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

Release 3.0 for Symantec ESM 6.5.x and 9.0.1 For Sybase Adaptive Server Enterprise on AIX, HP-UX, Linux, and Solaris

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

Documentation version: 3.0

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

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 assurance and maintenance contracts
- Information about the Symantec Buying Programs
- 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	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	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 is 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.

Contents

Chapter 1

Introducing Symantec ESM modules for Sybase Adaptive Server Enterprise

This chapter includes the following topics:

About the Symantec ESM modules for Sybase ASE

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

These modules implement the checks and options that 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 ASE 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 server in the same way that you use for other Symantec ESM modules.

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

You can use the ESM Application modules to scan the Sybase ASE servers for reporting vulnerabilities.

You can perform the following tasks using the ESM console:

- 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.

Template

Several of the documented modules use templates to store the Sybase ASE parameters and object settings. Differences between the current settings and template values are reported when the modules run. Modules use templates to store Sybase ASE parameters and object settings.

Table 1-1 Template name

Module	Check name	Template name	Predefined template
Sybase ASE Auditing	Procedure Audit Options	Sybase Procedure Audit Options	none
	Object Audit Options	Sybase ASE Object Audit Options	none
	Login Audit Options	Sybase ASE Login Audit Options	none
	Database Audit Options	Sybase Database Audit Options	none
	Global Audit Options	Sybase ASE Global Audit Options	none

Table 1-1 Template name *(continued)*

Module	Check name	Template name	Predefined template
Sybase ASE Configuration	Configuration Parameters	Sybase Configuration Parameter	none
	Device Status	Sybase ASE Device Status	none
Sybase ASE Object	Object Permission	Sybase ASE Object Permissions	none
	Exclude granted object perm	Sybase Granted object perm	excludegrantedobj perm.gop
	Stored procedure signature	Sybase Stored Procedure Signatures	none
Sybase ASE Patches	Patch templates	Sybase ASE Patch	sybasepatch.syq
Sybase ASE Password Strength	Password complexity parameters	Sybase Password Parameter	none

Where you can get more information

For more information about Symantec ESM modules and Security Updates, see the latest versions of the *Symantec Enterprise Security Administrator's Guide* and the *Symantec ESM Security Update User's Guide*.

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: Security Response Web site

Chapter 2

Installing Symantec ESM modules for Sybase ASE

This chapter includes the following topics:

Before you install

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

- Ensure that Sybase ASE client is installed on the same ESM agent computer that the Sybase ASE module should report on.
- Ensure that connectivity to all Sybase ASE servers is established. There must be a valid interfaces file at the following location on the ESM agent computer:

`/<sybase installed directory>/interfaces`

The interfaces file contains the names of the Sybase ASE servers and the ports on which it is running.

- Log on as root to install the esmsyb.tpi.
  If you want to use a non-root account for installation, See "About using an alternate account" on page 16..

About using an alternate account

In the previous releases, the root user logged on to the ESM agent computer to install and configure the ESM modules for Sybase ASE. In the current release, the non-root (alternate account) users can install and configure the ESM modules for Sybase ASE after the root has changed the ownership of the tpi and the SybaseSetup.

The root must change the ownership of the esmsyb.tpi, before the non-root user runs the esmsyb.tpi installer.

To change the ownership of the esmsyb.tpi

1. Log on to the ESM agent computer as the root.
2. Copy the esmsyb.tpi to the desired location on the same ESM agent computer.
3. Create a new group.

   The non-root user should be a member of the new group.
4. To change the ownership of the esmsyb.tpi from root group to another group, type the following at the command prompt:

   ```
   chown root: <group> esmsyb.tpi
   ```
5. To apply setuid bit to esmsyb.tpi, type the following at the command prompt:

   ```
   chmod 4750 esmsyb.tpi
   ```

   The users of the specified group are assigned the root's privileges to use the esmsyb.tpi.

To install esmsyb.tpi as a non-root user

1. Log on to the ESM agent computer as a non-root user.
2. Run the esmsyb.tpi to install the ESM modules for Sybase ASE.

See "Installing the ESM modules for Sybase ASE" on page 21.

See "Silently installing the ESM modules for Sybase ASE" on page 25.

The root must change the ownership of the SybaseSetup, before the non-root user configures ESM modules for Sybase ASE by using the SybaseSetup.

To change the ownership of the SybaseSetup

1. Log on to the ESM agent computer as the root.
2. From the `/esm/bin/<platform>` directory, copy the SybaseSetup to the desired location on the same ESM agent computer.
3. To change the ownership of the SybaseSetup from root group to another group, type the following in the command prompt:

   `chown root: <group> SybaseSetup.`

   The users of the specified group are assigned the root privileges to use the SybaseSetup.
4. To apply setuid bit to the SybaseSetup, type the following in the command:

   `chmod 4750 SybaseSetup.`

To configure ESM modules for Sybase ASE by using SybaseSetup as a non-root user

1. Log on to the ESM agent computer as a non-root user.
2. Run the SybaseSetup to configure the Sybase ASE servers.

See "Configuration of the ESM modules for Sybase ASE" on page 26.

See "Silently configuring the ESM modules for Sybase ASE" on page 28.

System requirements

Table 2-1 list the supported Sybase ASE versions and operating systems on which the ESM application modules for Sybase ASE can report.

Note: As per Symantec's End of Life product support policy, the ESM Modules for Sybase ASE are not supported on ESM 6.0.

Table 2-1 Supported Sybase ASE versions and operating systems

Supported operating systems	Architecture	Supported OS versions	Supported Sybase versions
AIX (32-bit)	RS 6000	5.2	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2
AIX (64-bit)	PPC 64	5.3, 6.1	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2, 15.0.3

Table 2-1 Supported Sybase ASE versions and operating systems *(continued)*

Supported operating systems	Architecture	Supported OS versions	Supported Sybase versions
Sun Solaris (32-bit and 64-bit)	SPARC	2.8, 2.9, 2.10	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2, 15.0.3
HP-UX (32-bit and 64-bit)	PARISC	11.11, 11.23, 11.31	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2
HP-UX (64-bit)	Itanium®	11.23	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2
Red Hat Enterprise Linux AS (32-bit and 64-bit)	x86, x64	3, 4	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2
Red Hat Enterprise Linux ES (32-bit and 64-bit)	x86, x64	3, 4, 5.0, 5.1, 5.2, 5.3	12.5.2, 12.5.4, 15.0.0, 15.0.1, 15.0.2

Note: You can use HPUX-Itanium only in a network-based environment. You can use the other operating systems in a network-based and host-based environment.

See "About configuring the Sybase ASE in a network-based environment" on page 27.

To install the ESM modules for Sybase ASE, you must have the following free disk space:

Table 2-2 Disk space requirements

Supported operating systems	Architecture	Supported OS Version	Disk space
AIX (32-bit)	RS 6000	5.2	57 MB
AIX (64-bit)	PPC 64	5.3, 6.1	71 MB
Sun Solaris (32-bit and 64-bit)	SPARC	2.8,2.9,2.10	26 MB

Table 2-2 Disk space requirements *(continued)*

Supported operating systems	Architecture	Supported OS Version	Disk space
HP-UX (32-bit and 64-bit)	PARISC	11.11, 11.23, 11.31	51 MB
Red Hat Enterprise Linux AS (32-bit and 64-bit)	x86, x64	3, 4	31 MB
Red Hat Enterprise Linux ES (32-bit and 64-bit)	x86, x64	3, 4, 5.0, 5.1, 5.2, 5.3	31 MB

About using parameters in the esmsybaseenv.dat file

This table lists the different parameters that you can use in the esmsybaseenv.dat file to work with the Sybase ASE modules.

