Symantec™ IT Management Suite 8.1 RU7 powered by Altiris™ technology Release Notes

Symantec™ IT Management Suite 8.1 RU7 powered by Altiris™ technology Release Notes

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Symantec IT Management Suite 8.1 RU7

This document includes the following topics:

About IT Management Suite

IT Management Suite is a tool for managing corporate IT assets such as desktop computers, laptop computers and servers that have Windows, UNIX, Linux, or Mac operating systems.

IT Management Suite is a collection of solutions and components that run on the Symantec Management Platform.

What's new in this release

In IT Management Suite 8.1 RU7, the following new features are introduced:

Table 1-1 New features

Feature	Description
Support for Windows 10 April 2018 Update.	Symantec Management Agent and solution plug-ins can be installed on Windows 10 April 2018 Update client computers. For the list of supported solutions and limitations refer to the following knowledge base article: http://www.symantec.com/docs/HOWTO128230
ITMS binaries for Mac are converted to 64-bit.	The Symantec Management Agent for Mac and all plug-ins for Mac are converted to 64-bit binaries.
Extended health information for the Symantec Endpoint Protection clients on Mac client computers.	Inventory Solution provides extended information for the Symantec Endpoint Protection 14 clients (SEP agents) and general information for SEP 14.2 agents that are installed on managed Mac computers in your environment. The extended SEP 14 agent health information for a selected client computer additionally includes inventory data that is related to infection status, Antivirus status, and last Antivirus scan date. The general SEP 14.2 agent health information includes the following items: ■ SEP client name ■ SEP client version and number of devices that have this version installed ■ Number of devices that do not have SEP client installed ■ Number of devices where inventory is not yet gathered To gather this information, ensure that the **SEP Agent** data class is enabled on an inventory policy or task page, at **Advanced Options > Data Classes > Software > Common**.
Ability to deliver the Symantec Endpoint Protection clients (SEP agents) to client computers.	Software Management Solution provides the predefined **Symantec Endpoint Protection Delivery** policy. The policy delivers a SEP installation package to Windows and Mac client computers, installs SEP agent, and makes sure it remains installed. The policy also upgrades the existing SEP agent if necessary. The **Conflicting SEP Delivery Policies** report presents the enabled **Symantec Endpoint Protection Delivery** policies that are targeted to the same computers. Running such policies may result in double installation of the SEP agent on the computers. The report lets you detect conflicting policies and resolve them to ensure that only one instance of SEP agent is installed on the computers. You can view this report in the Symantec Management Console, on the **Reports** menu, at **All Reports > Software > Delivery**. For more information about SEP management tasks, see the *Managing Symantec Endpoint Protection with IT Management Suite Whitepaper* at the following URL: https://www.symantec.com/docs/DOC11067

Table 1-1 New features *(continued)*

Feature	Description
Simplified software deployment application programming interface (API).	The Administrator Software Development Kit (ASDK) contains the new API that simplifies deployment of installable packages (i.e., self installable `.exe` files, `.msi` packages, `.rpm` packages). With just one method call, this API lets you import a package, create software component resource with the package, and then generate an installation policy for this resource. For more information, refer to the following knowledge base article: http://www.symantec.com/docs/DOC11040
Enhancements and changes of **View Update Notifications** privilege.	In previous versions of ITMS, the **View Update Notifications** privilege allowed you to configure if the update notification icon is displayed in the Symantec Management Console. Starting from this release, the privilege is renamed to **View Console Notifications** and lets you configure if the following notifications are displayed in the Symantec Management Console: ■ ITMS update notifications ■ Certificate expiration notifications
Certificate expiration notification.	The notification at upper right corner of the Symantec Management Console now displays notifications for certificates that will expire in 60 days. By default, these notifications are displayed only to **Administrator** role. The **View Console Notifications** privilege lets you configure if the certificate expiration notification is displayed in the Symantec Management Console.
Any script task return code is treated as success.	For a script task, **The task is succeeded if its return code is** option lets you specify custom success return codes. In addition to adding custom values, you can now select the option **Any** to treat all script task return codes as successful.
Support for iPXE	From this release onwards, Deployment Solution supports creating pre-boot configurations that can be deployed over HTTP. TECH250831
Changes in Workflow Solution	Password hint field is removed from the modify User Account page.

