

Symantec Enterprise Security Manager™ Signature Fix Update Guide

This document contains the procedures for updating Symantec ESM 6.5.2, 6.5.0, 6.0, and 5.5 agents and ESM 6.5.0, 6.5.2 and 6.0 managers, for fixing the remote code execution issues. For detailed information about this issue see the Symantec Enterprise Security Manager Signature Fix Release Notes.

Downloading the updates

Download the following archives as necessary, to update Symantec ESM 6.5.2, 6.5.0, 6.0, and 5.5 agents and ESM 6.5.0, 6.5.2 and 6.0 managers for fixing the remote code execution issues:

- [ESM65xSignatureFix.zip](#)
- [ESM60SignatureFix.zip](#)
- [ESM55SignatureFix.zip](#)

Extract the archive to a local directory. The update package contains agent folders that contain the update files for each supported platform (for example: c:\download\ESM65xSignatureFix\agent\w2k-ix86).

When manually updating ESM managers and ESM agents, you will need to locate and copy update files from the appropriate platform folder (for example: c:\download\ESM65xSignatureFix\agent\w2k-ix86\esmagent.exe).

Install / Upgrade

The install/upgrade for this release pushes OpenSSL to the agent platform, adds the Symantec certificates to the agent, and pushes the new agent code to the host. The upgrade for this release also includes the upgrade to the GPGV library to mitigate the vulnerabilities. You can use the following sequence to install the Signature Fix:

- After installing the Signature Fix, you will not be able to run a remote upgrade to install previous patches. Install all previous patches before installing the Signature Fix.
- Manually installing previous ESM versions, patches, or updates may overwrite the patched esmupdd (UNIX) or esmagent.exe (Windows), thus disabling the Signature security fixes.

Updating ESM agents manually

Before you manually update the Symantec ESM agents on Windows and UNIX, you have to create an x509 directory. The x509 directory stores the Symantec Certificate required to verify that remote upgrade packages are from Symantec.

To create the x509 directory

1. Create a directory named x509 under #esm.
(Example: For Windows: C:\program files\symantec\esm; For UNIX: /esm)
2. Create the certs directory under #esm/x509.
3. Create the casymc directory under #esm/x509.
4. Copy SymantecCACert.pem to #esm/x509/casymc.
5. Copy SymantecCodeSignCert.pem to #esm/x509/certs.

The following procedures describe the process of manually updating Symantec ESM agents to resolve the remote code execution issue:

To manually update an ESM agent on Windows

1. Stop the ESM Agent Service in Windows Service Manager.
2. Rename the current gpgv.exe, esmagent.exe in c:\program files\symantec\esm\bin\w3s-ix86 if you want to save the old file.
3. Copy the new gpgv.exe, esmagent.exe, iconv.dll file from c:\download\ESM65xSignatureFix\agent\w3s-ix86, and then paste the file into c:\program files\symantec\esm\bin\w3s-ix86.
4. Copy the new version.dat file from c:\download\ESM65xSignatureFix\agent\w3s-ix86, and then paste the file into c:\program files\symantec\esm\bin\w3s-ix86.
5. Restart the ESM Agent Service.

Example: manual update on Windows

On a Windows Server 2003 platform, copy esmagent.exe, gpgv.exe, iconv.dll, version.dat to the #esm/bin/w3s-ix86.

Note: On a Windows 2000 platform, copy the files to the #esm/bin/w2k-ix86.

To manually update an ESM agent on UNIX

1. Stop the ESM process using the esmsetup program.
2. Rename the current esmd, esmupdd, gpgv, and version.dat file using the following command:
mv /esm/bin/solaris-sparc/esmd /esm/bin/solaris-sparc/esmd-before-signature-fix
mv /esm/bin/solaris-sparc/esmupdd /esm/bin/solaris-sparc/esmupdd-before-signature-fix
mv /esm/bin/solaris-sparc/gpgv /esm/bin/solaris-sparc/gpgv-before-signature-fix
mv /esm/bin/solaris-sparc/version.dat /esm/bin/solaris-sparc/version.dat-before-signature-fix
3. Copy the new esmd, new_esmupdd, gpgv, and version.dat file to the agent using the following command:
cp /myFix/ESM65xSignatureFix/agent/solaris-sparc/esmd /esm/bin/solaris-sparc/
cp /myFix/ESM65xSignatureFix/agent/solaris-sparc/new_esmupdd /esm/bin/solaris-sparc/
mv /esm/bin/solaris-sparc/new_esmupdd /esm/bin/solaris-sparc/esmupdd
cp /myFix/ESM65xSignatureFix/agent/solaris-sparc/gpgv /esm/bin/solaris-sparc/
cp /myFix/ESM65xSignatureFix/agent/solaris-sparc/version.dat /esm/bin/solaris-sparc/
4. Set permissions and ownership to that of the original files that were re-named.
5. Wait for approximately 1 minute to allow the agent port to be unbound.
6. Restart the ESM process using the esmsetup program.