Table 2-3 Parameters and their usage

Parameter name	Description	Parameter value	Example
SymEsmDbaRoles	You can use this parameter to grant roles to the SYMESMDBA account while configuring the Sybase ASE.	The default roles are the sa_role and the sso_role. Apart from the default roles, you can assign any roles. You can add this parameter to the `esmsybaseenv.dat` file as config SymEsmDbaRoles <name of new roles>.	config SymEsmDbaRoles <role 1, role 2,...>

Table 2-3 Parameters and their usage *(continued)*

Parameter name	Description	Parameter value	Example
PassSpecString	You can use this parameter to specify the special characters that you can use while generating the password for the configured account.	The default special characters are the underscore (_) and the hash (#). The other special characters that you can use are $@%. You can add this parameter to the `esmsybaseenv.dat` file as config PassSpecString <special characters>.	config PassSpecString $@%
PassChangedPeriod	You can use this parameter to specify the period after which you want to change the password of the configured account.	If you want to change the password of your configured account then you set the Password expiration interval setting parameter to 0. If you do not specify any value then by default the value is 35 days. You can add this parameter to the `esmsybaseenv.dat` file as config PassChangedPeriod <number of days>.	config PassChangedPeriod 30

Table 2-3 Parameters and their usage *(continued)*

Parameter name	Description	Parameter value	Example
PrecreatedNoPassChange	You can use this password to not to change the password of the pre-created account.	If you do not want to change the password of your configured account then you set the PrecreatedNo PassChange parameter to 1. This value is not set by default.	config PrecreatedNoPassChange parameter to 1
UsingTimeout	You can use the parameter to specify the timeout period if the Sybase ASE server is unable to complete the request within the specified time.	If you set the default value to 0, the Sybase ASE server never times out. You can add this parameter to the `esmsybaseenv.dat` file as config UsingTimeout <number of seconds>.	config UsingTimeout 50

See "Installing the ESM modules for Sybase ASE" on page 21.

See "Configuring the Sybase ASE server by using the Sybase ASE Discovery module" on page 29.

Installing the ESM modules for Sybase ASE

You can install the Sybase ASE module on the ESM agent computer by using the esmsyb.tpi.

You must have SU 23 or later installed on the ESM agent computer before you install the ESM modules for Sybase ASE.

The installation program does the following:

- Extracts and installs module executables, configuration (.m) files, and the template files.
- Registers the .m and the template files by using the ESM agent's registration program.

Note: If you register the .m files during a module installation on an agent that is installed on the same platform, then you do not have to re-register the .m files again.

- Launches the SybaseSetup program to create the SYMESMDBA account for reporting.
  The password for the SYMESMDBA account is 12 characters long and is generated randomly. The password is encrypted by using a 256-bit AES encryption algorithm and is stored in the `/esm/config/SybaseModule.dat` file.

  Note: The SYMESMDBA account can perform only the Read operations.

- Grants the following default roles to SYMESMDBA account:
  - sa_role
  - sso_role
    You can either grant one role or multiple roles. You can grant a role in the following way:
    - Add a parameter "config SymEsmDbaRoles <name of new roles>" entry to the `esmsybaseenv.dat` file.
      You can use a comma or a space to separate the multiple roles.

      Note: The `esmsybaseenv.dat` file does not exist by default and you must create it manually.

- Auto-generates the password for the reporting account. The ESM modules for the Sybase ASE considers the following parameters during auto-generation of the passwords :
  - PassChangedPeriod
    The "PassChangedPeriod" parameter specifies the number of days after which you want to change the password of the configured account.
    If you set the "Password expiration interval" setting of the configured account to 0, the password changes after every policy run.
  - PrecreatedNoPassChange
    If you do not want to change the password of your pre-created account then you set the PrecreatedNoPassChange parameter to 1.

This value is not set by default. Periodically, you must manually change the pre-created account password that you have configured.

- PassSpecString
  The password must contain at least one upper-case, one lower-case, one numeric character (0-9), and one special character. The default special characters are the underscore (_) and the hash (#). If you want to use other special characters, you can also add a parameter ''config PassSpecString $@%" entry into the /esm/config/esmsybaseenv.dat file before you run the Sybase configuration.

Note: If you change the password for the pre-created account then you must modify the records by using the `/esm/bin/<platform>/SybaseSetup`.

To install the ESM modules for Sybase ASE

1. From the product disc, run the /DATABASES/Sybase/Modules/<architecture>/esmsyb.tpi.

   You can also download and copy the esmsyb.tpi from the Security Response Web site to the desired location.

2. Choose one of the following option:

Option 1	To display the contents of the package.
Option 2	To install the module.

3. The 'Do you wish to register the template or .m files?' message appears. Do one of the following:
   - Type a Y, if the files are not registered with the manager.
   - Type an N, if the files have already been registered and skip to See "To configure for the Sybase ASE servers on the ESM agent computers" on page 24.

Note: You must register the template and the .m files once for the agents that use the same manager on the same operating system.

---

4. Enter the ESM manager that the agent is registered to.

   Usually, it is the name of the computer that the manager is installed on.

5. Enter the ESM access name (login name) for the manager.

6 Enter the ESM password that is used to log on to the ESM manager.

7 Enter the network protocol that is used to contact the ESM manager.

8 Enter the port that is used to contact the ESM Manager. The default port is 5600.

9 Enter the name of the agent as it is currently registered to the ESM manager.

Usually, it is the name of the computer that the agent is installed on.

10 The 'Is this information correct?' message appears. Do one of the following:

- Type a Y, the agent continues with the registration to the ESM manager.
- Type an N, the setup prompts to re-enter the details of the new manager.

When the extraction is complete, you are prompted to add configuration records to enable the ESM security checking for your Sybase ASE.

11 The 'Continue and add configuration records to enable ESM security checking for your Sybase ASE? [yes]' message appears. Do one of the following:

- Type a Y, to configure the Sybase ASE module on the agent computer.
  If you have typed a Y, the installation program reads the existing configuration records and displays them.
- Type an N, the program installation continues without configuration.

To configure for the Sybase ASE servers on the ESM agent computers

1 To add a configuration record for the Sybase ASE server, do the following:

- Enter the Sybase path.
  You must specify the path where you have installed the Sybase ASE on the ESM agent computer.
- Enter the SYBASE_OCS directory in Sybase path [OCS-XX_0]: default OCS path.
  The ESM for Sybase ASE servers module installation program displays the existing Sybase ASE servers that are found in the OCS path that you provide.

2 The ‘Would you like to add a configuration record for this server’ “Server name”? message appears [yes]. Do the following:

- Enter the sa or pre-created login for server “Server name” [sa]:
- Enter the password that is used to log on to the “Server name” server:
- Re-Enter password:

The sa account creates the SYMESMDBA login account to perform the security checks and then displays the login information of the SYMESMDBA account.

3 The 'Is this information correct?' message appears. Do one of the following:

- Type a Y, to continue and add configuration records to enable the ESM security checking for your Sybase ASE.
- Type an N, to re-enter the configuration information.

After the setup completes the configuration for the first detected Sybase ASE server, you are prompted to configure the other detected Sybase ASE servers.

4 The 'Would you like to add a configuration record for this server "Server name"? [yes] message appears. Do the following:

- Type a Y, to add another server record.

5 The 'Would you like to continue for another Sybase path?' [no] message appears.

If you type an N, the configuration exits and the setup continues with the installation program. After you have created the configuration records for each Sybase ASE server, the program lists all of the configuration records.

6 The 'Do you wish to push the report content file [no]? message appears'. Do the following:

- Type a Y, to push the RDL package to the manager.
- Type an N, to exit the program.

Note: The encryption that is used to store the credentials for reporting is 256-bit AES encryption algorithm.

Silently installing the ESM modules for Sybase ASE

You can silently install the ESM modules for Sybase ASE by using the esmsyb.tpi.

Table 2-4 lists the command line options for silently installing the ESM modules for Sybase ASE.

Table 2-4 Options to silently install the ESM modules for Sybase ASE

Option	Description
-i	Install this tune-up/third-party package.

Table 2-4 Options to silently install the ESM modules for Sybase ASE *(continued)*

Option	Description
-d	Display the description and contents of this tune-up/third-party package.
-U	Specify the ESM access record name.
-e	Do not execute the before and after executables (installation without configuration).
-P	Specify the ESM access record password.
-p	Specify the TCP port to use.
-m	Specify the ESM manager name.
-t	Connect to the ESM manager by using TCP.
-x	Connect to the ESM manager by using IPX (Windows only).
-g	Specify the ESM agent name to use for registration
-K	Do not prompt for and do the re-registration of the agents.
-n	No return is required to exit the tune-up package (Windows only).
-N	Do not update the report content file on the manager.
-Y	Update the report content file on the manager.

To silently install the ESM modules for Sybase ASE without configuration

- At the command prompt, type the following:

```
./esmsyb.tpi -it -m <Manager Name> -U <Username> -p <port> -P
<password>-g <Agent Name> -e
```

If the installation succeeds, the return value is 0. If the installation fails, the return value is 1.