System requirements and supported platforms

Before you install Symantec IT Management Suite 8.1 RU7, read the section Hardware recommendation in the *IT Management Suite Planning for Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC9470

For information about the supported operating systems in Symantec Management Platform and the Symantec IT Management Suite solutions, see the knowledge base article at the following URL:

http://www.symantec.com/docs/HOWTO9965

General installation and upgrade information

The installation of IT Management Suite (ITMS) 8.1 RU7 involves installation of Symantec Management Platform (SMP) 8.1 RU7 and solutions using Symantec Installation Manager.

For more information on how to install and configure the product, see the *Installing the IT Management Suite solutions* chapter in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

Warning: Before you run any repair or reconfigure Deployment Solution from Symantec Installation Manager, read the following article:

TECH250873.

Upgrade to IT Management Suite 8.1 RU7

After you install this release update (8.1 RU7), you cannot uninstall it or roll back to the previous version of ITMS. After you install ITMS 8.1 RU7 for Symantec Management Platform, you need to enable upgrade policies for all plug-ins and the Symantec Management Agent to upgrade the client computers.

To avoid issues with cross-dependencies, Symantec recommends to install all available RU7 components at once.

Note: To upgrade to the latest release update, log on to the Notification Server computer with the SMP application identity credentials.

In ITMS 8.1 RU7, Symantec Installation Manager (SIM) automatically creates a registry backup in the support folder before starting the installation, upgrade, or release update installation of SIM and ITMS solutions. The registry backup is available at the following location:

`<installation_path>\Altiris\Symantec Installation Manager\Support`

If you encounter any errors because of missing registry entries or corrupted registry file, you can do one of the following:

- Restore the previous registry entries, and then run the installation or upgrade. To restore the previous registry entries, navigate to the registry backup, and then double-click the `AIMRoot.reg` file.
- Uninstall a solution, and then reinstall it, so that the registry entries are recreated. When you encounter the same error, repair the solution using SIM.
  For more information, see the following knowledge base article:
  http://www.symantec.com/docs/TECH183086

For more information about creating a support package, see the following knowledge base article:

http://www.symantec.com/docs/HOWTO93142

Upgrading Symantec Management Agent, site servers, and solution level plug-ins

After you upgrade IT Management Suite from version 8.1 to this release update, upgrade the Symantec Management Agent, the site servers, and the solution plug-ins.

Table 1-2 Process to upgrade Symantec Management Agent, site servers, and solution plug-ins

Step	Action	Description
Step 1	Upgrade the Symantec Management Agent on site servers.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the policies that upgrade the Symantec Management Agent on site servers.
Step 2	Upgrade the site servers.	In the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for various site server plug-ins. To upgrade a remote task server, in the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings > Notification Server > Task Service > Advanced**, and then locate and turn on the upgrade policies for the remote task servers. To upgrade a remote package server, in the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings > Notification Server > Package Service > Advanced > Windows**, and then locate and turn on the **Windows Package Server Agent Upgrade** policy.

Table 1-2 Process to upgrade Symantec Management Agent, site servers, and solution plug-ins *(continued)*

Step	Action	Description
Step 3	Upgrade the Symantec Management Agent on client computers.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the policies that upgrade the Symantec Management Agent on client computers.
Step 4	Upgrade solution-specific agents and plug-ins.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the plug-in upgrade policies. To upgrade the solution-specific plug-ins to the latest version, do the following: ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, under **Symantec Management Agent**, locate and turn on the upgrade policies for the Symantec Management Agent. ■ In the Symantec Management Console, on the **Settings** menu, click **All Settings**. In the left pane, expand **Notification Server > Site Server Settings**, and then locate and turn on the upgrade policies for the site server plug-ins. ■ In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. Then, in the left pane, locate and turn on the plug-in upgrade policies.

Symantec recommends that you configure a schedule for the upgrade policies. The default **Run once ASAP** option may not trigger the policy if this is not the first time you perform an upgrade. To speed up the upgrade process, consider temporarily changing the **Download new configuration every** setting on the **Targeted Agent Settings** page to a lower value.

If the upgrade policy is set to **Run once ASAP**, the policy is rolled out just once.

You can also clone the upgrade policies instead of creating additional schedules.

