Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark 1.1.0

For Sybase ASE 15.0.X

Symantec

Symantec™ Enterprise Security Manager Baseline Policy Manual for CIS Benchmark 1.1.0

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, the Symantec Logo, ActiveAdmin, BindView, bv-Control, and LiveUpdate 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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. 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.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Baseline Policy Manual for CIS Benchmark for Sybase ASE

This chapter includes the following topics:

Introducing the policy

The Symantec Enterprise Security Manager (ESM) Baseline Policy for the Center for Internet Security (CIS) Benchmark for Sybase ASE version 1.1.0 assesses a host's compliance with the benchmark's recommendations.

This release of the policy was built based on the CIS benchmark version 1.1.0 for Sybase ASE. This policy can be installed on Symantec ESM 9.0.1 and 10.0 managers running Security Update 40 or later and ESM Sybase application module version 4.0.

For information on the Center for Internet Security benchmarks, visit the following URL:

http://www.cisecurity.org

Installing the policy

Before you install the policy, you must decide on the Symantec ESM Managers that you want to install the policy. Since policies run on Managers, you do not require to install policies on agents. You must install the policy on Symantec ESM 9.0.1 and 10.0 managers with Security Update 40 or later and ESM Sybase application module version 4.0.

Obtaining and Installing the policy using LiveUpdate

You can install the LiveUpdate feature in the following ways:

- By using the LiveUpdate feature on the Symantec ESM console
- By using files from a Product disc or from the Internet

To install the policy using LiveUpdate

1. Connect the Symantec ESM Enterprise Console to the managers on which you want to install the policy.
2. Click the **LiveUpdate** icon to start the LiveUpdate Wizard.
3. In the wizard, ensure that Symantec LiveUpdate (Internet) is selected, and then click **Next**.
4. In the **Welcome to LiveUpdate** panel, click **Next**.
5. In the **Available Updates** panel, do one of the following:
   - To install all checked products and components, click **Next**.
   - To omit a product from the update, uncheck it, and then click **Next**.
   - To omit a product component, expand the product node, uncheck the component that you want to omit, and then click **Next**.
6. In the **Thank you** panel, click **Finish**.
7. In the list of managers panel, ensure that all the managers that you want to update are checked, and then click **Next**.
8. In the **Updating Managers** panel, click **OK**.
9. In the **Update Complete** panel, click **Finish**.

If you cannot use LiveUpdate to install the policy directly from a Symantec server, you can install the policy manually, using files from a Product disc or the Internet.

Note: To avoid conflicts with the updates that are performed by standard LiveUpdate installations, copy or extract the files into the LiveUpdate folder, which is usually Program Files/Symantec/LiveUpdate.

To install the policy from a Product disc or from the Internet

1. Connect the Symantec ESM Enterprise Console to the managers that you want to update.
2. From the Symantec Security Response Web site, download the executable files for Sybase ASE. You can go to the following link:

   http://securityresponse.symantec.com
3. On a computer running Windows NT/XP/Server 2003 that has network access to the manager, run the executable that you downloaded from the Symantec Security Response Web site.
4. Click **Next** to close the **Welcome** panel.
5. In the **License Agreement** panel, if you agree to the terms of the agreement, click **Yes**.
6. In the **Question** panel, click **Yes** to continue installation of the best practice policy.
7. In the **ESM Manager Information** panel, type the requested manager information, and then click **Next**.

   If the manager's modules have not been upgraded to Security Update 36 or later, the installation program returns an error message and stops the installation. Upgrade the manager to Security Update 36 or later, and then rerun the installation program.
8. Click **Finish**.

Chapter 2

Policy modules

This chapter includes the following topics:

Policy modules

The CIS Benchmark for Sybase ASE policy includes the modules that ensure compliance with various technical and administrative aspects. Each module lists the enabled checks with the standards that they address, the associated name lists, and the templates. As specific values are not required everywhere, default values and templates are provided. Although the policy appears as read only, you can copy or rename the policy, depending on the requirements of your corporate security policy.

File Attributes

This module reports changes in the attributes of system files.

Table 2-1 gives a list of the checks and their CIS sections.

Table 2-1 Checks and CIS sections

Check	CIS section
Exclude decreased permissions	5.3, 6.10
Group ownership	5.3, 6.10
Ignore symbolic links	5.3, 6.10
Local disks only	5.3, 6.10
Permissions	5.3, 6.10
User ownership	5.3, 6.10

Sybase ASE Account

This module checks for the server account that is based on the options that you have specified.

Table 2-2 gives a list of the checks and their CIS sections.

Table 2-2 Checks and CIS sections

Check	CIS section
Locked accounts not manually locked by ASE	1.4
Unlocked default logon accounts	1.4
Accounts with default master database	3.1.1

Sybase ASE Auditing

This module checks for the auditing setup that is based on the options that you have specified.

Table 2-3 gives a list of the checks and their CIS sections.

Table 2-3 Checks and CIS sections

Check	CIS section
Multiple audit tables	4.4

Table 2-3 Checks and CIS sections *(continued)*

Check	CIS section
Sufficient log space	4.1
Auditing enabled	4.3

Sybase ASE Configuration

This module checks for the Sybase configuration that is based on the options that you have specified.

Table 2-4 gives a list of the checks and their CIS sections.

Table 2-4 Checks and CIS sections

Check	CIS section
SSL encryption and strong cipher	2.1
Prohibited extended stored procedures	5.3.1, 5.3.2 **Note:** ESM modules for Sybase ASE are not host-based on Windows for CIS section 5.3.2, which is Windows specific. Therefore, the prohibited files check functionality is not provided. The extended stored procedures mentioned in CIS section 5.3.2 can be remotely checked.
Configuration parameters	1.8, 2.1, 2.2, 2.3, 2.4, 2.5.2, 3.5, 3.5.1, 4.2, 4.6, 4.7, 4.8, 5.1, 5.2
Net password encryption	2.5.1
Sample databases	6.6

Sybase ASE Object

This module checks for the Sybase server for database existence and its object permission that is based on the options that you have specified.

Table 2-5 gives a list of the checks and their CIS sections.

Table 2-5 Checks and CIS sections

Check	CIS section
Database backups protected **Note:** Use the **Database backup files** name list to specify the full path of the database dump files that should be included in this check. If the name list is empty, this check reports no problems found.	6.1
User access to database	3.2.1
Object permission	3.4

Sybase ASE Password Strength

This module checks for the password integrity that Sybase server account uses based on the options that you have specified.

Table 2-6 gives a list of the checks and their CIS sections.

Table 2-6 Checks and CIS sections

Check	CIS section
Encryption keys in database	3.6.2
Password protect encryption keys	3.6.3
Empty password	1.4, 1.6, 1.5
Password = login name	1.5
Password = any login name	1.5
Password = wordlist word	1.5
Password contains digits	1.6
Minimum password length	1.6
Roles without passwords	1.9
Roles - minimum password length	1.6, 1.6.1
Password complexity parameters	1.3, 1.6, 1.7, 1.8
System encryption password	3.6.1

Sybase ASE Patches

This module identifies the Sybase patches that are not installed on Sybase server.

Table 2-7 gives a list of the checks and their CIS sections.

Table 2-7 Checks and CIS sections

Check	CIS section
Patch templates	6.11

Sybase ASE Roles and Groups

This module checks for the roles and groups that are based on the options you have specified.

Table 2-8 gives a list of the checks and their CIS sections.

Table 2-8 Checks and CIS sections

Check	CIS section
Granted prohibited roles	1.4