Configuration of the ESM modules for Sybase ASE

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

Note: Before a policy run, you must configure the ESM modules for Sybase ASE related information and credentials for the application modules to report on. You can use a pre-created account or an sa account. With an sa account, ESM uses a SYMESMDBA account for reporting. Pre-created account is a non-sa account that you can create before the configuration.

Editing configuration records

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\<platform>\`.

Table 2-5 lists the options that you can use when running the SybaseSetup.

Table 2-5 Editing configuration records

Type	To do this
SybaseSetup -h	Display help.
SybaseSetup -c	Create configuration records for detected Sybase ASE servers.
SybaseSetup -a	Add a new configuration record for undetected Sybase ASE servers.
SybaseSetup -m	Modify existing Sybase ASE configuration records.
SybaseSetup -l	List existing Sybase ASE configuration records.
SybaseSetup -G	Add configuration records for the generic credentials.

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

About configuring the Sybase ASE in a network-based environment

You cannot install the ESM application modules for Sybase ASE on the HP-UX Itanium ESM agent computers. Instead, these agents must be queried from a remote ESM agent computer on a different platform that is supported for the ESM application modules for the Sybase ASE.

To report on a Sybase ASE in a network-based environment

1. Copy the Sybase ASE server and port information from the network-based Sybase ASE server interfaces file `/<Sybase Installed Directory>/interfaces` to the interfaces file that is present on the host-based Sybase ASE server.

   You must ensure that you can connect to the network-based Sybase ASE server by using the isql utility on the host-based Sybase ASE server.

2. Configure the host-based Sybase ASE server by using the SybaseSetup utility.

Note: You cannot use the Sybase ASE Discovery module to configure the network-based Sybase ASE server.

Silently configuring the ESM modules for Sybase ASE

You can silently configure the ESM modules for Sybase ASE by using the SybaseSetup. You can find the SybaseSetup at `/esm/bin/<OS architecture>/SybaseSetup`.

Table 2-6 lists the command line options for silently configuring the ESM modules for Sybase ASE.

Table 2-6 Options to silently configure the ESM modules for Sybase ASE

Option	Description
-h	Display help.
-a	Add a new configuration record for undetected Sybase ASE.
-n	Do not delete the existing SYMESMDBA account during configuration. **Note:** This is an optional switch.
-S <sybase dir>	Directory path of Sybase ASE.
-O <OCS dir>	Directory of Sybase OCS.
-A <account>	The sa login for Sybase ASE server to create SYMESMDBA account, or pre-created account for ESM to perform checks.
-P <password>	The password for Sybase ASE server login.

Table 2-6 Options to silently configure the ESM modules for Sybase ASE *(continued)*

Option	Description
-gif	Specify the file name that contains the encrypted generic credential record.
-gof	Specify the file name that should be created with the encrypted generic credentials record.
-ng	Use this option with -gif option. If you select the option and if at the same time, you replace the generic pre-created credentials with 'sa' credentials then all the records that are configured to use generic pre-created credentials are deleted from the configuration file.

Note: If you do not specify any option then ./SybaseSetup runs with the -h option.

To silently configure the ESM modules for Sybase ASE

- At the command prompt, type the following:

```
./SybaseSetup -a <SID> -S <sybase dir> -O <OCS dir> -A <account>
-P <password>
```

If the configuration succeeds, the return value is 0.

If the configuration fails, the return value is 255.

After you have run the SybaseSetup, the logs are created in `/esm/system/<hostname>/ EsmSybaseConfig.log`.

Configuring the Sybase ASE server by using the Sybase ASE Discovery module

The host-based Sybase ASE Discovery module automates the detection and configuration of new Sybase ASE servers that are not yet configured on the ESM agent computers. The Sybase ASE Discovery module also detects and automatically removes the deleted or the unreachable Sybase ASE servers.

You can configure the Sybase ASE servers by using the generic credentials. The generic credentials are the common Sybase ASE credentials that you can use across servers. The generic credentials can be a “sa” account or a pre-created account. If you use a “sa” account then a SYMESMDBA account is created on every server and is used for reporting.

If you use a pre-created account then you can add the new configuration option PrecreatedNoPassChange 1 in the esm/config/esmsybaseenv.dat file.

For more information on the PrecreatedNoPassChange parameter, See "Installing the ESM modules for Sybase ASE" on page 21.

Configuring a new Sybase ASE server

To report on the Sybase ASE server, you must first configure the Sybase ASE server on an ESM agent computer. The configuration helps the ESM application modules for Sybase ASE to understand which servers the module should report on.

To configure a new Sybase ASE server

1. Run the Sybase ASE Discovery module on the ESM agent computer that has the Sybase ASE server installed.

   The module lists all the new Sybase ASE servers that were not configured earlier.

2. Select multiple Sybase ASE servers and do one of the following:

   - Right-click and select **Correction** option.
     The Correction option configures the Sybase ASE servers with the server credentials. When you enter the pre-created credentials the server is configured using the pre-created credentials. When you enter the "sa" credentials the SYMESMDBA is created. However, if you are using the pre-created credentials then SYMESMDBA is not created.
   - Right-click and select **Snapshot Update** option.
     The Snapshot Update option configures the Sybase ASE servers with generic credentials. Before you select the Snapshot Update option, you must first configure the generic credentials.See "Configuring Sybase ASE with generic credentials" on page 32.

To configure a new Sybase ASE server automatically

1. Enable the check **Automatically add new Sybase ASE server**.

   The check automatically configures the newly discovered Sybase ASE server in the configuration file `/esm/config/SybaseModule.dat`. The check uses the generic credentials and attempts to connect to the server. After each successful connection, the Sybase ASE Discovery module adds a configuration record in the configuration file. If the connection attempt fails then the module returns a correctable message.

2. To use the **Correctable** option

   - Right-click on the message.

- Choose **Correction** option.
  You are prompted to enter the credentials to connect to the server again.
  Do one of the following
  - Enter pre-created credentials.
    The Sybase ASE server is configured using the pre-created credentials.
  - Enter “sa” credentials.
    The SYMESMDBA account is created.

Validating Sybase ASE server credentials

The **Validate configuration** check uses the configured credentials and connects to the server.

The module does the following:

- Checks whether the configured account is unlocked.
- Checks for the assigned roles of the configured account.

If the SymEsmDbaRoles parameter is configured in the `esmsybaseenv.dat` file then the module checks for the defined roles. By default the module checks for the “sa” and the “sso” roles.

If the validation of the SYMESMDBA account fails and the generic credentials are present then the SYMESMDBA account is recreated. For pre-created account, the module returns a correctable message. When the server is configured using pre-created account, auto-correction is not supported.

To use the Correction option

1. Right-click on the message.
2. Select **Correction** option.

   You are prompted to enter the credentials to connect to the server again. Do one of the following:
   - Enter the sa credentials.
     The SYMESMDBA account is recreated. This SYMESMDBA account is unlocked and the required roles are assigned to it.
   - Enter the pre-created credentials.
     The server is configured with the pre-created credential

See “Validate configuration” on page 41.

Configuring Sybase ASE with generic credentials

You can configure a new Sybase ASE server on an ESM agent computer by using a generic credential. The generic credential option helps you to configure a common Sybase ASE server credential for all the Sybase ASE servers on an ESM agent computer.

To specify generic credentials

1. On the command prompt , type SybaseSetup –G.
2. Enter the Generic Login ID: User name.
3. Enter a password for the generic login. Reconfirm the password.
4. Press Enter.

   The generic credentials are configured in the `SybaseModule.dat` file.

If you have a pre-created account configured and you want to replace it with an sa account then the setup returns a message warning that the records that were configured to use the pre-created generic credentials will be removed.

If you enter YES, the setup does the following:

- Removes the records that were configured to use the pre-created generic credentials.
- Replaces the generic credentials.
  You must run the Sybase ASE Discovery module again.

Reusing generic credentials of a Sybase ASE

If you want to specify a common generic credential on multiple ESM agent computers it is not necessary to use SybaseSetup –G option on every ESM agent computer. Instead, you can use -gif and -gof options to specify a generic credential. The specified generic credential is then stored in an encrypted format in a file that can be reused on every ESM agent computer.

To specify generic credentials

1. On the command prompt, type SybaseSetup -gof <filepath>

   For example: SybaseSetup -gof < /esm/bin/<platform>/pass.dat>.
2. Enter the Generic Login ID: User name.
3. Enter a password for the generic login. Reconfirm the password.
4. Press Enter.