For more information on the post-upgrade tasks, see the chapter *Performing post-upgrade tasks* in the *IT Management Suite Installation and Upgrade Guide* at the following URL:

http://www.symantec.com/docs/DOC9500

Post-upgrade versions of Symantec Management Agent and solution plug-ins

The Symantec Management Agent and its plug-in versions after you upgrade to ITMS 8.1 RU7 are as follows:

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU7

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Management Agent	8.1.6243	8.1.6216
Altiris Client Task Agent	8.1.6243	8.1.6216
Altiris Client Task Server Agent	8.1.6236	N/A
Altiris Pluggable Protocols Architecture Agent	8.1.6029	N/A
Inventory Agent	8.1.6288	8.1.6288
Application Metering Agent	8.1.5636	8.1.6288 (Mac only)
Server Inventory Agent	8.1.5636	8.1.6101
Inventory Rule Agent	8.1.6243	8.1.6216
Monitor Plug-in	8.1.6039	8.1.6039
Package Server	8.1.5844	8.1.6216
Power Scheme Task Plug-in	8.1.4504	N/A
Software Update Plug-in	8.1.5620	8.1.5836
Software Management Framework Agent	8.1.6243	8.1.6216
Software Management Solution Agent	8.1.6235	8.1.6235
Virtual Machine Management Task Handler	8.1.6215	N/A
Deployment Task Server Handler	8.1.5622	N/A
Deployment Package Server	8.1.5622	N/A
Deployment Plug-in for Windows (x64/x86)	8.1.6247	N/A
Deployment Plug-in for Linux (x64)	N/A	8.1.4536
Deployment Plug-in for Linux (x86)	N/A	8.1.4536
Deployment Plug-in for Mac	N/A	8.1.4536
Deployment NBS plug-in	8.1.6247	N/A
Symantec Workspace Streaming Agent	7.6.0.269	N/A
Symantec Workspace Virtualization Agent	7.6.269	N/A

Table 1-3 Symantec Management Agent and plug-in versions after upgrading to IT Management Suite 8.1 RU7 *(continued)*

Agent or plug-in	Windows	UNIX/Linux/Mac
Symantec Workspace Virtual Composer	7.6.0.269	N/A

Performing post installation tasks for Deployment Solution

The following table lists the upgrade scenarios for which you must recreate the automation folders after you install the ITMS 8.1 RU7:

Table 1-4 Post installation tasks for Deployment Solution

Upgrade	Windows automation folder	Mac automation volume	Linux automation folder
Upgrade from 8.1 to 8.1 RU7	Yes	Yes	Yes
Upgrade from 8.1 RU6 to 8.1 RU7	Yes	No	Yes

Post installation tasks for Deployment Solution

- Recreate the automation folders.
- Deploy automation folders on client computers.

Note: Symantec recommends that you clear the Internet browser cache before running deployment tasks.

To recreate the automation folders

1. In the Symantec Management Console, on the **Settings** menu, click **Deployment > Manage Preboot Configurations**.
2. On the **Manage Preboot Configurations** page, in the preboot configurations list, select the configuration that you want to recreate and click **Recreate Preboot Environment**.

   For Mac, you must recreate all the NetBoot images and the automation folders and create new preboot configurations.

   Symantec recommends that you wait for at least half an hour before running any deployment tasks. To see if the automation folder is updated, check the timestamp for the automation folders that are created at the following locations:

- PEInstall_x86

  ```
  <install_dir>\Notification
  Server\NSCap\bin\Win32\X86\Deployment\Automation\PEInstall_X86
  ```

- PEInstall_X64

  ```
  <install_dir>\Notification
  Server\NSCap\bin\Win64\X64\Deployment\Automation\PEInstall_x64
  ```

- LinInstall

  ```
  <install_dir>\Notification
  Server\NSCap\bin\UNIX\Deployment\Linux\x86\Automation\LinInstall_x86
  ```

To verify if the automation folder has been recreated, in the task manager, check if the Bootwiz.exe application has completed recreating the preboot configuration.

After recreating the automation folders, run the following tasks from the Task Scheduler to update the packages on Notification Server:

- NS.Delta Resource Membership Update
- NS.Package Distribution Point Update Schedule
- NS.Package Refresh

To deploy the automation folders on the Windows client computers

- Run the following automation folder upgrade policies:
  - **Deployment Automation Folder for Windows (x64) - Upgrade**
  - **Deployment Automation Folder for Windows (x86) - Upgrade**

To deploy the automation folders on the Linux client computers

1. Run the **Deployment Automation Folder for Linux-Uninstall** automation folder uninstall policy.
2. Run the **Deployment Automation Folder for Linux-Install** automation folder install policy.

