Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Release Notes

Symantec

Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Release Notes

Documentation version: 2.0

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 website at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

support.symantec.com

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_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Release Notes

This document includes the following topics:

About Symantec Data Center Security: Server Advanced

Symantec Data Center Security: Server Advanced (Data Center Security: Server Advanced) provides a policy-based approach to endpoint security and compliance. The intrusion prevention and intrusion detection features of Data Center Security: Server Advanced operate across a broad range of platforms and applications.

Table 1-1 Data Center Security: Server Advanced capabilities

Security and protection	Compliance
■ Real-time proactive enforcement ■ Intrusion and malware prevention ■ System hardening ■ Application control ■ Privileged user access control ■ Vulnerability and patch mitigation ■ Does not use signatures or require continual updates to content	■ Real-time monitoring and auditing ■ Host intrusion detection ■ File integrity monitoring ■ Configuration monitoring ■ Tracking and monitoring of user access ■ Logging and event reporting

The major benefits of Data Center Security: Server Advanced are as follows:

- Reduces emergency patching and minimizes patch-related downtime and IT expenses through proactive protection that does not require continuous updates.
- Reduces incidents and remediation costs with continuous security. Once the agent has a policy, it enforces the policy even when the computer is not connected to the corporate network. And even if a computer is unable to obtain the latest patches in a timely fashion, Data Center Security: Server Advanced continues to block attacks so that the computer is always protected.
- Provides visibility and control over the security posture of business-critical enterprise assets.
- Uses predefined compliance and hardening policies to provide efficient security management, reporting, alerting, and auditing of activities. Also provides compensating controls for compliance failures.

For more information, see the *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced Overview Guide* that is available at: http://www.symantec.com/docs/DOC9281.

What's new in this release

The Symantec Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 introduces the following new features:

Table 1-2 New features

Feature	Description
Support for Dockers	Data Center Security: Server Advanced provides detection and prevention capabilities for Docker using the Unix detection and Prevention policies. From Unified Management Console, you can view the docker containers, their status, and relevant monitoring and hardening events.
Policies page in the Unified Management Console	The Unified Management Console 6.7 contains a Policies page that lets you view the available Data Center Security: Server Advanced policies. The page also lets you search for a specific policy, view details of the policy, and assign the policy to a security group
Policy Search in the Java console	The Policy Search lets you search your Data Center Security: Server Advanced policies through the Java console. The console displays the search result in the Policy Summary page. You can right-click a policy to edit, export, rename, delete, or view the properties of the policy.
Unified Management Console integration with Management Server	Unified Management Console appliance is now integrated with the Management Server. So, there is no need of the virtual infrastructure to deploy Unified Management Console. When you install the Management Server, the Unified Management Console is also deployed on the same computer. Unified Management Console Database is created on the same Microsoft SQL Server instance that you select while installing the Management Server. Management Server gets registered with Unified Management Console as part of the installation. If you are upgrading to Unified Management Console 6.7, then you can migrate all the data and settings of the previous Unified Management Console to the Unified Management Console 6.7.

For the list of enhancements in this release, See “Enhancements in this release ” on page 8.

Enhancements in this release

To see the list of enhancements in:

- Data Center Security: Server Advanced, see Table 1-3
- Unified Management Console, see Table 1-4

The following table lists the enhancements in Data Center Security: Server Advanced 6.7.

Table 1-3 Enhancements in Data Center Security: Server Advanced

Feature	Description
Assigning a policy to a security group	The **Server > Policies** page of the Unified Management Console lets you select a policy and apply the selected policy to an existing or a new Data Center Security: Server Advanced security group. For more information, see the online help.
Updating an existing sandbox using automated application isolation policy creation	You can use the automated application isolation policy creation to update an existing custom sandbox. You can create the rules based on application profiling or policy violation events during a specific time frame. For more information, see online help.
Updates to the Management Server installation wizard	The Management Server installer is divided into two phases; installation and configuration. For more information, see online help.

The following table lists the enhancements in Unified Management Console 6.7.