   The `pass.dat` file is created with the encrypted generic credentials that are specified in Step 1.

To reuse generic credentials

1. Copy the `pass.dat` file on a Sybase ASE ESM agent computer where you want to import the generic credentials.
2. On the command prompt, type SybaseSETUP -gif <filepath>

   The generic credentials are imported in the `SybaseModule.dat` file.

See "Configuring a new Sybase ASE server" on page 30.

Removing unreachable or deleted servers

Although, you may have deleted a Sybase ASE server, the configuration information still exists in the configuration file `/esm/config/SybaseModule.dat`. The Sybase ASE Discovery module when executed removes the configuration information of such Sybase ASE servers.

To remove unreachable or deleted servers manually

1. Run the Sybase ASE Discovery module on the target ESM agent computers. The module lists all the unreachable and the deleted Sybase ASE servers that were configured earlier.
2. Select multiple Sybase ASE servers right-click, and select **Snapshot Update** option. The Snapshot Update option removes the configuration information of such Sybase ASE servers.

To remove unreachable or deleted servers automatically

- Enable the check **Automatically remove deleted Sybase ASE servers**. The module automatically removes the corresponding server records from the configuration file `/esm/config/SybaseModule.dat`.

About the Logging functionality on the Sybase ASE modules

The logging feature in the Sybase ASE modules enables the ESM agent to log the information, such as errors and exceptions that a module generates at the run time. This feature is currently enabled for the Sybase ASE Discovery module.

About the log levels of the messages

The ESM log level specifies the type and criticality of a message. You can manually create a configuration file on the ESM agent computer and specify the log level messages that you want to be logged.

ESM checks the log level that you set in the configuration file and stores only the qualifying messages in the log file.

See "Creating the configuration file" on page 35.

You can specify the following log levels:

ESM_LOG_ERROR	All errors are logged. The following are some examples of the errors: ■ Template file not found ■ Configuration file not found
ESM_LOG_WARNING	All warnings are logged.
ESM_LOG_INFORMATION	All information messages are logged. The information that is gathered during a policy run is also logged at this level. **Note:** When you enable the ESM_LOG_INFORMATION level, the performance of the module may be affected because all the information messages are logged.
ESM_LOG_TRACE	All debug information is logged.
ESM_LOG_MAXIMUM	Includes all log levels except ESM_NO_LOG.
ESM_NO_LOG	Disable logging for the module.

You specify the log level in the LogLevel parameter of the configuration file. For example, to log the messages that are related to critical failures, specify the log level as follows:

[sybasediscovery_LogLevel] = ESM_LOG_TRACE

You can also specify multiple log levels by separating them with a pipe (|) character as follows:

[sybasediscovery_LogLevel] = ESM_LOG_INFORMATION|ESM_LOG_ERROR

You can use log levels for specific operations as follows:

For regular policy runs	ESM_LOG_INFORMATION and ESM_LOG_ERROR
To generate detailed logs for policy failure	ESM_LOG_INFORMATION, ESM_LOG_ERROR, and ESM_LOG_TRACE

Creating the configuration file

You can create a configuration file named esmlog.conf in the <esm_install_dir>/config folder on the ESM agent computer and specify the values that ESM uses to store the logs of a module.

To create the configuration file

1. Change to the <esm_install_dir>/config folder.
2. Create a new text file and specify the parameters and their values.
3. Save the text file as esmlog.conf.

See "Parameters of the configuration file" on page 35.

The following is an example of the entries in the configuration file:

[MaxFileSize] = 1024

[NoofBackupFile] = 20

[LogFileDirectory] = <esm_install_dir>/system/agentname/logs

[sybasediscovery_LogLevel] = ESM_LOG_INFORMATION|ESM_LOG_TRACE

[sybasediscovery_LogLevel] = ESM_LOG_INFORMATION

Note: No default configuration file is shipped with the Sybase ASE modules. You need to manually create the file and specify the parameters in it.

Parameters of the configuration file

Table 2-7 lists the parameters that you need to specify in the configuration file.

Table 2-7 Configuration file parameters

Parameter name	Description	Range of values	Default value
[MaxFileSize]	Specify the maximum file size for the log file in MB	1 MB to 1024 MB (1 GB)	1 MB

Table 2-7 Configuration file parameters *(continued)*

Parameter name	Description	Range of values	Default value
[NoOfBackupFile]	Specify the number of backup files of the logs that can be stored per module. For example, if the value of NOOFBACKUPFILE is 3, then ESM stores a maximum of 3 backup files for the module.	0 to 20	1
[LogFileDirectory]	Specify the absolute path to store the log file and backup log files.	N/A	The directory /esm/system/ <hostname>/tmp/
[<module>_LogLevel]	Specify the log level along with the short name of the module. For example, to log all error messages for the Sybase ASE Discovery module, specify the following: [sybasediscovery_ LogLevel] =ESM_LOG_ERROR	N/A	ESM_LOG_ERROR

If the configuration file `esmlog.conf` is not present then the logging functionality appears to be disabled and no logs are generated.

About the ESM agent log file

The ESM agent computer now stores the log file `esmlog.conf` of the modules in the directory that the user specifies. If the directory that the user specifies does not exist, then the module first creates the directory and then stores the log files in it.

The log file has the following format:

<module_name>.log

The <module_name> is the short name of the module. For example, the log file of the Sybase ASE Discovery module is named sybasediscovery.log. The backup file name for Sybase ASE Discovery module is named sybasediscovery.log_1.bak and so on.

Note: During the process of logging, ESM locks the log file to store the logging information. If the log file is open at that time, the information about the logs may be lost.

Format of the log file

A log file contains the following fields:

Serial Number	Serial number of the log file entry The serial number is displayed in hexadecimal format. The serial number is reset in the next policy run on the module.
Thread ID	Thread identifier of the process that generated the message
Source File Name	Name of the source file that generates the message.
Line Number	Line number in the source file from where the message generates
Date	Date on which the log was created
Time	Time at which the log was created
Message	The actual message that was generated along with the log level of that message.

About the backup of logs

When the log file reaches a specified size limit, ESM backs up the log file. This size limit is configurable and you can specify it in the MaxFileSize parameter of the configuration file.

If the log file reaches the MaxFileSize value, ESM creates a backup of the log file depending on the NoofBackupFile value that is specified in configuration file. For example, if the NoofBackupFile value is 0, ESM overwrites the existing log file, if any, for the module.

Chapter 3

Symantec ESM module checks for Sybase ASE

This chapter includes the following topics:

About Symantec ESM module checks for Sybase ASE

By default, the checks are disabled when you install the module. To enable the checks, right-click on a policy and select **Properties**. The **Properties** dialog box is displayed. See the *Symantec Enterprise Security Manager Administrator's Guide* for more information on using module properties.

Sybase ASE Discovery

The checks in the Sybase ASE Discovery module automate the detection and configuration of new Sybase ASE servers that are not yet configured on the ESM agent computers. The Sybase ASE Discovery module also detects and automatically removes the deleted Sybase ASE servers from the `/esm/config/SybaseModule.dat` configuration file.

Note: The Sybase ASE Discovery module detects the new servers when you start the database server with the full path and use the option `-s <servername>`. For example, `/opt/sybase/ASE-12_5/bin/dataserver -sSYBASESERVER`.

Detect new database server

This check reports the Sybase ASE servers that are newly detected on the ESM agent computers and that were not configured earlier.

Table 3-1 lists the message output for the Detect new database server check.

Table 3-1 Detect new database server message

Message name	Title	Severity
ESM_SYBASE_NEW_ DB_SERVER_DETECTED	New Database Server	yellow-1

Detect deleted database server

This check reports the Sybase ASE servers that are deleted or unreachable but are still configured in the `/esm/config/SybaseModule.dat` configuration file.

Table 3-2 lists the message output for the Detect deleted database server check.

Table 3-2 Detect deleted database server message

Message name	Title	Severity
ESM_SYBASE_DEL_ DB_SERVER_DETECTED	Deleted Database Server	yellow-1

Automatically add new database server

This check works with the **Detect new database server** check. The check **Automatically add new database server** uses the generic credentials to automatically configure the newly detected Sybase ASE servers.

Table 3-3 lists the message output for the Automatically add new database server check.