Example: manual update on UNIX

The above example is for a Solaris system, copy esmd, new_esmupdd, gpgv, version.dat to /esm/bin/solaris-sparc. Rename new_esmupdd to esmupdd.

Updating ESM managers manually

The following procedures describe the process for manually updating Symantec ESM managers on Windows and UNIX to fix the remote code execution issue. Each manager must be updated manually.

To manually update an ESM manager on Windows

1. Stop the ESM Manager Service in Windows Service Manager.
2. Rename the current gpgv.exe file in c:\program files\symantec\esm\bin\w3s-ix86 if you want to save the old file.
3. Copy the new gpgv.exe and iconv.dll files from c:\download\ESM65xSignatureFix \manager\w3s-ix86.
4. Paste the new gpgv.exe and iconv.dll files into c:\program files\symantec\esm\bin\w3s-ix86.
5. Restart the ESM Manager Service.

Example manual ESM manager update on Windows

On Windows Server 2003, copy the gpgv.exe and iconv.dll to the #esm/bin/w3s-ix86.

To manually update an ESM manager on UNIX

1. Stop the ESM process using the esmsetup program.
2. To rename the current gpgv file, type the following command:
mv /esm/bin/solaris-sparc/gpgv /esm/bin/solaris-sparc/gpgv-before-signature-fix
3. To copy the new gpgv file to the manager, type the following command:
cp /myFix/ESM65xSignatureFix/manager/solaris-sparc/gpgv /esm/bin/solaris-sparc/
4. Restart the ESM process using the esmsetup program.

Example manual ESM manager update on UNIX

On Solaris, copy the gpgv to the #esm/bin/solaris-sparc.

Updating ESM agents remotely

The following procedure describes the process for remotely updating Symantec ESM agents to fix the remote code execution issue for all supported ESM platforms. If a firewall is enabled on the host machine, ensure that it allows incoming traffic on port 5599 to perform a remote upgrade.

Note: Before remotely updating ESM 6.5.2, 6.5.0, 6.0, and 5.5 agents, you must move the manager folder from the main folder (for example: c:\download\ESM65xSignatureFix\manager to c:\download\ESM65\manager).

If the manager folder is not moved, it may interfere with the remote update of ESM agents.

To remotely update ESM agents

1. On your system where the ESM manager is installed (for example: c:\program files\symantec\esm), you must rename the agent directory c:\program files\symantec\esm\update\agent, so that LiveUpdate will update with the files necessary for the Signature Fix.
2. In the Symantec ESM console, in the Enterprise tree, locate the agent you want to update.
3. Right-click the agent, and then click **Enable LiveUpdate** to enable the agents that you want to update.
4. Group ESM 6.5.2, 6.5.0, 6.0, and 5.5 agents into separate domains.
5. To LiveUpdate the agents, do one of the following:
 - In the ESM 6.5.0 or 6.5.2 console, select the CD, a local directory, or a network path.
 - In the ESM 6.0 console, select the CD or network drive.
6. Browse to the directory that contains your extracted downloaded zipped files for the fixes.

Make sure that you select the directory just above the agent folder. For example, if you are updating ESM 6.0 agents, select the ESM60SignatureFix directory. (Example: c:\download\ESM60SignatureFix)

You must update the ESM 6.5.2, 6.5.0, 6.0, and 5.5 agents in separate passes. If you have the manager installed on c:\program files\symantec\esm, when you push each upgrade package, the package goes to the same directory (c:\program files\symantec\esm\update) on the manager.

Before you push the second package, you must rename the first package so that it does not combine with the other fixed version numbers, i.e. 6.0 with 6.5.2, etc.

7. Push the files to the manager.
8. The console will only push the agent files to the manager for the agent Operating Systems registered to that manager.
9. Right-click the domain, and then click **Remote Upgrade**.
If you do not see all the agent names in the left panel, these agents must be LiveUpdate-enabled.
10. When the first batch of agents are successfully updated, repeat steps 4 through 8 for the next batch of agents belonging to the next version.