Table 1-4 Enhancements in Unified Management Console

Feature	Description
Automated data migration	Unified Management Console 6.7 provides an option to migrate all the data and settings from an existing Unified Management Console appliance automatically during the installation process.
FQDN support	During the installation process, Unified Management Console 6.7 provides you an option to create certificates using Fully Qualified Domain Name (FQDN). If you choose the option, the Management Server is registered with the Unified Management Console using FQDN and the certificates are also created using FQDN. Before opting to use FQDN, ensure that the FQDN is resolvable in the network.

New platform support

Data Center Security: Server Advanced adds support on the following platforms:

- Docker containers
- Oracle Linux UEK R4
- IDS support is added for AWS Linux
- IPS support is added for Solaris 11

- SUSE Linux Enterprise Server 12 SP1

Data Center Security: Server adds support on the following platforms:

- VMware NSX 6.1.7 and 6.2.2
- VMware vCNS 5.5.4.3

System requirements

To know the system requirements for:

- Symantec Data Center Security: Server Advanced 6.7, see System requirements for Data Center Security: Server Advanced.
- Symantec Data Center Security: Server 6.7, see System requirements for Data Center Security: Server.

Installing and upgrading

Depending on the type of installation, perform the following tasks.

- Installing Symantec Data Center Security: Server Advanced
- Installing Symantec Data Center Security: Server
- Upgrading to Symantec Data Center Security: Server Advanced 6.7
- Upgrading to Symantec Data Center Security: Server 6.7

For more information about the installation and upgrade procedures, see the *Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced 6.7 Planning and Deployment Guide* that is available at http://www.symantec.com/docs/DOC9277.

Resolved issues in this release

For the resolved issues in 6.7:

- Data Center Security: Server Advanced agents, see Table 1-5.
- Management Server, see Table 1-6.
- Management console (Java console), see Table 1-7.

The Data Center Security: Server Advanced agent issues that were resolved in this release.

Table 1-5 Resolved issues of agent

Issue	Description
Installing agent with RT-FIM enabled on computers using SolarFlare network adapters used to result in crash.	The RT-FIM driver had a conflict with OpenOnLoad kernel module on computers which use certain SolarFlare network adapters. The RT-FIM driver has been updated and will not conflict with the OpenOnLoad kernel module. Affected operating systems: All supported Linux platforms. Affected versions: 6.6 MP1 and earlier.
In certain scenario, the computer used to be unresponsive with NFSD kernel module loaded.	On running a specific command on a NFS mounted partition, NFS server having an agent used to become unresponsive. Affected operating systems: All supported Linux platforms. Affected versions: 6.6 MP1 and earlier.
On Solaris 10 computers, under heavy network operations, applications were being routed incorrectly to a custom sandbox.	Some applications were being routed incorrectly to a different sandbox on a computer with heavy network operations. Affected operating systems: Solaris 10 platforms. Affected versions: 6.6 MP1 and earlier.
In certain scenario, agent IDS service used to crash.	When IDS policy containing multiple filenames with invalid file path syntax is applied to the agent, agent IDS service crashes. Affected operating systems: All supported Windows platforms. Affected versions: 6.0 and later.
In certain scenario, IDS Service used to crash.	IDS service used to crash when Windows event is generated from an application not having meta-data. Affected operating systems: All supported Windows platforms. Affected versions: 6.6 MP1 and earlier
With certain applications installed, the IDS service was causing computer reboot.	During the computer boot up, there were few computer calls that were hooked by an application before the agent starts. In such cases, agent computer used to reboot on start of IDS service. Affected operating systems: All supported Linux platforms. Affected versions: 6.6 MP1 and earlier.

Table 1-5 Resolved issues of agent *(continued)*

Issue	Description
In certain scenario, Windows agent computer becomes unresponsive.	Windows server computer used to get into unresponsive state due to a deadlock caused by SISIPSDriver while performing cleanup task on process termination. Affected operating systems: All supported Windows platforms. Affected versions: 6.6 MP1 and earlier.

The Data Center Security: Server Advanced Management Server issues that were resolved in this release.

Table 1-6 Resolved issues of Management Server

Issue	Description
In certain scenario, unable to view predefined application list.	Predefined application list in policy editor failed to load, if the added application name had a comma. Affected operating systems: All supported Management Server platforms. Affected versions: 6.0 and later.