Table 3-3 Automatically add new database server message

Message name	Title	Severity
ESM_SYBASE_NEW_ DB_SERVER_ADDED	Added New Database Server	yellow-1
ESM_SYBASE_ADD_ DB_SERVER_FAILED	Failed to Add New Database	yellow-1

Automatically remove deleted database server

This check works with the **Detect deleted database server** check to automatically remove the deleted or the unreachable Sybase ASE server records from the `/esm/config/SybaseModule.dat` configuration file.

Table 3-4 lists the message output for the Automatically remove deleted database server check.

Table 3-4 Automatically remove deleted database server message

Message name	Title	Severity
ESM_SYBASE_DEL_ DB_SERVER_DETECTED	Deleted Database Server	yellow-1

Validate configuration

This check validates the entries of the configuration records for successful connection and assigned roles. The Sybase ASE Discovery module automatically corrects the accounts, if the generic credential that is used is sa and the configuration record entry is SYMESMDBA.

Table 3-5 lists the message output for the Validate configuration check.

Table 3-5 Validate configuration message

Message name	Title	Severity
ESM_SYBASE_ CREDENTIALS_VERIFIED	Server validation successful	yellow-1
ESM_SYBASE_ CREDENTIALS_FAILED	Sybase validation failed	yellow-1
ESM_SYBASE_ CREDENTIALS_RECTIFIED	Sybase server credentials rectified	yellow-1
ESM_SYBASE_CREDENTIALS_ ROLES_FAILED	Sybase server credentials roles validation failed	yellow-1

Sybase ASE Account

The checks in the Sybase ASE Account module evaluate the account settings of the Sybase ASE server. The checks report on the accounts that are found to be new or deleted.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes. Use the name list to include or exclude the Sybase ASE servers for all the Sybase ASE Account checks.

Automatically update snapshots

Enable this check to automatically update the snapshots with the current information.

Unlocked default logon accounts

This check reports the default logon accounts that should be locked. Use the name list to include the default logon accounts that you want the check to report on. If the name list is left empty the check reports no problems found.

Table 3-6 lists the new message for the Unlocked default logon accounts check.

Table 3-6 Unlocked default logon accounts message

Message name	Title	Severity
ESM_SYBASE_DEFAULT_LOGON_ACCOUNT	Unlocked default logon account	Yellow-2

Logon accounts

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

Table 3-7 lists the new message for the Logon accounts check.

Table 3-7 Logon accounts message

Message name	Title	Severity
ESM_SYBASE_LOGON_ACCOUNTS	Logon accounts	Yellow-2

New logon accounts

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

Table 3-8 lists the new message for the New logon accounts check.

Table 3-8 New logon accounts message

Message name	Title	Severity
ESM_SYBASE_NEW_LOGON_ACCOUNTS	New logon accounts	Yellow-2

Deleted logon accounts

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

Table 3-9 lists the new message for the Deleted logon accounts check.

Table 3-9 Deleted logon accounts message

Message name	Title	Severity
ESM_SYBASE_DELETED_LOGON_ACCOUNT	Deleted logon accounts	Yellow-2

Database user aliases

This check reports the aliases of the database users that are present on the server. Use the name list to include or exclude the database users whose aliases you want to report.

Table 3-10 lists the new message for the Database user aliases check.

Table 3-10 Database user aliases message

Message name	Title	Severity
ESM_SYBASE_ALIAS	Alias of the Database user	Yellow-2

Login triggers

This check reports the Sybase ASE logins that have login triggers assigned to them and the global login trigger defined on the Sybase ASE server. Use the name list to include or exclude the login names that the check should report on.

The Global login trigger is useful when you want all the logins to apply the same login trigger.

The login triggers that the check reports are the ASE stored procedures. These stored procedures are automatically executed in the settings when you successfully log on to the Sybase ASE server.

Table 3-11 lists the new message for the Login triggers check.

Table 3-11 Login triggers message

Message name	Title	Severity
ESM_SYBASE_GLOBAL_TRIGGER	Global login trigger	Yellow-2
ESM_SYBASE_LOGIN_TRIGGER	Login trigger	Yellow-2

The following table lists the messages the check reports on different versions:

Sybase ASE all versions	ESM_SYBASE_LOGIN_ TRIGGER
Sybase ASE 12.5.4 and later and 15.0.2 and later versions	ESM_SYBASE_GLOBAL_ TRIGGER

Inactive accounts

This check reports the unlocked Sybase ASE logins that have not logged on to the server for more than the days that are specified in the **Days since last login** text box. Use the name list to include or exclude the login names that the check should report on. Sybase ASE 15.0.2 and later supports this check.

Enable the configuration parameter 'enable the last login updates.'

The check also reports those login accounts that do not have an entry against the last login date parameter but were created earlier than the days specified. Moreover, the check reports those login accounts as inactive whose last login date parameter indicates that there has been no login to the server for more than the days specified.

An inactive account is an easy target for those who can break into your system. Hence, you should remove or disable all inactive accounts.

Note: If you specify 0 in the **Days since last login** text box, the check overlooks that value and by default reports on 30 days.

Table 3-12 lists the new message for the Inactive accounts check.

Table 3-12 Inactive accounts message

Message name	Title	Severity
ESM_SYBASE_LAST_ LOGIN_UPDATE	Last login update not enabled	Yellow-2
ESM_SYBASE_INACTIVE_ ACCOUNT	Inactive account	Red-4

Accounts with system roles

This check reports the accounts that have both the sa_role and sso_role assigned to them. Use the name list to include or exclude the login names that the check should report on.

Table 3-13 lists the new message for the Accounts with system roles check.

Table 3-13 Accounts with system roles message

Message name	Title	Severity
ESM_SYBASE_SA_SSO_ROLE	Account with system roles	Red-4

Accounts with default master database

This check reports the accounts that have master as their default database. Use the name list to include or exclude the login names that the check should report on.

Table 3-14 lists the new message for the Accounts with default master database check.

Table 3-14 Accounts with default master database message

Message name	Title	Severity
ESM_SYBASE_DEFAULT_DB_MASTER	Accounts with default master database	Red-4

Sybase ASE Auditing

The checks in the Sybase ASE Auditing module validate the audit settings of the Sybase ASE server.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Auditing enabled

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

Table 3-15 lists the new message for the Auditing enabled accounts check.

Table 3-15 Auditing enabled message

Message name	Title	Severity
ESM_SYBASE_AUDITING_NOT_ENABLED	Auditing enabled	Red-4

Auditing threshold procedure

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

This check works with the **Audit segments** check.

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

Table 3-16 lists the new message for the Auditing threshold procedure check.

Table 3-16 Auditing threshold procedure message

Message name	Title	Severity
ESM_SYBASE_NO_THRESHOLD_PROCEDURE	Auditing threshold procedure	Red-4

Audit segments

This check specifies which audit segments to check for an audit threshold procedure. The **Auditing threshold procedure** check works in collaboration with the **Audit segments** check.

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

Audit queue size

This check reports the 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 3-17 lists the new message for the Audit queue size check.

Table 3-17 Audit queue size message

Message name	Title	Severity
ESM_SYBASE_AUDIT_QUEUE_SIZE	Audit queue size	Red-4

Suspend audit when dev is full

This check reports the Sybase ASE servers that have a parameter value for the Suspend audit when dev 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 3-18 lists the new message for the Suspend audit when dev is full check.

Table 3-18 Suspend audit when dev is full message

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

Trunc transaction log on chkpt

This check reports the Sybase ASE servers and their databases that are not configured to truncate transaction logs when performing a checkpoint. Use the name list to include or exclude the databases that the check should report on.

Table 3-19 lists the new message for the Trunc transaction log on chkpt check.

Table 3-19 Trunc transaction log on chkpt message

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

Procedure Audit Options

This check reports the audit configuration settings of the stored procedures and triggers that are different from the settings that are specified in the Sybase ASE Procedure Audit Options template.

The check includes information on the default audit options that are used for any new procedure or trigger created on the specified database.

Table 3-20 lists the new message for the Procedure Audit Options check.

Table 3-20 Procedure Audit Options message

Message name	Title	Severity
ESM_SYBASE_AUDIT_OPTION	Audit Option	Red-4

Object Audit Options

This check reports the object-specific audit configuration settings on tables and the views that are different from the settings that are specified in the Sybase ASE Object Audit Options template.

For example: selecting, inserting, updating, or deleting rows of a particular table or view.

Table 3-21 lists the new message for the Object Audit Options check.

Table 3-21 Object Audit Options message

Message name	Title	Severity
ESM_SYBASE_AUDIT_OPTION	Audit Option	Red-4

Login Audit Options

This check reports the audit configuration settings for the specified user login that are different from the settings that are specified in the Sybase ASE Login Audit Options template.

Table 3-22 lists the new message for the Login Audit Options check.

Table 3-22 Login Audit Options message

Message name	Title	Severity
ESM_SYBASE_AUDIT_OPTION	Audit Option	Red-4

Database Audit Options

This check reports the audit configuration settings of databases that are different from the settings that are specified in the Sybase Database Audit Options template.

For example: altering a database, bulk copy (bcp in) of data into a database, granting or revoking access to objects in a database, and creating objects in a database.

Table 3-23 lists the new message for the Database Audit Options check.

Table 3-23 Database Audit Options message

Message name	Title	Severity
ESM_SYBASE_AUDIT_OPTION	Audit Option	Red-4

Global Audit Options

This check reports the global audit configuration settings that are different from the settings that are specified in the Sybase ASE Global Audit Options template. These global audit configuration settings affect the entire server.

Global options apply to commands that affect the entire server, such as booting the server, disk commands, and allowing ad hoc, user-defined audit records.

Table 3-24 lists the new message for the Global Audit Options check.

Table 3-24 Global Audit Options message

Message name	Title	Severity
ESM_SYBASE_AUDIT_OPTION	Audit Option	Red-4

Sybase ASE Configuration

The checks in the Sybase ASE Configuration module validate the configuration settings of the Sybase ASE server.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Version and product level

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

Table 3-25 lists the new message for the Version and product level check.

Table 3-25 Version and product level message

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

Configuration parameters

This check reports server configuration parameters that do not match the values that you specify in the template.

Table 3-26 lists the new messages for the Configuration parameters check.

Table 3-26 Configuration parameters message

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

Master dev default disk status

This check reports servers that have the master device default disk status enabled. The default disk status is enabled by default and therefore allows the user databases to be installed on the master device.

Table 3-27 lists the new message for the Master dev default disk status check.

Table 3-27 Master dev default disk status message

Message name	Title	Severity
ESM_SYBASE_DEVICE_DEFAULT	Master dev default disk status	Yellow-2

Device status

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

Table 3-28 lists the new messages for the Device status check.

Table 3-28 Device status message

Message name	Title	Severity
ESM_SYBASE_SYD_ GREEN_LEVEL	Device status	Green-1
ESM_SYBASE_SYD_ YELLOW_LEVEL	Device status	Yellow-2
ESM_SYBASE_SYP_RED_ LEVEL	Device status	Red-4

Net password encryption

This check reports the remote servers for which the 'net password encryption' option is set to false.

The Net password encryption option lets you specify whether to initiate a remote server connection by using the client side password encryption handshake or the 'unencrypted password' handshake sequence.

Table 3-29 lists the new messages for the Net password encryption check.

Table 3-29 Net password encryption message

Message name	Title	Severity
ESM_SYBASE_NO_ NET_PASSWD_ENCRYPT	Net password encryption	Red-4

Trusted remote logins

This check reports any remote logins with the trusted status that are found on the Sybase ASE servers.

The use of trusted mode reduces the security of your server as the passwords of these trusted users are not verified. Set the trusted option to false, if you want to ensure user authorization.

Table 3-30 lists the new messages for the Trusted remote logins check.

Table 3-30 Trusted remote logins message

Message name	Title	Severity
ESM_SYBASE_ TRUSTED_REMOTE_LOGIN	Trusted remote login	Red-4

Databases on master device

This check reports the databases that are present on the master device. Use the name list to include or exclude the database names.

Table 3-31 lists the new message for the Databases on master device check.

Table 3-31 Databases on master device message

Message name	Title	Severity
ESM_SYBASE_DATABASE_ON_MASTER	Databases on master device	Yellow-2

Sybase homes

This check reports the Sybase home and the OCS directory for the Sybase ASE servers that are configured in the `SybaseModule.dat` file.

Table 3-32 lists the new messages for the Sybase homes check.

Table 3-32 Sybase homes message

Message name	Title	Severity
ESM_SYBASE_HOME_DATFILE	Sybase home	Green-0

Sample databases

This check reports the sample databases that you should remove from the Sybase ASE servers. Use the name list to include the database names that the check should report on. If the name list is left empty the check reports no problems found.

Table 3-33 lists the new messages for the Sample databases check.

Table 3-33 Sample databases message

Message name	Title	Severity
ESM_SYBASE_SAMPLE_DB	Sample database	Red-4

Sybase ASE Object

The checks in the Sybase ASE Object module validate the various permissions that are set on the objects of the Sybase ASE server. The permissions that the check reports on are as follows:

- Permission on objects
- New permissions
- Deleted permissions
- New databases
- Deleted databases

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Automatically update snapshots

Enable this check to automatically update snapshots with the current information.

Database status

This check reports databases and status that are configured to the Sybase ASE. Use the name list to include or exclude the database names that the check should report on.

Table 3-34 lists the new message for the Database status check.

Table 3-34 Database status message

Message name	Title	Severity
ESM_SYBASE_ DATABASE	Database status	Green-0

User access to database

This check reports the databases that allow access to the user that you specify in the **User** text box. In the text box, you can use comma to report on multiple users or "*" to report on all the users. Use the name list to include or exclude the databases that the check should report on.

If you drop the guest user from the master database, then the server users who are not yet added to any databases cannot log on to the Adaptive Server.

Table 3-35 lists the new message for the User access to database check.

Table 3-35 User access to database message

Message name	Title	Severity
ESM_SYBASE_USER_ACCESS_DATABASE	Databases	Yellow-2

New database

This check reports databases that were added to the Sybase ASE after the last snapshot update. Use the name list to include or exclude the database names that the check should report on.

Table 3-36 lists the new message for the New database check.

Table 3-36 New database message

Message name	Title	Severity
ESM_SYBASE_NEW_DATABASE	New database	Yellow-2

Deleted database

This check reports databases that were deleted from the Sybase ASE after the last snapshot update. Use the name list to include or exclude the database names that the check should report on.

Table 3-37 lists the new message for the Deleted database check.

Table 3-37 Deleted database message

Message name	Title	Severity
ESM_SYBASE_DELETED_DATABASE	Deleted database	Yellow-2

Object permission

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

Table 3-38 lists the new messages for the Object permission check.

Table 3-38 Object permission message

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

Object types to check

Use the name list to include or exclude the object types that the Sybase ASE object checks should report on.

For example: stored procedure, user table, or system table.

Databases to check

Use the name list to include or exclude the databases that the Sybase ASE object checks should report on.

Object actions to check

Use the name list to include or exclude the object actions that the Sybase ASE object checks should report on.

For example: grant or deny.

Objects to check

Use the name list to include or exclude the object names that the Sybase ASE object checks should report on.

The object names can be the name of an object, stored procedure, view, trigger, and so on. You may also use the wild cards.

Grantors to check

Use the name list to include or exclude the grantors that the Sybase ASE object checks should report on.

Grantable object permission

This check reports object permissions that are grantable. Use the name list to include or exclude the grantee the check should report on.

Table 3-39 lists the new message for the Grantable object permission check.

Table 3-39 Grantable object permission message

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

Granted object permission

This check reports object permissions that are granted. Use the name list to include or exclude the grantee that the check should report on.

Table 3-40 lists the new message for the Granted object permission check.

Table 3-40 Granted object permission message

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

New granted object permission

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

Table 3-41 lists the new messages for the New granted object permission check.

Table 3-41 New granted object permission message

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

Table 3-41 New granted object permission message *(continued)*

Message name	Title	Severity
ESM_SYBASE_NEW_OBJ_COLUMN	New granted object permissions	Yellow-2
ESM_SYBASE_NEW_OBJECT	New granted object permissions	Yellow-2

Deleted granted object perm

This check reports the objects or the granted object permissions that were deleted from the Sybase ASE after the last snapshot update. Use the name list to include or exclude the grantee names that the check should report on.

Table 3-42 lists the new messages for the Deleted granted object perm check.

Table 3-42 Deleted granted object perm message

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

Exclude granted object perm

This check excludes the granted object permissions that the **Granted object permission** check reports. Use the name list to specify a template that contains entries to be excluded. This check works with the **Granted object permission** check.

Accounts with CREATE permission

This check reports the database users, roles, and groups that are explicitly granted CREATE permissions. Use the **Keys** list to specify the CREATE permissions that the check should report on. Use the **Databases to check** name list to include or exclude the databases that you want the check to report on. Use the **Grantees to check** name list to include or exclude the grantees that the check should report on.