To deploy the automation folders on the Linux or Mac client computers

1. Run the following automation folder uninstall policies:
   - **Deployment Automation Folder for Linux-Uninstall**
   - **Deployment Automation Folder for Mac-Uninstall**
     After you enable the **Deployment Automation folder for Mac-Uninstall** policy, you must manually delete the DSAutomation partition that is present in the unmounted and unallocated state.
     If you do not want to run the uninstall policy to uninstall the automation folder from the client computer, you must manually erase the disk and the volume of the client

computer. If you manually erase the disk and the volume of the client computer, ensure that you clean the Non-volatilerandom-accessmemory (NVRAM) of the client computer. For information on how to clean the NVRAM of a client computer, see the following article:
https://support.apple.com/en-us/HT204063

2 Run the following automation folder installation policies:

- **Deployment Automation Folder for Linux-Install**
- **Deployment Automation Folder for Mac-Install**

Fixed issues

IT Management Suite 8.1 RU7 contains fixed issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Fixed Issues" on page 13.
- Deployment Solution
  See "Deployment Solution Fixed Issues" on page 14.
- Inventory Solution
  See "Inventory Solution Fixed Issues" on page 15.
- ITMS Management Views
  See "ITMS Management Views Fixed Issues" on page 15.
- Patch Management Solution
  See "Patch Management Solution Fixed Issues" on page 16.
- Software Management Solution
  See "Software Management Solution Fixed Issues" on page 16.
- Workflow Solution
  See "Workflow Solution Fixed Issues" on page 17.

Symantec Management Platform Fixed Issues

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

This release contains fixed issues for the following components:

- Notification Server
  See Table 1-5 on page 14.
- Task Server
  See Table 1-6 on page 14.

- UNIX/Linux/Mac
  See Table 1-7 on page 14.

Table 1-5 Fixed issues for Notification Server

Issue	Article link
Inv_Audit data is being deleted before the time range that is defined in the **coresettings.config**.	N/A
Automation policy that uses the built-in **Set Asset Status** task does not display all required options in the **Assets Data Source** drop-down list.	N/A

Table 1-6 Fixed issues for Task Server

Issue	Article link
Boot To production task stops the job and does not continue to the next step.	TECH250324
If two users belong to the same role and one user creates a target then the other user is not able to use this target for launching a **Power Control**, **Service Control**, and **Run Script** task.	N/A

Table 1-7 Fixed issues for UNIX/Linux/Mac

Issue	Article link
Aex-pluginmanager causes consistent high CPU usage on RHEL servers.	N/A

Deployment Solution Fixed Issues

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

Table 1-8 Fixed issues for Deployment Solution

Issue	Article link
For WinPE 10 , the **Partition Disk** task does not work properly and displays an error when you run the `chkdsk` command.	N/A
Predefined Computers lists computers from only the Basic Inventory.	N/A
The delay interval that Deployment Solution plug-in uses to validate package readiness is high.	N/A
DeployAnywhere fails to run as no system disk is involved in the imaging operation during the **Deploy Image** task.	N/A

Table 1-8 Fixed issues for Deployment Solution *(continued)*

Issue	Article link
Images the are imported on the site server with Resource Import Tool shows up as Software Library in disk images. Following error is displayed: `The system cannot find the file specified.`	N/A

Inventory Solution Fixed Issues

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

Table 1-9 Fixed issues for Inventory Solution

Issue	Article link
The status of an unmanaged Symantec Endpoint Protection (SEP) agent is incorrectly reported on the **SEP Agent Health** page in the **Computer Details** flipbook. After the inventory data is gathered for the SEP agent that is not centrally managed by a management server, the **SEP Manager Server** status is displayed as **No data available**.	N/A
If you open the **Agentless Inventory Home** page that contains an agentless inventory task scheduled to run in the past without repeat, an error is displayed on the page.	N/A
Two scroll bars appear on application metering policy pages, under **Policy Rules/Actions**.	N/A
Information about the hard disk drive serial number is not reported if you run inventory scan on the NVMe drives that have non-alphanumeric characters for the serial number.	N/A
After the software is uninstalled from a UNIX, Linux or Mac client computer, its software inventory data remains in the inventory reports.	N/A

ITMS Management Views Fixed Issues

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

Table 1-10 Fixed issues for ITMS Management Views

Issue	Article link
When you import a software resource with a custom .bmp format icon to the Notification Server using the Software Replicator utility, the custom icon is not displayed on the **Software** view page.	N/A
When you select a client computer on the **Computers** view page, the Computer summary pane (right) does not display any data and remains empty if the Inventory Solution is not installed.	N/A

