symantec. Confidence in a connected world.

Support Home | Supported Products A to Z

Symantec.com > Enterprise > Support > **Knowledge Base**

Unable to communicate with the reporting component after logging into the Symantec Endpoint Protection Manager

PRINT THIS PAGE

Question/Issue:

The Symantec Endpoint Protection Manager (SEPM) console shows the following error: "Unable to communicate with the reporting component... " After clicking OK to this message, either the Home, Monitors and Reports pages are dimmed or the data does not load.

Symptoms:

There are multiple possible reasons for this issue and this document will detail all known solutions - troubleshooting opportunities.

Cause:

There are a number of possible causes. This article details the known solutions or troubleshooting methods.

Solution:

Reset Internet Information Services (IIS)

In some cases simply resetting IIS can resolve this issue. Follow the steps below:

1. Exit SEPM
2. Click **Start** > **Run**.
3. Type `iisreset`
4. Click **OK**.
5. Log into SEPM again.

Check the IIS Configuration

Verify IIS permissions and account(s) rights are set correctly

Use the Microsoft IIS Diagnostics Toolkit to identify all the rights and permissions on the accounts. The toolkit is available from Microsoft at:

http://www.microsoft.com/downloads/details.aspx?familyid=9BFA49BC-376B-4A54-95AA-73C9156706E7&displaylang=en

Verify the DefaultAppPool identity is set to 'Network Service'

1. Open the IIS Administrator
2. Expand <**server name**> > **Application Pools**
3. Right-click **DefaultAppPool** and select **Properties**
4. On the **Identity tab** verify the **Predefined radio button** is selected and that **Network Service** is on the drop down list
5. If **Network Service** is listed then try adding the **Local System**

   Note: Parts of these instructions cannot be performed with Windows XP running IIS 5.1 or Windows 2000 running IIS 5.0.
   For either, there is no "application pool in the configuration and "IP address and domain name restrictions" are dimmed in the virtual server settings.
   Microsoft purposely denies access to these settings.

Verify user rights.

1. Run gpedit.msc
2. Expand **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies**
3. Select **User Rights Assignment** in the left-hand pane
4. Go to the **Adjust memory Quotas for a Process** item and double click.
5. Verify that **LOCAL SERVICE** and **NETWORK SERVICE** are listed under the Local Security Setting tab.
6. Go to the **Replace a process-level token** item and double click. Again, verify that **LOCAL SERVICE** and **NETWORK SERVICE** are listed.

   Note: If the "Add User or Group..." button is disabled, it may be locked by a domain GPO (group policy object) which will require an assessment of domain GPOs.
7. Restart the IIS Admin service to update any changes

Verify Authentication and Access Control.

1. Open the IIS Administrator
2. Right-click **Default Web Site** and click **Properties**
3. On the **Directory Security** tab, under **Authentication and Access Control**, click **Edit**
4. Verify that **Enable Anonymous Access** is selected
5. Please select the appropriate setting if you are utilizing **Authenticated Access**

If SSL is not implemented, verify that Secure Communications is not selected

1. Open the IIS Administrator
2. Right-click **Default Web Site** and select **Properties**

3. On the **Directory Security** tab, under Secure Communications click **Edit**
4. Verify **Require Secure Channel (SSL)** is not selected

Re-enable logging in IIS

Examine the IIS logs to get the full error code. The default location for the logs is **C:\Windows\System32\LogFiles\W3SVC1**
In the IIS manager, right click each site where you wish to have the logs, such as Reporting and Secars, and select **Log visits** and click OK.

If you have to contact technical support, have these logs ready for the technicians.

Testing the ODBC Connection

Note: On a 64-bit computer, a 32-bit DSN is created and is accessible via (by default) C:\Windows\SysWoW64\Odbcad32.exe.

For an embedded (Sybase) database

1. Verify that the **Symantec Embedded Database** service is running and that the **dbsrv9.exe** process is listening on TCP port 2638
2. Test the ODBC connection.
    1. Open **Control Panel** > **Administrator Tools**
    2. Double click **Data Sources (ODBC)**
    3. On the **System DSN** tab, double-click **SymantecEndpointSecurityDSN**
    4. Go through the wizard to ensure the following settings:

       ```
       Name: SymantecEndpointSecurityDSN
       Description: <Anything>
       Server: Servername\InstanceName (Can be blank as it is localized, otherwise specify the default: sem5)
       Login ID: dba
       Password: <password>
       ```
    5. Leave the defaults for the rest of the items and click **Finish**
    6. Click **Test Data Source** , it should return "Success"
    7. Click **OK**

For an SQL database

1. Verify the following:
    - You specified a named instance during installation and configuration. For example: \\<server name>\<instance name>
    - The SQL Server is running and properly configured
    - The network connections between Symantec Endpoint Protection Manager and the SQL database.
2. Test the ODBC connection.
    1. Open **Control Panel** > **Administrator Tools**
    2. Double click **Data Sources (ODBC)**
    3. On the **System DSN** tab, double-click **SymantecEndpointSecurityDSN**
    4. Go through the wizard to ensure the following settings:

       ```
       Name: SymantecEndpointSecurityDSN
       Description: <Anything>
       Server: Servername\InstanceName (Only enter the server name or IP address if using the default instance)
       Login ID: sa
       Password: <password>
       ```
    5. Leave the defaults for the rest of the items and click **Finish**
    6. Click **Test Data Source** , it should return "Success"
    7. Click **OK**

Check system resources

You should have at least 1GB of RAM available. If not, CPU usage may be high and this could be affecting the issue. Refreshing the console may help temporarily but it is only a workaround and not a solution.

Loopback address disabled

Reporting pages may fail to appear if loopback addresses are disabled on the computer. If you have disabled loopback addresses on your computer, you must associate the word localhost with your computer IP address. You can use the Windows hosts file to do this. For example, on computers running Windows XP, do the following:

1. Change the directory to the location of your hosts file. By default, the hosts file is located in%SystemRoot%\system32\drivers\etc
2. Open the hosts file with an editor such as Microsoft Notepad.
3. Add the following line to the file:

   ```
   xxx.xxx.xxx.xx   localhost   # to log on to reporting functions
   ```
   (where xxx.xxx.xxx.xx is the IP address of your computer)
4. Save and close the hosts file.

Remote Desktop Protocol (RDP)

There may be various issues with unpredictable results associated with RDP when installing or managing SEP or SEPM. To avoid these, it is best to install or manage SEP or SEPM locally. If that is not possible you can:

- Use pcAnywhere
- Use the switch that Microsoft recommends to shadow a console session within an RDP session.

Note: A Windows Server 2003 server must be configured to permit remote control

For reference, read the Microsoft article: *How to Connect to and Shadow the Console Session with Windows Server 2003 Terminal Services*
http://support.microsoft.com/kb/278845

Verify the version of PHP that SEPM is using
Running multiple versions of PHP installed and used by different software products may cause conflicts. PHP performs a check for global configuration (php.ini) in a variety of locations. It forces each product to use its own interpreter which allows the product to operate properly and to use the correct version of PHP associated with each product.

To check if there is a version conflict with the version of PHP that SEPM is using:

1. Open a blank document with a text editor (Notepad for example.)
2. Copy/paste the following code into the document:

   ```
   <?phpinfo();?>
   ```
3. Save the document as **phpinfo.php** in the folder **C:\Program Files\Symantec\Symantec Endpoint Protection Manager\PHP**
4. Click **Start > Run**
5. In the Open box type: `cmd`
6. In the command window type:

   ```
   cd "C:\Program Files\Symantec\Symantec Endpoint Protection Manager\PHP"
   php phpinfo.php | more
   ```

   If you see text output to the screen that displays the status of PHP, then PHP is installed.
7. Confirm that this is the correct version by:
   - comparing it to the version of the file: **"C:\Program Files\Symantec\Symantec Endpoint Protection Manager\PHP\php.exe".**
     The version displayed by the php command and the version of the file should match.
   - See the line in the output text on screen that says `Loaded Configuration File =>`
     This is the configuration file the installed version of PHP is using. Ideally, this file will be: **C:\Program Files\Symantec\Symantec Endpoint Protection Manager\PHP\Php.ini**
8. If you see text that says: " 'php' is not recognized as an internal or external command", then the PHP installation for SEPM is broken. In this case, do the following:
   1. Close the command prompt.
   2. Copy the file 'phpinfo.php' to **C:\**
   3. Click **Start > Run.** Type `cmd`
   4. In the command window type: `php phpinfo.php | more`
      - If the command returns: " 'php' is not recognized as an internal or external command", then PHP is not installed and registered with the OS. the problem is not with SEPM as long as step 6 produced a result.
      - If the command returns a status of PHP, then PHP is installed and registered with the operating system. If the version displayed here does not match the version installed with SEPM (step 7), then there is a problem (version mismatch).
   5. Close the command prompt.
   6. Copy the 'phpinfo.php' file to: **C:\Program Files\Symantec\Symantec Endpoint Protection Manager\Inetpub\Reporting**
   7. Open the web browser to: http://LocalHost:8014/Reporting/phpinfo.php. A browser page describing the PHP status should display. If a 404 page "Page not found" displays, turn your troubleshooting to IIS.

Resolving a PHP version conflict with SEPM

If you do find a PHP version conflict, read the article: *Specifying the php.ini file used by the Symantec Endpoint Protection Manager (SEPM) Reporting website* at http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008060213161448

If this article does not work try the following workaround. Be advised that any application depending on the PHP version different from the PHP version used by SEPM may be disabled or broken.

1. Make a back up of the PHP folder that is *not* the SEPM version. Call this folder A.
2. Copy the contents of the PHP folder **C:\Program Files\Symantec\Symantec Endpoint Protection Manager\PHP** to folder A (overwriting any and all files)
3. Restart the SEPM service. A restart of the entire computer may be needed.

Uninstall/Reinstall the SEPM
If it proves necessary to uninstall and reinstall the SEPM, follow the instructions in the following articles:

How to install Symantec Endpoint Protection and Symantec Endpoint Protection Manager through Remote Desktop
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008030509272248

How to manually uninstall Symantec Endpoint Protection Manager 11.0
http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2007101615023748

References:
Title: 'How to work with Data Sources (ODBC) or ODBC connection in 64bit Windows OS'
Document ID: 2008021900094548

Document ID: 2008042212582048
Last Modified: 01/27/2010
Date Created: 04/22/2008
Operating System(s): Windows 2000 Professional, Windows 2000 Server/Advanced Server, Windows XP Professional Edition, Windows Server 2003 Web/Standard/Enterprise/Datacenter Edition, Windows Server 2003 x64 Edition
Product(s): Endpoint Protection 11
Release(s): Endpoint Protection 11.0.2

Site Index · Legal Notices · Privacy Policy · Site Feedback · Contact Us · Global Sites · License Agreements