Table 3-43 lists the new messages for the Accounts with CREATE permission check.

Table 3-43 Accounts with CREATE permission message

Message name	Title	Severity
ESM_SYBASE_CREATE_PERM	Account with CREATE permission	Yellow-2

Stored procedure signature

This check reports the occurrences of the stored procedures, whose signatures are different from the signatures that you define in the template. If you do not define any signature for the stored procedure in the template, then the check reports the signatures of the matched stored procedure. You can use the **Template update** feature to update the template with the signatures that the check reports.

Note: This check only supports the stored procedures and does not support the extended stored procedures.

For more information on the Sybase Stored Procedure Signatures template, see the *Symantec Enterprise Security Manager™ Modules for Sybase Adaptive Server Enterprise Release Notes*.

To update the template

1. Right-click on the message.
2. Choose **Update Template**.

Note: You can use the Sybase Stored Procedure Signatures template to report on the custom stored procedure such as sp_extrapwdchecks, sp_cleanpwdchecks, and so on.

Table 3-44 lists the new messages for the Stored procedure signature check.

Table 3-44 Stored procedure signature message

Message name	Title	Severity
ESM_SYBASE_ SP_SIG_MISMATCH	Stored procedure signature mismatch	Red-4
ESM_SYBASE_MISSING_SP	Missing stored procedure	Yellow-2

Table 3-44 Stored procedure signature message *(continued)*

Message name	Title	Severity
ESM_SYBASE_ HIDDEN_SP	Hidden stored procedure	Yellow-2

Grantees to check

Use the name list to specify the grantees that should be excluded or included for the **Accounts with CREATE permissions** check and **Proxy access permission** check.

Accounts with set proxy permission

This check reports the database users, roles, and groups that are explicitly granted the set proxy or set session authorization permissions. Use the **Grantees to check** name list to include or exclude the grantees that the check should report on.

Table 3-45 lists the new messages for the Accounts with set proxy permission check.

Table 3-45 Accounts with set proxy permission message

Message name	Title	Severity
ESM_SYBASE_SET_ PROXY_PERM	Accounts with set proxy permission	Yellow-2

Sybase ASE Password Strength

The checks in the Sybase ASE Password Strength module evaluate the security risks that are associated with the accounts that are present on the server.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Empty password

This check reports Sybase ASE logins with empty or NULL passwords.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Table 3-46 lists the new message for the Empty password check.

Table 3-46 Empty password message

Message name	Title	Severity
ESM_SYBASE_NULL_PASSWORD	Empty password	Red-4

Password = login name

This 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.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Table 3-47 lists the new message for the Password = login name check.

Table 3-47 Password = login name message

Message name	Title	Severity
ESM_SYBASE_GUESSED_PASSWORD	Guessed password	Red-4

Password = any login name

This check reports the Sybase ASE logins with the 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.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Table 3-48 lists the new message for the Password = any login name check.

Table 3-48 Password = any login name message

Message name	Title	Severity
ESM_SYBASE_GUESSED_PASSWORD	Guessed password	Red-4

Password = wordlist word

This check reports the matches between the Sybase ASE login passwords and the words that are present in the enabled word files. For shorter run times, in the **Percent of words per policy run** text box, type a number less than or equal to 100. The number defines the percentage of words that are examined during each run. In the word list, each run starts where the previous run ended.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Table 3-49 lists the new message for the Password = wordlist word check.

Table 3-49 Password = wordlist word message

Message name	Title	Severity
ESM_SYBASE_GUESSED_PASSWORD	Guessed password	Red-4

Reverse order

This check works with the **Password = login name**, **Password = any login name**, and **Password = wordlist word** checks. Enable this check with the **Password = login name** check to report on the logins that has the password as the reverse order of the login name. Enable this check with the **Password = any login name** check to report on the logins that has password as the reverse order of any login name. Enable this check with the **Password = wordlist word** check to report the logins that contains the passwords that match the reverse order of the entries in the enabled word files.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Double occurrences

This check works with **Password = login name**, **Password = any login name**, and **Password = wordlist word** checks. Enable this check with the **Password = login name** check to report on the logins that has the password as the double occurrences of the login name. Enable this check with the **Password = any login name** check to report on the logins that has the password as double occurrences of any login name. Enable this check with the **Password = wordlist word** check to report the logins that contains the passwords that match the double occurrences of the entries in the enabled word files.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Plural

This check works with **Password = login name**, **Password = any login name**, and **Password = wordlist word** checks. Enable this check with the **Password = login name** check to report on the logins that has the password as the plural of the login name. Enable this check with the **Password = any login name** check to report on the logins that has the password as plural of any login name. Enable this check with the **Password = wordlist word** check to report the passwords that match the plural forms of the entries in the enabled word files.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Prefix

This check works with **Password = login name**, **Password = any login name**, and **Password = wordlist word** checks. Enable this check with the **Password = login name** to report on the logins that has the password as the login name with the prefix that you specify in the **Prefixes to use** list. Enable this check with the **Password = any login name** check to report on the logins that has the password as any login name with the prefix that you specify in the **Prefixes to use** list. Enable this check with the **Password = wordlist word** check to report the passwords that match the entries in the enabled word files with a prefix that you specify in the **Prefixes to use** list. Use the name list to specify the prefixes that the check should report on.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Suffix

This check works with **Password = login name**, **Password = any login name**, and **Password = wordlist word** checks. Enable this check with the **Password = login name** to report on the logins that has the password as the login name with the suffix that you specify in the **Suffixes to use** list. Enable this check with the **Password = any login name** check to report on the logins that has the password as any login name with the suffix that you specify in the **Suffixes to use** list. Enable this check with the **Password = wordlist word** check to report the passwords that match the entries in the enabled word files with a suffix that you specify in the **Suffixes to use** list. Use the name list to specify the suffixes that the check should report on.

Note: Sybase ASE 15.0.2 and later versions do not support this check.

Roles without password

This check reports roles that do not have passwords. Use the **Roles** list to include or exclude the roles that the check should report on.

Table 3-50 lists the new message for the Roles without password check.

Table 3-50 Roles without password message

Message name	Title	Severity
ESM_SYBASE_ROLE_NO_PASSWORD	Role without password	Yellow-2

Hide guessed password details

When you enable this check, the security checks no longer display the details of the guessed password. This check works with the **Password = login name**, `Password = any login name`, **password = wordlist word**, **Reverse order**, **Double occurrences**, **Plural**, **Prefix**, and **Suffix** checks.

Password complexity parameters

This check reports the values for the password complexity options that do not match with the values that you specify in the template. You can use the `sp_passwordpolicy` stored procedure to set the password complexity options. The `sp_passwordpolicy` stored procedure is available on Sybase ASE 12.5.4 and later and 15.0.2 and later versions.

Note: Sybase ASE 12.5.4, 15.0.2, and 15.0.3 versions support this check.

For more information on the Sybase Password Parameter template, see the *Symantec Enterprise Security Manager™ Modules for Sybase Adaptive Server Enterprise Release Notes*.

Table 3-51 lists the new messages for the Password complexity parameters check.

Table 3-51 Password complexity parameters message

Message name	Title	Severity
ESM_SYBASE_SP_ GREEN_LEVEL	Unauthorized password complexity parameter	Green-0
ESM_SYBASE_SP_ YELLOW_LEVEL	Unauthorized password complexity parameter	Yellow-2
ESM_SYBASE_SP_ RED_LEVEL	Unauthorized password complexity parameter	Red-4

Login options(account)

This check works with the **Password expiration**, **Minimum password length**, and **Maximum failed login attempts** checks. The **Login options(account)** check reports the individual login accounts that do not satisfy the condition that you specify in the login configuration parameters-related checks. Use the name list to include or exclude the logon accounts that the check should report on.

Password contains digits

This check reports the servers that have minimum required digits in the password set less than the value specified in the **Min digits in password** text box. The check searches for the value 'min digits in password' option that the sp_passwordpolicy stored procedure sets. If the value is unavailable then the check uses the 'check password for digit' value of the global setting to report on.

Table 3-52 lists the new message for the Password contains digits check.

Table 3-52 Password contains digits message

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

Roles to check

Use the name list to specify the roles that you want to include or exclude from reporting violations. Use this name list with the **Login options(account)** check to report the members of the roles that you want to include or exclude from reporting violations.