The Management Console (Java console) issues that were resolved in this release.

Table 1-7 Resolved issues of Management Console

Issue	Description
* gets added to application directory path of Unix IPS policies.	In Unix IPS policies, while adding any directory path to **Application Rules** section, * was getting added at the end of the directory path. Affected versions: 6.6 and later.

Known issues in this release

For the known issues in 6.7 of:

- Data Center Security: Server Advanced, see Table 1-8 .
- Data Center Security: Server, see Table 1-9
- Unified Management Console, see Table 1-10.

Table 1-8 Known issues of Data Center Security: Server Advanced

Issue description	Workaround
In a multi Data Center Security: Server setup, if you unregister the Management Server with VMware NSX, and then try to re-register the Management Server with VMware NSX, Management Server registration with VMware NSX fails.	Reboot the computer on which the Management Server is installed.
In the Unified Management Console, if you navigate to **Server** > **Events** > **Audit Events**, some of the events do not display the name for **Machine Name**. Additionally, the value for the **User Name** displays as UNAUTHORIZED.	Not available.
If the IP address of the Management Server computer is changed, then the Management Server registration with Unified Management Console is not updated, and you cannot re-register the Management Server with Unified Management Console. This issue occurs if you are using DHCP on your Management Server computer.	Use the static IP on the Management Server computer before installing or upgrading to Management Server 6.7.
If you install an Agent on the Management Server computer and check the **Detect Duplicate Agent Registration** with IP address or Host Name, then the Agent does not appear in the Unified Management Console > **Assets** tab.	Do one of the following: ■ Clear the **Detect Duplicate Agent Registration** check box. ■ Check the **Detect Duplicate Agent Registration** check box, and then check **Asset Name** check box.
If you install an Agent on the Management Server computer and check the **Detect when Duplicate Agent is registered** with Agent Name, Host Name, and IP address, then the Virtual Agent representing the docker containers does not appear in the Unified Management Console > **Assets** tab.	Not applicable
If the Management Server services are installed on the same host as the SQL Server database, the SQL Server services may not be fully started before the Management Server services attempt to initialize the database pool connections.	Change the start up type for each of the Management Server service from **Automatic** to **Automatic (Delayed Start)**.
When a hardened policy is applied on the Asset on which the Management server, Management Console, and an Agent is installed, and if you try to re-launch the Server Configuration wizard, then the Management Server configuration wizard is not launched.	Tune the policy or temporarily override the protection.

Table 1-8 Known issues of Data Center Security: Server Advanced *(continued)*

Issue description	Workaround
While updating custom sandbox for tuning a policy violation events, if you have a similar custom sandbox name in multiple policies and violation events exists for these policies in database, then the violation events coming from all the policies may be considered for processing.	Not available.
Override tool on Solaris 11 (x86_64 and Sparc) computer fails to work.	You can use the sisipsconfig tool to toggle the prevention state.
Root user cannot uninstall a package including Docker and MySQL when prevention policy is applied on an agent running on an Ubuntu computer.	Login as a root user and disable the prevention policy before uninstalling a package on Ubuntu platform.
Upgrading the Management Server to 6.7 with large data set can cause problems with SIS Manager Service to restart at the end of installation, which displays an error message on installation wizard.	Restart the sis manager service.
If you import the policy pack using the Unified Management Console, then the name of the newly imported policy templates are appended with invalid characters	Not available
After installing the agent on Solaris 11 (x86_64 & SPARC), network controls are not working.	Not available
In the Unified Management Console, if you use a backward slash in the **Path** field while adding a LiveUpdate Server, and then if you try to edit and save a SVA Config Policy that is published, the application throws an error message.	While adding or editing a LiveUpdate server, use a forward slash (/) in the **Path** field.
On the Solaris 11 computer, the NFS file system is not supported.	Not available
When you run the server.exe installer, the UMC Registration window displays the IP address even though you select FQDN Only option.	Not available
When you install the Management Server, in the **Installation Type** and **Installation Summary** page, the installation type displays **Use Existing Database**, instead of **Use existing MSSQ Instance**.	Not available
IPS behavior for non existent remote file is different for pre and post vista opearting systems. On post-vista operating system, deny event is generated, and on pre-vista computer, deny event is not generated.	Not available

