform Documentation page

Table 1-11 Information resources that you can use to get more information
(continued)

Document	Description	Location
Symantec Management Platform Release Notes	Information about new features and important issues in the Symantec Management Platform.	Symantec Management Platform Documentation page
Symantec Management Platform Installation Guide	Information about using Symantec Installation Manager to install the Symantec Management Platform products.	http://www.symantec.com/docs/DOC4798
Knowledge base	Articles, incidents, and issues about this product.	SymWISE support page
Symantec Connect	An online magazine that contains best practices, tips, tricks, and articles for users of this product.	Symantec Connect page