Patch Management Solution Fixed Issues

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

Table 1-11 Fixed issues for Patch Management Solution

Issue	Article link
When you run the **Check Software Update Package Integrity** task with the registry key **DeleteFilesObsolete = 1**, non-obsolete update package files are also deleted.	N/A
The x86 software update plug-in may install on the x64 computers that are predefined by Deployment solution because the target **All Computers without Software Update Plug-in Installed** does not check for Symantec Management Agent on the computers.	N/A
When you run the report **Windows Software Update Delivery - Details**, right-click a bulletin, and then click **View Incomplete Installations**, the **Status** column in the report is **Undefined** even if the status data is available.	N/A
The software update plug-in installation policy has the default target **All Computers without Software Update Plug-in Installed** that includes Ubuntu client computers.	N/A

Software Management Solution Fixed Issues

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

Table 1-12 Fixed issues for Software Management Solution

Issue	Article link
In the existing Managed Software Delivery policies, some referenced components are missing. Referenced packages and command lines are also missing in the policy UI.	N/A

Table 1-12 Fixed issues for Software Management Solution *(continued)*

Issue	Article link
You cannot schedule software or package delivery tasks on the computers that are predefined by Deployment solution but do not have the Software Management Solution plug-in installed.	N/A
The rule **File Resources for executable files** replicates executable files from the child Notification Server computer to the parent Notification Server computer but the **Clean up File Resource Task** removes some of the replicated files.	N/A
Notification Server receives numerous failed task status events from Managed Software Delivery policies.	N/A
When you have two Notification Servers that share the same UNC as the Software Library, and on the second server, you edit the software resource that is imported from the first server, the software folder with the package that corresponds to the resource is deleted from the UNC directory.	N/A
When you publish a software component or a Managed Delivery Policy with this component to the Software Portal for a user, the user sees two equal publications in the Software Portal.	N/A
Enhanced user interface of the Software Portal does not open for some users.	N/A
Enhanced user interface of the Software Portal does not list the software categories in the alphabetical order.	N/A
When a user opens enhanced user interface of the Software Portal, the portal displays the full list of the software that is available to the user instead of only recommended software.	N/A

Workflow Solution Fixed Issues

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

Table 1-13 Fixed issues for Workflow Solution

Issue	Article link
Date Time Picker component throws an exception when you enter invalid date values.	N/A
The date and time on the Process History Web Parts of the Process View Page a.	N/A
If you manually set timezone to Central America, the settings are saved as Central America (US and Canada) time zone.	N/A

Table 1-13 Fixed issues for Workflow Solution *(continued)*

Issue	Article link
For Milestone by Process Priority' Rule Action does not work with extended Incident data type.	TECH248643
User Search fails to display list of users based on Last Name.	N/A
Explicit Permission for KB Articles generates following error when you access the Article category: `User doesn't have access to view this article.`	N/A
The '<' and '>' do not appear in the comment section of the Process View Page.	N/A
The Workflow Component **Send Email with SSL over SMTP** does not work.	N/A
The **Get Computer Info component** is not present in 8.1 RU5 onwards.	N/A
An error is displayed if you try to save an SMP resource with multi-row data class after removing the rows.	N/A
The Value Datatypes (Number (integer) and Number(Decimal)) that are configured as input parameters are not accepted as default values configured in Debug to published web services.	N/A
ServiceDesk Process View Pages do not refresh automatically after you make changes.	N/A
Datetime.Kind errors appear in 3 separate places: ■ `Audithistory Errors` ■ `Reporting Gateway` ■ `LogicBase.Ensemble.Workflow.Reporting.Gateways.ProcessReportStorageGateway.Pos tUserActivity`	

Known Issues

IT Management Suite 8.1 RU7 contains known issues for the following solutions and components:

- Symantec Management Platform
  See "Symantec Management Platform Known Issues" on page 19.
- Deployment Solution
  See "Deployment Solution Known Issues" on page 19.
- Inventory Solution
  See "Inventory Solution Known Issues" on page 20.

- Patch Management Solution
  See "Patch Management Solution Known Issues" on page 20.
- Software Management Solution
  See "Software Management Solution Known Issues" on page 21.

Symantec Management Platform Known Issues

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

The known issues are listed for the following components:

- Network Discovery
  See Table 1-14 on page 19.