Post Signature Fix installation

After the Signature Fix is installed, all previous versions of Agent Remote Upgrade packages are invalid. You must upgrade to ESM version 6.5.3.

Note: On UNIX only, Remote Tuneup of tpk can no longer be executed after applying the Signature Fix. Run Live-Update via Policy run to obtain the module updates; or you may execute the tpk packages manually on the agent machine.

Note: During deployment of the Signature Fix on the ESM agent, you must disable the firewall or allow traffic on port 5599. By default, Windows XP, Linux, and SuSE firewalls are enabled.

The following procedure describes the process for checking the status of the upgraded agents when the update is complete:

To check the status of an agent update

1. Right-click the manager, and then click Check remote upgrade status.
The following table describes the status of an agent update:

Status	Description
Clock status	Waiting to be upgraded
Gray status	The upgrade is in progress
Green status	The upgrade was successful
Red status	The upgrade failed

2. In the Upgrade Status window, select an agent. In the right pane the verbose upgrade status is displayed.

Additional remote upgrade status information

As an agent upgrade progresses you can click on each of the agents to see its status. The following table describes the list of possible upgrade statuses and related information.

Status	Additional information
Successfully upgraded	Check to see if the agent got the fix (i.e. the new esmd, esmupdd, gpgv for UNIX or the new esmagent.exe, iconv.dll, gpgv.exe for Windows and the new version.dat for UNIX and Windows) but that all of the other files remained the same.
Upgrade failed	Check error message(s) to debug further.
Server is not running...	Go to the machine to make sure that the agent is running.
Agent is not allowed for remote upgrade/LiveUpdate...	You must enable the agent for LiveUpdate. Right click on Agent Properties , and then click LiveUpdate . Also, make sure that the agent was installed with LiveUpdate enabled. On UNIX, run /esm/esmsetup, enable options 4, and then 6, and then 2. On Windows, run the setup, and then click Enable LiveUpdate.
Agent is already updated	This could mean that the agent update file has not yet been pushed from the console to the manager. This could be because when live update was run, no agents belonging to that operating system had been registered yet with the manager. Run LiveUpdate again to push the pertinent files to the manager.

Products not updated by Signature Fix

The following ESM agent platforms do not have updates available for download. However, the vulnerability can be removed by a manual procedure.

ESM agent platform
Sequent 4.4.2 SGI Irix 6.2, 6.3 NCR 3.2+

Updating unpatched ESM agents manually

To manually update the ESM agent on UNIX, you must remove the esmupdd file from the <OS> directory to resolve the remote code execution issue.

To manually update an unpatched ESM agent on UNIX

1. Remove the esmupdd file from the #esm/bin/<OS> directory, where <OS> is Sequent 4.4.2, SGI Irix 6.2, 6.3, or NCR 3.2+.

Error messages

1. Received from a Signature Fixed agent when remotely upgrading to a non-SMIME package.

UNIX

The following message appears in the esmupdd.log:

```
[06763] esmupdd: Signature verification failed for file `~/esm/system/qa4hplk/tmp/tmp_esmupdd',  
error-code=-5
```

Windows

The following message appears in the esmagent.log:

```
[02140] Update server: Signature verification failed for file `c:\program  
files\symantec\esm\system\22-c-4-8\tmp\esmupdat.exe', error-code=-5
```

2. Received from a non-Signature Fixed agent when doing a remote upgrade of a SMIME package.

UNIX

The following message appears in the esmupdd.log:

```
[20993] esmupdd: error exec'ing /esm/system/qa-swatlnxopt1/tmp/tmp_esmupdd; Exec format  
error(8)
```

Windows

The following message appears in the esmagent.log:

```
[03964] Update server: Error starting update service in run_program.; Failure to start service  
Esmupdate. Error number 6; Access is denied
```

3. Received from signature verification failed

When signature verification fails due to expired certificates, invalid Certificate Authority, the following message appears:

```
Signature verification failed for file <file>, error-code=-8
```

Note: gpgv 1.4.5 must be patched on both the ESM manager and the agent. This is compatible with version 1.0.6 already released.

Determining patch application

The following procedure describes the process for verifying that the Signature Fix has been applied to the ESM agent.