Password expiration

This check reports the Sybase ASE servers that have the system-wide 'password expiration' configuration parameter higher than the value that you specify in the **Maximum password age** text box or that have the 'password expiration' configuration parameter value set to 0. Enable this check with the **Login options(account)** check to report all the login accounts with the 'password expiration' configuration parameter set more than the value that you specify in the **Maximum password age** text box or that have the 'password expiration' configuration parameter value set to 0 . Enable this check with the **Roles to check** name list to specify the roles whose members you want to include or exclude from reporting the violations in the 'Password expiration' settings.

Table 3-53 lists the new message for the Password expiration check.

Table 3-53 Password expiration message

Message name	Title	Severity
ESM_SYBASE_MIN_ PASSWORD_AGE	Password expiration	Yellow-2

Maximum failed login attempts

This check reports the Sybase ASE servers that have the system-wide 'maximum failed login attempts' configuration parameter set higher than the value you specify in the **Maximum failed login attempts** text box or that have the 'maximum failed login attempts' configuration parameter less than or equal to 0. Enable this check with the **Login options(account)** check to report all the login accounts that have the 'maximum failed login attempts' configuration set higher than the value that you specify in the **Maximum failed login attempts** text box or that have the 'maximum failed login attempts' configuration parameter less than or equal to 0. Enable this check with the **Roles to check** name list to specify the roles whose members you want to include or exclude from reporting the violations in the **Maximum failed login attempts** settings.

Table 3-54 lists the new message for the Maximum failed login attempts check.

Table 3-54 Maximum failed login attempts message

Message name	Title	Severity
ESM_SYBASE_MAX_ FAIL_LOGIN_ATMPT	Maximum failed login attempts	yellow-2

Minimum password length

This check reports the Sybase ASE servers that have the system-wide 'minimum password length' configuration parameter less than the value that you specify. Enable this check with the **Login options(account)** check to report all the login accounts with the 'minimum password length' configuration parameter less than the value that you specify. Enable this check with the **Roles to check** name list to specify the roles whose members you want to include or exclude from reporting the violations in the 'minimum password length' settings.

Table 3-55 lists the new message for the Minimum password length check.

Table 3-55 Minimum password length message

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

Roles - minimum password length

This check reports the roles that have the password length set less than the value specified in the **Minimum password length** text box. Enable this check with the **Roles to check** name list to specify the roles you want to include or exclude from reporting the violations in the minimum password length settings.

Roles - password expiration

This check reports the roles that have the password expiration configuration parameter higher than the value that you specify or the roles that have the password expiration configuration parameter value set to 0. Enable this check with the **Roles to check** name list to specify the roles you want to include or exclude from reporting the violations in the password expiration settings.

Roles - maximum failed login attempts

This check reports the roles that have the maximum failed login attempts configuration parameter set higher than the value specified in the **Maximum failed login attempts** text box or the roles that have the maximum failed login attempts configuration parameter less than or equal to 0. Enable this check with the **Roles to check** name list to specify the roles you want to include or exclude from reporting the violations in the maximum failed login attempts settings.

Maximum reported messages

This check limits the number of messages that the module returns.

You can specify a limit for the number of messages that the module returns. On reaching the maximum limit for a single message, the module displays the message again with the number of the repeating instances of the message that are not reported.

Monitor password age

This check reports any unlocked accounts with the passwords that are older than the limit that you specify. This check works with the use **Roles to check** name list. Use **Roles to check** name list to include or exclude the roles. The check **Monitor password age** reports on the members of the included roles that you include in the name list.

This check proves to be beneficial if there is no password expiration setting present on the server. In this case, the check **Monitor password age** reports the login accounts that have not changed their password within the specified days.

Table 3-56 lists the new message for the Monitor password age check.

Table 3-56 Monitor password age message

Message name	Title	Severity
ESM_SYBASE_MONITOR_PASSWORD_AGE	Monitor password age	Red-4

Sybase ASE Patches

The checks in the Sybase ASE patches module validate whether the Sybase ASE servers are up to date with the latest patch level.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Patch templates

This check specifies the Sybase ASE Patch template files for the module to use.

Table 3-57 lists the new message for the Patch templates check.

Table 3-57 Patch templates message

Message name	Title	Severity
ESM_SYBASE_PATCH_NOT_FOUND	Patch not found	Red-4

Sybase ASE Roles and Groups

The checks in the Sybase ASE Roles and Groups reports the roles that are new or deleted, database roles, and the groups of the Sybase ASE server.

Servers to check

This check specifies the Sybase ASE servers that the module includes or excludes.

Role status

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

Table 3-58 lists the new message for the Role status check.

Table 3-58 Role status message

Message name	Title	Severity
ESM_SYBASE_ROLE_STATUS	Roles status	Green-0

Role grantees

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

Table 3-59 lists the new message for the Role grantees check.

Table 3-59 Role grantees message

Message name	Title	Severity
ESM_SYBASE_ROLE_GRANTEE	Role grantees	Green-0

New roles

This 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 3-60 lists the new messages for the New roles check.

Table 3-60 New roles message

Message name	Title	Severity
ESM_SYBASE_NEW_ ROLE	New roles	Yellow-2
ESM_SYBASE_NEW_ ROLE_GRANTEE	New roles	Yellow-2

Deleted roles

This 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 3-61 lists the new messages for the Deleted roles check.

Table 3-61 Deleted roles message

Message name	Title	Severity
ESM_SYBASE_DELETED_ ROLE	Deleted roles	Yellow-2
ESM_SYBASE_DELETED_ ROLE_GRANTEE	Deleted roles	Yellow-2

Accounts to check

Use this check to include or exclude the login accounts for the **Granted prohibited roles** check.

Database groups

This check reports database groups. Use the name list to include or exclude the databases that the check should report on.

Table 3-62 lists the new message for the Database groups check.

Table 3-62 Database groups message

Message name	Title	Severity
ESM_SYBASE_ DATABASE_GROUP	Database groups	Green-0

Group members

This check reports group members. Use the name list to include or exclude the databases that the check should report on.

Table 3-63 lists the new message for the Group members check.

Table 3-63 Group members message

Message name	Title	Severity
ESM_SYBASE_GROUP_ MEMBER	Group members	Green-0

New groups

This check reports the database groups and members that were added to the database after the last snapshot update. Use the name list to include or exclude the databases that the check should report on.

Table 3-64 lists the new messages for the New groups check.

Table 3-64 New groups message

Message name	Title	Severity
ESM_SYBASE_NEW_GROUP	New groups	Yellow-2
ESM_SYBASE_NEW_ GROUP_MEMBER	New groups	Yellow-2

Deleted groups

This check reports the database groups and members that were deleted from the database after the last snapshot update. Use the name list to include or exclude the database names that the check should report on.

Table 3-65 lists the new messages for the Deleted groups check.

Table 3-65 Deleted groups message

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

Automatically update snapshots

Enable this option to automatically update the snapshots with the current information.

Granted prohibited roles

This check reports the accounts that have been granted specified roles. Use the name list to include or exclude the prohibited roles that the check should report on.

Table 3-66 lists the new messages for the Granted prohibited roles check.

Table 3-66 Granted prohibited roles message

Message name	Title	Severity
ESM_SYBASE_PROHIBIT_ROLE	Granted Prohibited role	Red-4

Chapter 4

Troubleshooting

This chapter includes the following topics:

Encryption exception

An error may display when you run a policy asking you to reconfigure the module.

Table 4-1 lists the error message that is displayed and the solution for the error.

Table 4-1 Encryption exception

Error	Solution
Encryption exception	This error may occur if you have set SSLConfigure=0 after configuring the Sybase ASE module. Or, if you have renamed or deleted the AESConfigSYB.dat file. To solve this problem, you need to reconfigure the Sybase ASE module. If you want to generate logs for encryption, add Debugon=1 in the AESConfigSYB.dat file from the esm\config folder. It generates SYBASEdebuglog.log in the esm\system\<platform> folder.

RDL error

The following list contains the RDL 6.5.3 error and its solution:

Table 4-2 lists the rdl message that is displayed and the solution for the error.

Table 4-2 RDL error

Error	Solution
If you have ESM modules for Sybase ASE and RDL 6.5.3 installed on the same computer, the RDL database does not get populated with correct module IDs of the Sybase modules.	Upgrade RDL 6.5.3 to RDL 6.5.3 SP2.