Table 1-14 Known issues for Network Discovery

Issue	Article link
After Network Discovery, an incorrect operating system is displayed in Resource Manager for a computer that has Windows Server Core, version 1803 or 1709 installed.	N/A

Deployment Solution Known Issues

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

Table 1-15 Known issues for Deployment Solution

Issue	Article Link
For SUSE 12 SP3 Desktop edition, the **Scripted OS Install** task fails and displays the following error: `Packages could not be found..` Workaround: Click **OK** in the dialog box that appears on the client computer.	N/A
The **Install Windows OS** task fails if you use the default setting for the configuration option. Workaround: Select another option from the drop-down list for the **Configuration** option and then select the **Use inventory data to reconfigure computer**.	N/A
For WinPE 10, the **Partition Disk** task is unable to create required partitions.	N/A

Table 1-15 Known issues for Deployment Solution *(continued)*

Issue	Article Link
Automation folder is no longer functional after you deploy a BIOS-based image to a UEFI computer.	N/A
Sometimes, package upload from Symantec Management Console fails for OS Files and Drivers upload.	N/A
For macOS Sierra 10.13 NetInstall (SOI) is not currently supported.	N/A
For macOS Sierra 10.13 sometimes the **Deploy Image** task of Apple file system containers fails with following error: Could not mark APFS container as new/unique.	N/A
Deploy Image task fails to deploy an image of a computer with RHEL 7.2 operating system and XFS file system.	N/A
For macOS Sierra 10.13 clients, you cannot create image of volumes of Apple File System containers.	N/A

Inventory Solution Known Issues

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

Table 1-16 Known issues for Inventory Solution

Issue	Article link
The **Control SEP Service State** task fails to start the Symantec Endpoint Protection service and the return code 4 is reported when the startup type of the service on a client computer is set to **Disabled**.	N/A

Patch Management Solution Known Issues

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

Table 1-17 Known issues for Patch Management Solution

Issue	Article link

After upgrade of Patch Management Solution for Mac, the following tasks fail to run on the Mac client computers that still have the older version of Symantec Management Agent:
■ Run System Assessment Scan on Mac Computers
■ Install All Available Updates
■ Install All Recommended Updates
■ Install All Updates Not Requiring Restart
■ Install All Updates Requiring Restart
The error details are as follows:
`Failure message: command finished with error code: (133) unknown error.`
`Package download status: package downloaded successfully, but failed to launch the program.`
Workaround: Upgrade Symantec Management Agent to fix the issue.
	N/A

Software Management Solution Known Issues

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

Table 1-18 Known issues for Software Management Solution

Issue	Article link
When on the parent Notification Server computer, you right-click the **Symantec Endpoint Protection Delivery** policy, and then click **Replicate Now**, the Symantec Endpoint Protection (SEP) release that is associated with the policy is also replicated. However, the replicated SEP release is not listed on the child Notification Server computer, at **Manage > Software > Deliverable Software > SEP Releases**. Workaround: You can perform differential or complete replication to solve the issue.	N/A

Table 1-18 Known issues for Software Management Solution *(continued)*

Issue	Article link
You can use a **Symantec Endpoint Protection Delivery** policy to deliver Symantec Endpoint Protection client (SEP agent) to Windows and Mac client computers. However, SEP delivery supports only the following SEP installation package files: ■ Non-DMG based ZIP files for Mac ■ EXE files for Windows ■ EXE self-extracting (SFX) archive files for Windows Workaround: You can use Managed Software Delivery policies to deliver SEP agent that is installed with other types of installation package files.	N/A
The Software Portal user can configure a user profile so that the **Installation Succeeded** notification appears when the application that the user has requested in the Software Portal is installed on the user's device. However, on Windows devices, the notification may be displayed for too short time (less than 30 seconds), and the user may overlook it.	N/A
The non-working link to the Software Portal appears in the Symantec Management Agent context menu on a Mac computer that has no access to the Software Portal if you enable the **Software Portal Client Access Policy**, check the corresponding option, and then target the policy to the Mac computer without Software Management plug-in installed.	N/A
Enhanced user interface of the Software Portal (enhanced UI) is not supported in Safari 8 that is included with Mac OS X 10.10. Workaround: You can open the enhanced UI after you upgrade to Mac OS X 10.10.5 and Safari 10.	N/A
Even if you apply the legacy UI to the Software Portal, the enhanced UI opens on client computers with Cloud-enabled Management enabled.	N/A

Where to get more information

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

Table 1-19 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: https://www.symantec.com/products/products-az Open your product's support page, and then under **Common Topics**, click **Release Notes**.
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: https://www.symantec.com/products/products-az 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: ■ Click the page and then press the F1 key. ■ Use 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 1-20 Symantec product information resources

Resource	Description	Location
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	Knowledge Base

Table 1-20 Symantec product information resources *(continued)*

Resource	Description	Location
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: ■ Deployment and Imaging ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming