

Symantec Enterprise Security Manager™ Modules for Sybase Adaptive Server Enterprise User's Guide

Release 1.0 for Symantec ESM 6.0, 6.1.1, and 6.5.x

For Sybase Adaptive Server Enterprise on AIX, HP-UX, and Solaris



Symantec Enterprise Security Manager™ Modules for Sybase

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

Copyright ©2007 Symantec Corporation.

All Rights Reserved.

Symantec, the Symantec Logo, LiveUpdate, Symantec Enterprise Security Architecture, Enterprise Security Manager, and NetRecon 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.

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
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Technical support

As part of Symantec Security Response, the Symantec Global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible 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 as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features that are available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.htm, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

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

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with 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 on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Technical support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product feature and function, installation, and configuration. The Technical Support group also authors 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 technical 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
- A telephone and web-based support that provides rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support that is available 24 hours a day, 7 days a week worldwide. Support is provided in a variety of languages for those customers that are enrolled in the Platinum Support program
- Advanced features, including Technical Account Management

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

www.symantec.com/techsupp/

Select your country or language under Global Support. The specific features that are available may vary based on the level of maintenance that was purchased and the specific product that you are using.

Contacting Technical Support

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

www.symantec.com/techsupp/

Select your region or language under Global 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 recreate the problem.

When contacting the Technical Support group, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
 - Error messages/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/techsupp/

Select your region or language under Global Support, and then select the Licensing and Registration page.

Customer Service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Select your country or language under Global Support.

Customer Service is available to assist with 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 insurance and maintenance contracts
- Information about Symantec Value License Program
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

- Asia-Pacific and Japan: contractsadmin@symantec.com
- Europe, Middle-East, and Africa: semea@symantec.com
- North America and Latin America: [supportolutions@symantec.com](mailto:supportsolutions@symantec.com)

Additional Enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively. Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring and management capabilities, each focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Chapter 1	Introducing Symantec ESM modules for Sybase Adaptive Server Enterprise	
	About the Symantec ESM modules for Sybase ASE	13
	What you can do with the Symantec ESM modules for Sybase ASE	14
	Where you can get more information	14
Chapter 2	Installing Symantec ESM modules for Sybase ASE	
	Before you install	15
	System requirements	15
	Installing the ESM modules for Sybase ASE	16
	Editing configuration records	18
Chapter 3	Symantec ESM module checks for Sybase ASE	
	About Symantec ESM module checks for Sybase ASE	19
	Sybase account checks	19
	Servers to check	20
	Automatically update snapshots	20
	Enabled default logon accounts	20
	Logon accounts	20
	New logon accounts	20
	Deleted logon accounts	21
	Sybase audit checks	21
	Servers to check	21
	Auditing enabled	21
	Auditing threshold procedure	22
	Audit segments	22
	Audit queue size	22
	Suspend audit when device is full	23
	Truncate transaction log on checkpoint	23
	Sybase configuration checks	23
	Servers to check	23
	Version and product level	24
	Configuration parameters	24
	Master device default status	24
	Device status	25

Sybase object checks	25
Servers to check	25
Automatically update snapshots	25
Database status	26
User access to databases	26
New database	26
Deleted database	27
Object types to check (name list)	27
Databases to check (name list)	27
Object actions to check (name list)	27
Objects to check (name list)	27
Grantors to check (name list)	27
Grantable object permissions	28
Granted object permissions	28
New granted object permissions	28
Deleted granted object permissions	29
Object permissions	29
Sybase password checks	30
Servers to check	30
Empty password	30
Password = login name	30
Password = any login name	30
Password = wordlist word	31
Reverse order	31
Double occurrences	31
Plural	31
Prefix	32
Suffix	32
Password contains a digit	32
Minimum password length	32
Minimum password age	33
Role without password	33
Sybase patches checks	33
Servers to check	33
Patch templates	33
Creating Sybase ASE patches template file	34
Sybase role and group checks	35
Servers to check	35
Automatically update snapshots	35
Roles status	35
Role grantees	35
New roles	35
Deleted roles	36

Database groups	36
Group members	36
New groups	37
Deleted groups	37

Introducing Symantec ESM modules for Sybase Adaptive Server Enterprise

This chapter includes the following topics:

- [About the Symantec ESM modules for Sybase ASE](#)
- [What you can do with the Symantec ESM modules for Sybase ASE](#)
- [Where you can get more information](#)

About the Symantec ESM modules for Sybase ASE

The Symantec Enterprise Security Manager (ESM) modules for Sybase Adaptive Server Enterprise (ASE) database servers extends Symantec ESM protection to your Sybase ASE servers.

These modules implement 60 new checks and options, which are specific to Sybase ASE servers, to protect them from exposure to known security problems. The modules may be installed locally on the Symantec ESM agent that resides on your Sybase ASE server. The modules may also assess Sybase servers over the network and be installed on an ESM agent that has the Sybase ASE client installed.

You can use the Symantec ESM modules for Sybase ASE in the same way that you use other Symantec ESM modules.

What you can do with the Symantec ESM modules for Sybase ASE

You can perform the following tasks by using the Symantec ESM modules for Sybase ASE:

- Create a policy
- Configure the policy
- Create a rules template
- Run the policy
- Review the policy run
- Correct security problems from the console
- Create reports

Where you can get more information

See the latest versions of the Symantec Enterprise Security Administrator's Guide and the Symantec ESM Security Update User's Guide for more information about Symantec ESM modules and Security Updates.

For more information on Symantec Enterprise Security Manager (ESM), Symantec ESM Security Updates, and Symantec ESM support for database products, see the Symantec Security Response Web site at the following URL:

<http://securityresponse.symantec.com>

Installing Symantec ESM modules for Sybase ASE

This chapter includes the following topics:

- [Before you install](#)
- [System requirements](#)
- [Installing the ESM modules for Sybase ASE](#)

Before you install

Before you can install the Symantec ESM modules for Sybase ASE, you must do the following:

- Ensure that connectivity to all Sybase ASE servers is established. There must be a valid interfaces file on the target host.
- Log on as root to install the .tpi.

System requirements

[Table 2-1](#) lists the supported operating systems on which you can install ESM modules for Sybase ASE, and the operating systems on which these modules can report.

Table 2-1 ESM modules for Sybase ASE system requirements

Supported operating systems	Supported OS versions	Supported Sybase versions
AIX-RS6k-433 (64 bit)	5.1, 5.2	15.x.x

Table 2-1 ESM modules for Sybase ASE system requirements

Supported operating systems	Supported OS versions	Supported Sybase versions
Sun Solaris, Solaris-Sparc (32 and 64-bit)	2.7, 2.8, 2.9, 2.10	15.x.x
AIX (32 and 64-bit)	5.1, 5.2, 5.3	12.5.x
HP-UX (32 and 64-bit)	11, 11.11, 11.23	12.5.x

AIX, HP-UX, and Solaris can be used in a host-based or network-based, agentless environment.

Installing the ESM modules for Sybase ASE

You must install the modules on a Symantec ESM agent that is installed on the Sybase ASE server or on an ESM agent that has the Sybase ASE client configured to communicate with the Sybase ASE server. Installation is the same on each platform.

Modules are stored in an installation package that is named `esmsyb1.tpi`. The package does the following:

- Extracts and installs module executables, configuration (.m) files, and template files.
- Registers the .m and template files using your agent’s registration program.
- Calls the `SybaseSetup` program to create the SYMESMDBA account. See [“Editing configuration records”](#) on page 18 for more information.
 The password for the SYMESMDBA account is 12 characters long and is generated randomly. The password is encrypted using a proprietary encryption function and is stored in the following file: `/esm/config/esmsybaseenv.dat`

Note: The SYMESMDBA account performs only read operations.

- Grants the following default roles:
 - `sa_role`
 - `sso_role`
 The privileges of these default roles can be changed in the `esmsybaseenv.dat` file. Add a `“config SymEsmDbRole <name of new roles>”` entry to the SYMESMDBA account, separated by a comma or a space.

In the ESM modules for Sybase ASE release, the password must contain at least one upper-case, one lower-case, one number (0-9), and one special character. The default special characters are: `_` and `#`.

This is the character set that is used if the "config PassSpecString" entry is not defined in the `/esm/config/esmsybaseenv.dat` file.

To use another set of special characters, you must add, for example, a "config PassSpecString \$#_" entry into the `/esm/config/esmsybaseenv.dat` file before running the `tpi` or `SybaseSetup` program.

To install the ESM modules for Sybase ASE:

- 1 From a command prompt, install the module tune-up/installation package. The install package is named `esmsyb1.tpi`.
- 2 Type **2** to select the option that installs the module.
- 3 Do one of the following:
 - Type **yes** to register the template or `.m` files.
 - Type **no** if you have already registered these `.m` files when you installed the module on another agent on the same platform that is registered to this manager. This option is the default.
- 4 Type **yes** to continue and add configuration records.
- 5 Type the Sybase path. This is the path to your `$SYBASE` install directory.
- 6 Type the `SYBASE_OCS` directory or press Enter to accept the default. This is the directory from which you want to run the SQL (`isql`) client. It is a subdirectory of `$SYBASE`.
- 7 Type **yes** to add a configuration record for the listed Sybase ASE servers.
- 8 Type the login for the first server.
This login should be the SA login or a login with equivalent privileges. This login will be used to create a SYMESMDBA account that the modules will use to perform the security checks.
- 9 Type the password for the first server.
- 10 Retype the password for the first server.
- 11 Confirm that the information is correct.
- 12 Type **no** when you have finished adding configuration information for the listed servers.

Editing configuration records

After installing Symantec ESM Modules for Sybase ASE, you can edit the configuration records. A configuration record is created for each Sybase server when you enable security checking during installation.

You can add, modify, or remove the Sybase ASE servers that are configured for Symantec ESM security checks by using the SybaseSetup program. By default, SybaseSetup is located in the \ESM\bin\

[Table 2-2](#) lists the options that you can use when running the SybaseSetup.

Table 2-2 Editing configuration records

Action	Command
Display help.	SybaseSetup -h
Create configuration records for detected Sybase ASE servers.	SybaseSetup -c
Add a new configuration record for undetected Sybase ASE servers.	SybaseSetup -a
Modify existing Sybase ASE configuration records.	SybaseSetup -m
List existing Sybase ASE configuration records.	SybaseSetup -l

Note: If no option is specified, SybaseSetup runs with the -c option.

Symantec ESM module checks for Sybase ASE

This chapter includes the following topics:

- [About Symantec ESM module checks for Sybase ASE](#)
- [Sybase account checks](#)
- [Sybase audit checks](#)
- [Sybase configuration checks](#)
- [Sybase object checks](#)
- [Sybase password checks](#)
- [Sybase patches checks](#)
- [Sybase role and group checks](#)

About Symantec ESM module checks for Sybase ASE

By default, the checks are disabled when you install the module. To enable the checks, use the module properties functions. See the Symantec Enterprise Security Manager Administrator's Guide for more information on using module properties.

Sybase account checks

The following checks evaluate computers for security risks that are associated with Sybase ASE accounts.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE account security checks.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Enabled default logon accounts

The Enabled default logon accounts check reports default logon accounts that are enabled and should be disabled. Use the include list to specify logon names that should be disabled on the server.

[Table 3-1](#) shows the new message for the Enabled default logon accounts check.

Table 3-1 Enabled default logon accounts message

Message name	Title	Severity
ESM_SYBASE_DEFAULT_LOGON_ACCOUNT	Enabled default logon accounts	Yellow-2

Logon accounts

The Logon accounts check reports logon accounts and status. Use the name list to include or exclude logon names for this check.

[Table 3-2](#) shows the new message for the Logon accounts check.

Table 3-2 Logon accounts message

Message name	Title	Severity
ESM_SYBASE_LOGON_ACCOUNTS	Logon accounts	Yellow-2

New logon accounts

The New logon accounts check reports logon accounts that were added to the database after the last snapshot update. Use the name list to include or exclude logon names for this check.

[Table 3-3](#) shows the new message for the New logon accounts check.

Table 3-3 New logon accounts message

Message name	Title	Severity
ESM_SYBASE_NEW_LOGON_ACCOUNTS	New logon accounts	Yellow-2

Deleted logon accounts

The Deleted logon accounts check reports logon accounts that were deleted from the database after the last snapshot update. Use the name list to include or exclude logon names for this check.

[Table 3-4](#) shows the new message for the Deleted logon accounts check.

Table 3-4 Deleted logon accounts message

Message name	Title	Severity
ESM_SYBASE_DELETED_LOGON_ACCOUNT	Deleted logon accounts	Yellow-2

Sybase audit checks

The following checks evaluate computers for security risks that are associated with Sybase ASE auditing.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE audit security checks.

Auditing enabled

The Auditing enabled check reports Sybase ASE servers that do not have auditing enabled in the configuration parameters.

[Table 3-5](#) shows the new message for the Auditing enabled check.

Table 3-5 Auditing enabled message

Message name	Title	Severity
ESM_SYBASE_AUDITING_NOT_ENABLED	Auditing enabled	Red-4

Auditing threshold procedure

The Auditing threshold procedure check reports Sybase ASE servers that do not have an auditing threshold procedure enabled. It checks the sybsecurity database to see if a valid audit procedure is defined for each audit segment.

This check requires the Audit segments check to be selected.

Use the name list to define valid threshold procedure names. An empty name list will return a message for each segment list in the Audit segments check name list.

