Legal Notice

Copyright © 2015 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Technical Support

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

Symantec’s support offerings include the following:

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

For information about Symantec’s support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

Licensing and registration
If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:
www.symantec.com/business/support/

Customer service
Customer service information is available at the following URL:
www.symantec.com/business/support/
Customer Service is available to assist with non-technical questions, such as the following types of issues:
  Questions regarding product licensing or serialization
  Product registration updates, such as address or name changes
  General product information (features, language availability, local dealers)
  Latest information about product updates and upgrades
  Information about upgrade assurance and support contracts
  Information about the Symantec Buying Programs
  Advice about Symantec’s technical support options
  Nontechnical presales questions
  Issues that are related to CD-ROMs, DVDs, or manuals
Support agreement resources

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

Asia-Pacific and Japan  customercare_apj@symantec.com
Europe, Middle-East, and Africa  semea@symantec.com
North America and Latin America  supportsolutions@symantec.com
This chapter includes the following topics:

- About DCS:SA and FIPS 140-2 level 1 compliance

**About DCS:SA and FIPS 140-2 level 1 compliance**

Symantec Data Center Security: Server Advanced v6.5 adheres to the FIPS 140-2 Level 1 standards. Deploying DCS:SA in a FIPS-compliant configuration ensures FIPS compliance for the following types of communications:

- Console-to-server
- Windows agent-to-server

By default, FIPS mode is enabled in all new installations of DCS:SA consoles. For the server component, you must enable the FIPS mode manually.

**About the features that handle sensitive information and their FIPS-compliance**

To ensure FIPS 140-2 Level 1 compliance, DCS:SA uses the following algorithms and technologies:
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| DCS:SA management server and console communication | All the communications between the DCS:SA management server and the console take place over TLS tunnel. The DCS:SA management server supports the following cipher suites:  
  - TLS_RSA_WITH_AES_128_CBC_SHA  
  - TLS_RSA_WITH_AES_256_CBC_SHA |
| DCS:SA management server and Windows agent communication | All the communications between the DCS:SA management server and the Windows agents take place over TLS tunnel. The DCS:SA management server supports the following cipher suites:  
  - TLS_RSA_WITH_AES_128_CBC_SHA  
  - TLS_RSA_WITH_AES_256_CBC_SHA |
| OpenSSL changes on Windows agents | Symantec uses OpenSSL FIPS object module v2.0.5 with OpenSSL 1.0.1j to handle communications on the agent side. |
| Use of RSA BSAFE crypto provider libraries:  
  - RSA BSAFE Crypto-J 6.1.1  
  - RSA BSAFE Cert-J 6.1.0.0.1  
  - RSA BSAFE SSL-J 6.1.2  
  - JCE Unlimited Strength for Java 7 | The RSA BSAFE crypto provider libraries are used for all cryptographic operations on the management server and console as follows:  
  - Hashing DCS:SA user account passwords  
  - Encrypting vCenter passwords required for VMWare Service Composer integration.  
  - Generating keys for SSL TLS connections between the management server, Windows agents, and consoles.  
  - TLS connections between the management server, Windows agent, and console with cipher suites as specified above.  
  - JCE Unlimited Strength library is used along with RSA BSAFE libraries for extended keysize support in AES and RSA encryption algorithms. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of SHA-256 algorithm</td>
<td>MD5 usage has been replaced by SHA-256 wherever MD5 was being used.</td>
</tr>
</tbody>
</table>
Deploying DCS:SA for FIPS 140-2 level 1 Compliance

This chapter includes the following topics:

■ Prerequisites to work in a FIPS-enabled environment
■ About DCS:SA versions that support FIPS 140-2 level 1 compliance
■ Enabling FIPS mode
■ Disabling FIPS mode

Prerequisites to work in a FIPS-enabled environment

To work in a FIPS-compliant environment, ensure that you perform the following configurations:

■ In case of upgrade from SCSP v5.2.9 or earlier to DCS:SA v6.5, users must authenticate themselves before enabling the FIPS mode on the upgraded server.

■ Users must accept the certificate while logging to the console for the first time after upgrading to DCS:SA v6.5.

FIPS compliance does not support SSL certificates with MD5 as signature algorithm. The old MD5 SSL certificates are retained on the agent if you have upgraded the management server gradually or directly from SCSP v5.2.0 to DCS:SA v6.5. In such a scenario, you must manually create and apply the certificates on the agents after the upgrade.

See “Generating SHA-256 certificates manually” on page 14.
About DCS:SA versions that support FIPS 140-2 level 1 compliance

Currently, SDCS:SA 6.0 MP1 and DCS:SA v6.5 support FIPS 140-2 level 1 compliance.

Enabling FIPS mode

FIPS mode is enabled by default for the console. When a user installs DCS:SA v6.5 console or upgrades to DCS:SA v6.5 console, FIPS mode is enabled by default.

FIPS mode is disabled by default on the management server. FIPS mode is not enabled when you install or upgrade to the DCS:SA v6.5 server. On DCS:SA v6.5 Windows agents, FIPS enabled by default and the communication between the server and the agent is FIPS-compliant only after you enable FIPS on the server.

To enable FIPS on the server, you must execute the ConfigFIPS.vbs script file.

The ConfigFIPS.vbs script file is present at the following locations:

For server 
<installation-directory>\Server\tools

For console 
<installation-directory>\Console

Disabling FIPS mode

To disable FIPS mode on the console:

- Execute the ConfigFIPS.vbs script with the –d switch from the command prompt.

This script file is present at the following location:

<installation-directory>\Console

To disable FIPS mode on the server:

1. Execute ConfigFIPS.vbs script with the –d switch from the command prompt.
2. This script file is present at the following location:
   <installation-directory>\Server\tools
Limitations

This chapter includes the following topics:

- DCS:SA limitations for FIPS compliance

DCS:SA limitations for FIPS compliance

The following limitations are present in DCS:SA with regards to FIPS compliance:

- The DCS:SA server installation generates SHA-1 certificates by default. However, FIPS recommends that you use SHA-256 certificates. You can manually create the SHA-256 certificates.
  
  See “Generating SHA-256 certificates manually” on page 14.

  Use of SHA-256 certificates may result in compatibility issues with agents that use OpenSSL version earlier than 0.9.8o. They are unable to communicate with the DCS:SA Management Server.

  To handle this use case, you need to do the following:

  - Along with Primary management server which uses SHA-1 certificate, install Tomcat-only server. Generate SHA-256 certificates on Tomcat-only server and enable FIPS mode on it.

  - Register agents with OpenSSL version 0.9.8o and above with the Tomcat-only server, which uses SHA-256 certificates.

  - Register the agents that use OpenSSL version older than 0.9.8o with the primary management server that uses SHA-1 certificates.
Appendix

This appendix includes the following topics:

- Generating SHA-256 certificates manually

Generating SHA-256 certificates manually

The DCS:SA server installation generates SHA-1 certificates by default. However, as per FIPS guidelines, if you want to work in a strictly FIPS-compliant environment, you must use SHA-256 certificates. You can manually create the SHA-256 certificates.

Preparing for manual generation of SHA-256 certificates

1. Copy the original certificate files to a safe location.
   The certificates can be found at the following locations:
   - %programfiles%\Symantec\Data Center Security Server\server\agent-cert.ssl
   - %programfiles%\Symantec\Data Center Security Server\server\server-cert.ssl
   - %programfiles%\Symantec\Data Center Security Server\server\server-console-cert.ssl

2. Save a copy of the server.xml file that is present at the following location:
   %programfiles%\Symantec\Critical System Protection\server\tomcat\conf
   From the server.xml file, record the value for keystorepass, which is an alphanumeric string of 40 characters.

3. Record the Common Name (CN) parameter. For the DCS:SA server, this value is always SCSP_Management_Server.
4 Record the Hostname of the SCSP server, which you need for the OU parameter.

5 Locate the keytool.exe that is present at the following location:
   %programfiles%\Symantec\Data Center Security Server\Server\jre\bin

Creating the SHA-256 certificates manually

1 From the command-line, access the keytool utility that is present at the following location:
   %programfiles%\Symantec\Critical System Protection\server\jre\bin

2 Copy the server-cert.ssl to this location:
   %programfiles%\Symantec\Critical System Protection\server\jre\bin

3 Using the command line, enter the following:

   keytool.exe -delete -keystore server-cert.ssl -alias sss
   -storepass [40 character alpha-numeric string that is found in the server.xml file] -storetype PKCS12

4 Using the command line, enter the following:

   keytool.exe -genkey -keystore server-cert.ssl -alias sss -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -storetype PKCS12
   -storepass [40 character alpha-numeric string found in the server.xml file]
   -keypass [40 character alpha-numeric string found in server.xml] -dname "CN=SCSP_Management_Server, OU=[SCSP server hostname]"

5 Via the command line, enter the following:

   keytool.exe -export -Alias sss -rfc -keystore server-cert.ssl
   -file agent-cert.ssl -storepass [40 character alpha-numeric string found in the server.xml file] -storetype PKCS12

6 Use the agent-cert.ssl created in Step 5 for agent-server communication.

7 Repeat Step 2 through Step 4 for the server-console-cert.ssl file.

Replacing existing certificates with newly created certificates

1 On the DCS:SA server, do the following:
   ■ Stop the DCS:SA management service
   ■ Replace the original server-cert.ssl found at the following location with the new certificates created by using keytool:
     %programfiles%\Symantec\Critical System Protection\server
   ■ Replace the original server-console-cert.ssl found at the following location with the new certificates created by using keytool:
%programfiles%\Symantec\Critical System Protection\server

- Replace the original agent-cert.ssl that is present at the following location with the new agent-cert.ssl created by using keytool:
  %programfiles%\Symantec\Critical System Protection\server

- Restart the DCS:SA management server service

2 On the DCS:SA agent, do the following:

- Copy the newly created agent-cert.ssl to the agent machine.

- Update the agent to use the new agent-cert.ssl with the following command (forces use of new agent-cert.ssl file):
  sisipsconfig -c agent-cert.ssl

- To test the connection from the command prompt:
  sisipsconfig -t
Additional Resources

This appendix includes the following topics:

- Where to get more information

Where to get more information

Product manuals for DCS:SA are available on the DCS:SA product media. Updates to the documentation are available from the Symantec Technical Support and Business Critical Services (BCS) Web sites.

The DCS:SA product manuals are as follows:

- Installation Guide Online Help
- DCS:SA Online Help
- Planning and Deployment Guide
- Overview Guide
- Administrator's Guide
- Prevention Policy Reference Guide
- Detection Policy Reference Guide
- Agent Guide
- Implementation Guide Integration with VMware NSX (for Security Virtual Appliance)
- Operations Director Reference Guide
- vSphere Support Guide
- Release Notes
- Platform and Feature Matrix
The following table lists additional information that is available from the Symantec Web sites.

<table>
<thead>
<tr>
<th>Type of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Knowledge Base</td>
<td><a href="http://www.symantec.com/business/support/">http://www.symantec.com/business/support/</a></td>
</tr>
<tr>
<td>Releases and updates</td>
<td></td>
</tr>
<tr>
<td>Manuals and other documentation</td>
<td></td>
</tr>
<tr>
<td>Contact options</td>
<td></td>
</tr>
<tr>
<td>Virus and other threat information</td>
<td><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></td>
</tr>
<tr>
<td>and updates</td>
<td></td>
</tr>
</tbody>
</table>