Table 1-8 Known issues of Data Center Security: Server Advanced *(continued)*

Issue description	Workaround
In the Management Console, if you navigate to **Policies** > **Detection**, and edit **Windows Teletemetry Policy** and add an exception by selecting Allow or Deny in the Disposition field, the DNET events in SISIDSEvents.csv file displays the disposition value as 'A' and 'D' instead of 'Allow' and 'Deny'.	Not available
Inside the Docker container, the driver is unable to populate `/proc` and `/sys` paths. Instead, the driver can see the content of these directories directly. Because of this, you will not be able to get the output for `pstree` and `top` commands inside the containers. When the preventions is enabled, some containers will fail to start as the container fails to write into `/proc` directory while creating process with PID 1.	Disable the prevention for the container sandbox.
In both pre-vista and post-vista operating systems, whenever any service tries to access a process added under **deny_ps**, the process is successfully getting blocked. However, in pre-vista operating system, an event is generated for 'Create' operation, and for Post-vista operating system, an event is generated for 'Execute' operation. On post-vista operating systems, the driver is able to prevent a process that is routed to deny_ps from even starting. That is why the PPST event is generated for 'Execute' operation rather than 'create' operation. On pre-vista operating system, a process that is routed to deny_ps actually gets created but then is unable to run. That is why the PPST event is generated for the 'create' operation.	Not available

Table 1-8 Known issues of Data Center Security: Server Advanced *(continued)*

Issue description	Workaround
If you are already using Data Center Security: Server Advanced and have configured to use the Windows authentication for Database connection and services, then, after upgrading to Data Center Security: Server Advanced 6.7, the Unified Management Console services will run in **Local System** account.	You must configure and update the logon user account details for the following Unified Management Console services: ■ **Symantec UMC Credential Service** ■ **Symantec UMC Telemetry Service** To update the user account details, perform the following in the same sequence. 1 Click Start and enter services.msc in the **Search** field and press Enter. 2 Right-click on the service, and click **Properties** . 3 To specify the user account that the service can use to log on, click the **Log On** tab > **This account**, and click **Browse**. 4 Enter a user account in the **Select User** dialog box. Ensure that you enter the Windows user account details on which the Management Server is running. 5 Type the password for the user account in **Password** and **Confirm password** fields, and click **OK**.

Table 1-9 Known issues of Data Center Security: Server

Issue description	Workaround
In the Unified Management Console, if you navigate to **Server** > **Security Groups** > **NSX Security Groups**, the NSX security groups may display the GVM as GNTP protected or AV protected, even though the GVM is powered off.	Not available.

Table 1-10 Known issues of Unified Management Console

Issue description	Workaround
The password of the dcsadmin user does not support the followng characters. ■ " ■ %	Not available.

Table 1-10 Known issues of Unified Management Console *(continued)*

Issue description	Workaround
The Tomcat only installation type does not validate or authenticate the provided user details in the UMC details page.	Run the configuration wizard if a wrong user was added.
If Operations Director is registered with UMC in a multiple server environment then Operations Director can be launched only from the UMC with which it was registered. Operations Director is inaccessible from the other servers.	Not available.

Where to get more information

The latest information for DCS: Server, Monitoring Edition, and Server Advanced is available at:

- Symantec™ Data Center Security: Server, Monitoring Edition, and Server Advanced Online help.

Product manuals are available at:

- Symantec™ Data Center Security: Server - Documentation Set.
- Symantec™ Data Center Security: Monitoring Edition - Documentation Set.
- Symantec™ Data Center Security: Server Advanced - Documentation Set.

The following table lists additional information that is available from the Symantec web sites.

Table 1-11 Symantec web sites

Type of information	Web address
Public Knowledge Base Releases and updates Manuals and other documentation Contact options	http://www.symantec.com/business/support/
Virus and other threat information and updates	http://securityresponse.symantec.com