[Table 3-6](#) shows the new message for the Auditing threshold procedure check.

Table 3-6 Auditing threshold procedure message

Message name	Title	Severity
ESM_SYBASE_NO_THRES HOLD_PROCEDURE	Auditing threshold procedure	Red-4

Audit segments

The Audit segments check specifies which audit segments to check for an audit threshold procedure. This check is required by the Auditing threshold procedure check and must be run at the same time.

Use the name list to define the audit segments to check. An empty name list will return a message for every audit segment in the sybsecurity database.

Audit queue size

The Audit queue size check reports Sybase ASE servers that have an audit queue size larger than the specified value.

When you set the audit queue size, consider that a large value may lose audit records if the system goes down before writing records to the table. However, a value that is too low may result in frequent saves to the disk and may significantly slow the system.

[Table 3-7](#) shows the new message for the Audit queue size check.

Table 3-7 Audit queue size message

Message name	Title	Severity
ESM_SYBASE_AUDIT_ QUEUE_SIZE	Audit queue size	Red-4

Suspend audit when device is full

The Suspend audit when device is full check reports Sybase ASE servers that have a value for Suspend audit when device is full that does not match the specified value. A value of 0 causes the server to truncate the next audit table and begin using it as the latest audit table once the current audit table fills. A value of 1 causes the server to suspend the audit process and all user processes that cause an auditable event until an empty table is set as the current audit table.

[Table 3-8](#) shows the new message for the Suspend audit when device is full check.

Table 3-8 Suspend audit when device is full message

Message name	Title	Severity
ESM_SYBASE_SUSPEND_AUDITING	Suspend audit when device is full	Red-4

Truncate transaction log on checkpoint

The Truncate transaction log on checkpoint check reports Sybase ASE servers and their databases that are not configured to truncate transaction logs when performing a checkpoint. Use the Databases name list to include or exclude databases from this check.

[Table 3-9](#) shows the new message for the Truncate transaction log on checkpoint check.

Table 3-9 Truncate transaction log on checkpoint message

Message name	Title	Severity
ESM_SYBASE_TRUNCATE_LOG	Truncate transaction log on checkpoint	Red-4

Sybase configuration checks

The following checks evaluate computers for security risks that are associated with Sybase ASE server configurations.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE Configuration security checks.

Version and product level

The Version and product level check reports the Sybase ASE server's version and product level.

[Table 3-10](#) shows the new message for the Version and product level check.

Table 3-10 Version and product level message

Message name	Title	Severity
ESM_SYBASE_VERSION_LEVEL	Sybase version and product level	Green-0

Configuration parameters

The Configuration parameters check reports server configuration parameters that do not match values specified in the template.

[Table 3-11](#) shows the new messages for the Configuration parameters check.

Table 3-11 Configuration parameters messages

Message name	Title	Severity
ESM_SYBASE_SYP_GREEN_LEVEL	Sybase ASE Configuration Parameters	Green-1
ESM_SYBASE_SYP_YELLOW_LEVEL	Sybase ASE Configuration Parameters	Yellow-2
ESM_SYBASE_SYP_RED_LEVEL	Sybase ASE Configuration Parameters	Red-4
ESM_SYBASE_SYP_NOT_FOUND	Sybase ASE Configuration Parameters	Yellow-2

Master device default status

The Master device default status check reports servers that have the master device default disk status turned on. By default, the default disk status is turned on. This allows user databases to be installed on the master device.

[Table 3-12](#) shows the new message for the Master device default status check.

Table 3-12 Master device default status message

Message name	Title	Severity
ESM_SYBASE_DEVICE_DEFAULT	Master device default status	Yellow-2

Device status

The Device status check reports device status as specified in enabled Sybase ASE Device Status templates.

[Table 3-13](#) shows the new message for the Device status check.

Table 3-13 Device status messages

Message name	Title	Severity
ESM_SYBASE_SYD_GREEN_LEVEL	Device status	Green-1
ESM_SYBASE_SYD_YELLOW_LEVEL	Device status	Yellow-2
ESM_SYBASE_SYD_RED_LEVEL	Device status	Red-4

Sybase object checks

The following checks evaluate computers for security risks that are associated with Sybase ASE server objects.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE object security checks.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Database status

The Database status check reports databases and status that are configured to the Sybase ASE. Use the name list to include or exclude database names for this check.

[Table 3-14](#) shows the new message for the Database status check.

Table 3-14 Database status message

Message name	Title	Severity
ESM_SYBASE_ DATABASE	Database status	Green-0

User access to databases

The User access to databases check reports Sybase ASE databases that allow user access, such as guest. Use the Databases name list to include databases for this check. Use the value field to include user names for this check. The user names must be separated by a comma.

If you drop the guest user from the master database, server users who have not been added to any databases will not be able to log in to the Adaptive Server.

[Table 3-15](#) shows the new message for the User access to databases check.

Table 3-15 User access to databases message

Message name	Title	Severity
ESM_SYBASE_USER_ ACCESS_DATABASE	Databases	Yellow-2

New database

The New database check reports databases that were added to the Sybase ASE after the last snapshot update. Use the name list to include or exclude database names for this check.

[Table 3-16](#) shows the new message for the New database check.

Table 3-16 New database message

Message name	Title	Severity
ESM_SYBASE_NEW_ DATABASE	New database	Yellow-2

Deleted database

The Deleted database check reports databases that were deleted from the Sybase ASE after the last snapshot update. Use the name list to include or exclude database names for this check.

[Table 3-17](#) shows the new message for the Deleted database check.

Table 3-17 Deleted database message

Message name	Title	Severity
ESM_SYBASE_DELETED_DATABASE	Deleted database	Yellow-2

Object types to check (name list)

Use the Object types to check name list to specify object types (stored procedure, user table, or system table) to include or exclude for the Sybase ASE object checks following the name lists.

Databases to check (name list)

Use the Databases to check name list to specify databases to include or exclude for the Sybase ASE object checks following the name lists.

Object actions to check (name list)

Use the Object actions to check name list to specify object actions (Grant, Deny) to include or exclude for the Sybase ASE object checks following the name lists.

Objects to check (name list)

Use the name list to specify object names to include or exclude for the Sybase ASE object checks following the name lists. The object names may be the name of an object, stored procedure, view, trigger, etc. Wild cards may be used as well.

Grantors to check (name list)

Use the name list to specify grantors to include or exclude for the Sybase ASE object checks following the name lists.

Grantable object permissions

The Grantable object permissions check reports object permissions that are grantable. Use the name list to include or exclude grantee names for this check.

[Table 3-18](#) shows the new message for the Grantable object permissions check.

Table 3-18 Grantable object permissions message

Message name	Title	Severity
ESM_SYBASE_ GRANTABLE_PERM	Grantable object permissions	Red-4

Granted object permissions

The Granted object permissions check reports object permissions that are granted. Use the name list to include or exclude grantee names for this check.

[Table 3-19](#) shows the new message for the Granted object permissions check.

Table 3-19 Granted object permissions message

Message name	Title	Severity
ESM_SYBASE_GRANTED _PERM	Granted object permissions	Green-0

New granted object permissions

This check reports objects or granted object permissions that were added to the Sybase ASE after the last snapshot update. Use the name list to include or exclude grantee names for this check.

[Table 3-20](#) shows the new message for the New granted object permissions check.

Table 3-20 New granted object permissions messages

Message name	Title	Severity
ESM_SYBASE_NEW_OBJ_ ACTION	New granted object permissions	Yellow-2
ESM_SYBASE_NEW_OBJ_ COLUMN	New granted object permissions	Yellow-2
ESM_SYBASE_NEW_ OBJECT	New granted object permissions	Yellow-2

Deleted granted object permissions

The Deleted granted object permissions check reports objects or granted object permissions that were deleted from the Sybase ASE after the last snapshot update. Use the name list to include or exclude grantee names for this check.

[Table 3-21](#) shows the new message for the Deleted granted object permissions check.

Table 3-21 Deleted granted object permissions messages

Message name	Title	Severity
ESM_SYBASE_DELETED_ OBJ_ACTION	Deleted granted object permissions	Yellow-2
ESM_SYBASE_DELETED_ OBJ_COLUMN	Deleted granted object permissions	Yellow-2
ESM_SYBASE_DELETED_ OBJECT	Deleted granted object permissions	Yellow-2

Object permissions

The Object permissions check reports unauthorized object permissions as specified in the enabled Sybase ASE Object Permission templates.

[Table 3-22](#) shows the new message for the Object permissions check.

Table 3-22 Object permissions messages

Message name	Title	Severity
ESM_SYBASE_SYB_OBJ_ RED_LEVEL	Object existence	Red-4
ESM_SYBASE_SYB_OBJ_ YELLOW_LEVEL	Object existence	Yellow-2
ESM_SYBASE_SYB_OBJ_ GREEN_LEVEL	Object existence	Green-0
ESM_SYBASE_SYB_RED_ LEVEL	Object permissions	Red-4
ESM_SYBASE_SYB_ YELLOW_LEVEL	Object permissions	Yellow-2
ESM_SYBASE_SYB_ GREEN_LEVEL	Object permissions	Green-0

Sybase password checks

The following checks evaluate computers for security risks that are associated with Sybase ASE passwords.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE password security checks.

Empty password

The Empty password check reports Sybase ASE logins with empty or NULL passwords.

[Table 3-23](#) shows the new message for the Empty password check.

Table 3-23 Empty password message

Message name	Title	Severity
ESM_SYBASE_NULL_PASSWORD	Empty password	Red-4

Password = login name

The Password = login name check reports Sybase ASE logins with matching login names and passwords. To apply this check to role passwords, enable this check and the role password check in the Password policy.

[Table 3-24](#) shows the new message for the Password = login name check.

Table 3-24 Password = login name message

Message name	Title	Severity
ESM_SYBASE_GUESSED_PASSWORD	Password = login name	Yellow-2

Password = any login name

The Password = any login name check reports Sybase ASE logins with passwords that match any login name. To apply this check to role passwords, enable this check and the Role password check in the Password policy.

[Table 3-25](#) shows the new message for the Password = any login name check.

Table 3-25 Password = any login name message

Message name	Title	Severity
ESM_SYBASE_GUESSED_ PASSWORD	Password = any login name	Yellow-2

Password = wordlist word

The Password = wordlist word check reports matches between the Sybase ASE login passwords and words in enabled word files. To apply this check to role passwords, enable this check and the Role password check in the Password policy.

[Table 3-26](#) shows the new message for the Password = wordlist word check.

Table 3-26 Password = wordlist word message

Message name	Title	Severity
ESM_SYBASE_GUESSED_ PASSWORD	Password = wordlist word	Yellow-2

Reverse order

When the Reverse order option is enabled, password checks that guess passwords report logins containing passwords that match the reverse order of login names or entries in enabled word files. To apply this option to role passwords, enable this option and the Role password check in the Password policy.

Double occurrences

When the Double occurrences option is enabled, password checks report logins containing passwords that match double versions of login names or entries in enabled word files. To apply this option to role passwords, enable this option and the Role password check in the Password policy.

Plural

When the Plural option is enabled, password checks report logins with passwords that match plural forms of login names or entries in enabled word files. To apply this option to role passwords, enable this option and the Role password check in the Password policy.

Prefix

When the Prefix option is enabled, password checks report logins with passwords that match forms of login names or entries in enabled word files with a prefix. Use the option's name list to specify the prefixes to be used. To apply this option to role passwords, enable this option and the Role password check in the Password policy.

Suffix

When the Suffix option is enabled, specified suffixes are added to the user names and wordlist words that are used to guess passwords, for example, mail and mailbox. Use the option's name list to specify the suffixes to be used. The Suffix option affects the behavior of enabled Password = login name, Password = any login name, and Password = wordlist word security checks. To apply this option to role passwords, enable this option and the Role password check in the Password policy.

Password contains a digit

The Password contains a digit check reports Sybase ASE servers that do not have the configuration parameter enabled that requires new passwords to contain at least one character or digit.

[Table 3-27](#) shows the new message for the Password contains a digit check.

Table 3-27 Password contains a digit message

Message name	Title	Severity
ESM_SYBASE_PASS WORD_CONTAINS_DIGIT	Password contains a digit	Yellow-2

Minimum password length

The Minimum password length check reports Sybase ASE servers that have a minimum password length setting lower than the specified value for this check.

[Table 3-28](#) shows the new message for the Minimum password length check.

Table 3-28 Minimum password length message

Message name	Title	Severity
ESM_SYBASE_MIN_ PASSWORD_LEN	Minimum password length	Yellow-2

Minimum password age

The Minimum password age check reports Sybase ASE servers that have a system wide password expiration setting that is higher than the specified number days for this check.

[Table 3-29](#) shows the new message for the Minimum password age check.

Table 3-29 Minimum password age message

Message name	Title	Severity
ESM_SYBASE_MIN_PASSWORD_AGE	Minimum password age	Yellow-2

Role without password

The Role without password check reports roles that do not have passwords. Use the Roles list to include or exclude roles for this check.

[Table 3-30](#) shows the new message for the Role without password check.

Table 3-30 Role without password message

Message name	Title	Severity
ESM_SYBASE_ROLE_NO_PASSWORD	Role without password	Yellow-2

Sybase patches checks

The following options evaluate computers for security risks that are associated with Sybase ASE patches.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE patches security checks.

Patch templates

The Patch templates option specifies Sybase ASE Patch template files to be used by this module.

Table 3-31 shows the new message for the Patch templates check.

Table 3-31 Patch templates message

Message name	Title	Severity
ESM_SYBASE_PATCH_NOT_FOUND	Patch templates	Red-4

Creating Sybase ASE patches template file

To create Sybase ASE patches template file, do the following:

- Enter data in the following fields of the Sybase ASE patches template file:
 - Sybase ASE version:** Enter the Sybase ASE version. Refer to the Sybase ASE version installed on the remote systems. To know the Sybase ASE version, refer to the name of the directory where Sybase is installed. For example, if the directory name is ASE-12_5, the installed Sybase ASE version is 12.5.
 - Platform:** Select the platform of the remote system on which the Sybase database is installed or the platform for which the patch is released.
 - Product:** Enter the name of the database. For example, Adaptive Server 12.5.
 - Patch Id:** Enter the Sybase ASE patch id. For example, 116591-05.
 - Date:** Enter the date when the patch was released.
 - Architecture:** Select the architecture of the remote system on which the Sybase database is installed or the architecture for which the patch is released.
 - Description:** Enter the description for the patch installed. For example, the patch 116591-05 is meant for the Sun Cluster 3.1:HA-Sybase Patch.
- To add a new row, click **Add Row**. A new row is added at the bottom of the table.
- To delete a row (or rows), select the row (or rows), and click **Remove Rows**.
- Click **Save** to save the template file.
- Click **Close** to close the template file.
- Click **Help** to know more about how to use the template editor.

Sybase role and group checks

The following checks evaluate computers for security risks that are associated with Sybase ASE roles and groups.

Servers to check

The Servers to check option specifies the servers that are included or excluded by all Sybase ASE role and group security checks.

Automatically update snapshots

Enable this option to update snapshots automatically with current information.

Roles status

The Roles status check reports roles and their status. Use the role list to include or exclude roles for this check.

[Table 3-32](#) shows the new message for the Roles status check.

Table 3-32 Roles status message

Message name	Title	Severity
ESM_SYBASE_ROLE_STATUS	Roles status	Green-0

Role grantees

The Role grantees check reports role grantees. Use the role list to include or exclude roles for this check.

[Table 3-33](#) shows the new message for the Role grantees check.

Table 3-33 Role grantees message

Message name	Title	Severity
ESM_SYBASE_ROLE GRANTEE	Role grantees	Green-0

New roles

The New roles check reports roles and members that were added to the database after the last snapshot update. Use the name list to include or exclude role names for this check.

Table 3-34 shows the new message for the New roles check.

Table 3-34 New roles messages

Message name	Title	Severity
ESM_SYBASE_NEW_ROLE	New roles	Yellow-2
ESM_SYBASE_NEW_ROLE_GRANTEE	New roles	Yellow-2

Deleted roles

The Deleted roles check reports roles and members that were deleted from the database after the last snapshot update. Use the name list to include or exclude role names for this check.

Table 3-35 shows the new message for the Deleted roles check.

Table 3-35 Deleted roles messages

Message name	Title	Severity
ESM_SYBASE_DELETED_ROLE	Deleted roles	Yellow-2
ESM_SYBASE_DELETED_ROLE_GRANTEE	Deleted roles	Yellow-2

Database groups

The Database groups check reports database groups. Use the name list to include or exclude databases for this check.

Table 3-36 shows the new message for the Database groups check.

Table 3-36 Database groups message

Message name	Title	Severity
ESM_SYBASE_DATABASE_GROUP	Database groups	Green-0

Group members

The Group members check reports group members. Use the name list to include or exclude databases for this check.

[Table 3-37](#) shows the new message for the Group members check.

Table 3-37 Group members message

Message name	Title	Severity
ESM_SYBASE_GROUP_MEMBER	Group members	Green-0

New groups

The New groups check reports database groups and members that were added to the database after the last snapshot update. Use the name list to include or exclude databases for this check.

[Table 3-38](#) shows the new message for the New groups check.

Table 3-38 New groups messages

Message name	Title	Severity
ESM_SYBASE_NEW_GROUP	New groups	Yellow-2
ESM_SYBASE_NEW_GROUP_MEMBER	New groups	Yellow-2

Deleted groups

The Deleted check reports database groups and members that were deleted to the database after the last snapshot update. Use the name list to include or exclude database names for this check.

[Table 3-39](#) shows the new message for the Deleted groups check.

Table 3-39 Deleted groups messages

Message name	Title	Severity
ESM_SYBASE_DELETED_GROUP	Deleted groups	Yellow-2
ESM_SYBASE_DELETED_GROUP_MEMBER	Deleted groups	Yellow-2

A

About

- Symantec ESM module checks for Sybase 19
- Symantec ESM module for Sybase 13

Account checks

- Deleted logon accounts 21
- Enabled default logon accounts 20
- Logon accounts 20
- New logon accounts 20
- Servers to check 20

Audit checks

- Audit queue size 22
- Audit segments 22
- Auditing enabled 21
- Auditing threshold procedure 22
- Servers to check 21
- Suspend audit when device is full 23
- Truncate transaction log on checkpoint 23

Audit queue size

- Audit checks 22

Audit segments

- Audit checks 22

Auditing enabled

- Audit checks 21

Auditing threshold procedure

- Audit checks 22

Automatically update snapshots

- Object checks 20, 25
- Role and group checks 35

C

Configuration checks

- Configuration parameters 24
- Device status 25
- Master device default status 24
- Servers to check 23
- Version and product level 24

Configuration parameters

- Configuration checks 24

D

Database groups

- Role and group checks 36

Database status

- Object checks 26

Databases to check name list

- Object checks 27

Deleted database

- Object checks 27
- Deleted granted object permissions
 - Object checks 29
- Deleted groups
 - Role and group checks 37
- Deleted logon accounts
 - Account checks 21
- Deleted roles
 - Role and group checks 36
- Device status
 - Configuration checks 25
- Double occurrences
 - Password checks 31

E

- Empty password
 - Password checks 30
- Enabled default logon accounts
 - Account checks 20

G

- Grantable object permissions
 - Object checks 28
- Granted object permissions
 - Object checks 28
- Grantors to check name list
 - Object checks 27
- Group members
 - Role and group checks 36

I

- Installation
 - before you install 15
 - installing the ESM module for Sybase 16

L

- Logon accounts
 - Account checks 20

M

- Master device default status
 - Configuration checks 24
- Minimum password age
 - Password checks 33
- Minimum password length
 - Password checks 32

More information 14

N

Name lists

- Databases to check 27
- Grantors to check 27
- Object actions to check 27
- Object types to check 27
- Objects to check 27

New database

- Object checks 26

New granted object permissions

- Object checks 28

New groups

- Role and group checks 37

New logon accounts

- Account checks 20

New roles

- Role and group checks 35

O

Object actions to check name list

- Object checks 27

Object checks

- Automatically update snapshots 20, 25
- Database status 26
- Databases to check name list 27
- Deleted database 27
- Deleted granted object permissions 29
- Grantable object permissions 28
- Granted object permissions 28
- Grantors to check name list 27
- New database 26
- New granted object permissions 28
- Object actions to check name list 27
- Object permissions 29
- Object types to check name list 27
- Objects to check name list 27
- Servers to check 25
- User access to databases 26

Object permissions

- Object checks 29

Object types to check name list

- Object checks 27

Objects to check name list

- Object checks 27

P

- Password = any login name
 - Password checks 30
- Password = login name
 - Password checks 30
- Password = wordlist word
 - Password checks 31
- Password checks
 - Double occurrences 31
 - Empty password 30
 - Minimum password age 33
 - Minimum password length 32
 - Password = any login name 30
 - Password = login name 30
 - Password = wordlist word 31
 - Password contains a digit 32
 - Plural 31
 - Prefix 32
 - Reverse order 31
 - Role without password 33
 - Servers to check 30
 - Suffix 32
- Password contains a digit
 - Password checks 32
- Patch templates
 - Patch checks 33
- Patches checks
 - Patch templates 33
 - Servers to check 33
- Plural
 - Password checks 31
- Prefix
 - Password checks 32

R

- Reverse order
 - Password checks 31
- Role and group checks
 - Database groups 36
 - Deleted groups 37
 - Deleted roles 36
 - Group members 36
 - New groups 37
 - New roles 35
 - Role grantees 35
 - Roles status 35
 - Servers to check 35
- Role and group checks checks

- Automatically update snapshots 35
- Role grantees
 - Role and group checks 35
- Role without password
 - Password checks 33
- Roles status
 - Role and group checks 35

S

- Servers to check
 - Account checks 20
 - Audit checks 21
 - Configuration checks 23
 - Object checks 25
 - Password checks 30
 - Patches checks 33
 - Role and group checks 35
- Suffix
 - Password checks 32
- Suspend audit when device is full
 - Audit checks 23
- System requirements 15

T

- Truncate transaction log on checkpoint
 - Audit checks 23

U

- User access to databases
 - Object checks 26

V

- Version and product level
 - Configuration checks 24