To determine proper patch application

1. In an ESM console, after deploying the Signature Fix, right-click on the agent. (On UNIX agents, a policy must be run before the new version is displayed.)
2. Click **Properties**. On the agent's ESM version, the following information is displayed:

ESM 6.5.0 and 6.5.2

Windows: 6.5 (2007/01/30 00:12)
aix-ppc64: 6.5 (2007/01/30 01:52)
aix-rs6k: 6.5 (2007/01/30 00:21)
hpux-hppa: 6.5 (2007/01/30 00:20)
hpux-ia64: 6.5 (2007/01/30 01:52)
lnx-ia64: 6.5 (2007/01/30 00:33)
lnx-x86: 6.5 (2007/01/30 00:16)
solaris-sparc: 6.5 (2007/01/30 00:19)
solaris-x86: 6.5 (2007/01/30 00:32)

ESM 6.0

Windows: 6.0 (2007/01/31 13:50)
aix-ppc64: 6.0 (2007/01/30 13:09)
aix-rs6k: 6.0 (2007/01/30 13:09)
hpux-hppa: 6.0 (2007/01/30 12:59)
hpux-ia64: 6.0 (2007/01/30 12:59)
lnx-ia64: 6.0 (2007/01/30 14:10)
lnx-x86: 6.0 (2007/01/30 12:52)
osf1-axp: 6.0 (2007/01/30 15:11)
solaris-sparc: 6.0 (2007/01/30 13:00)

ESM 5.5

Windows: 5.5 (2007/01/31 12:59)
aix-rs6k: 5.5 (2007/01/30 16:33)
hpux-hppa: 5.5 (2007/01/30 16:24)
lnx-x86: 5.5 (2007/01/30 16:27)
solaris-sparc: 5.5 (2007/01/30 16:34)

Symantec Certificates

The following table lists the content of the Symantec CA Certificate and the Symantec Code Sign Certificate:

Certificate File Name	Certificate Issuer	Certificate Subject	Valid From	Valid To	Public Key	Thumbprint
SymantecCACert.pem	CN = Symantec CSM CA OU = Symantec Compliance and Security Management Group O = Symantec Corporation L = Santa Monica S = California C = US	CN = Symantec CSM CA OU = Symantec Compliance and Security Management Group O = Symantec Corporation L = Santa Monica S = California C = US	Thursday, January 25, 2007 5:23:14 AM	Monday, January 25, 2027 5:23:14 AM	RSA 4096 Bits	e1 45 f2 99 2f 5b b0 03 b8 f5 72 a8 e5 fa 5e dc bc 2b 72 d8
SymantecCodeSignCert.pem	CN = Symantec CSM CA OU = Symantec Compliance and Security Management Group O = Symantec Corporation L = Santa Monica S = California C = US	CN = Symantec CSM Code Signing OU = Symantec Compliance and Security Management Group O = Symantec Corporation L = Santa Monica S = California C = US	Thursday, January 25, 2007 5:24:25 AM	Tuesday, January 24, 2017 5:24:25 AM	RSA 2048 Bits	52 01 a4 00 9e 4e de de 8e 3b 54 d5 8d f4 61 00 02 d5 da 53

Known issues

The following are known issues with the Signature Fix:

- On UNIX, core files are created on the agent #esm/bin/#platform directory when remotely upgrading to the Signature Fix. This does not affect the product. Remove the files manually.
- Solaris-x86 remote upgrade is not supported. Solaris-x86 agents must be updated manually.
- Aix-ppc64 remote upgrade is not supported. Aix-ppc64 agents must be updated manually.
- HP-UX 11i v2 (Itanium) remote upgrade is not supported on ESM 6.0. HP-UX 11i v2 (Itanium) agents must be updated manually on ESM 6.0.
- The Signature Fix is available for the AIX 4.3.1, AIX 4.3.3, SUN 2.6, OSF 4.0/5.1, and HP 10.20 platforms; however, upgrade to ESM 6.5.3 agent is not supported.
- After an agent is upgraded to the Signature Fix using the remote upgrade method, the correct version of the agent installed is found in the #esm/bin/#platform/version.dat file on the agent. The version displayed on the remote upgrade status screen is not valid.

Signature Fix remote upgrade is not supported for all special ESM 6.0 agents that were released post-ESM 6.0 on Symantec's security response Web site starting with SU21. You must install ESM 6.5.x Console/Manager to remote upgrade; otherwise, the agents must be manually patched. For example:

ESM 6.0 SUSE Linux Standard Server 8 Agent Setup

<<http://securityresponse.symantec.com/avcenter/security/ESM/esmSU18/suse-ix86/esmsuse.tar>>

ESM 6.0 Windows Server 2003 for 64-Bit Itanium-based Systems Agent Setup

<<http://securityresponse.symantec.com/avcenter/security/ESM/esmSU20/w3s-ia64/esm-w3s-ia64.exe>>

ESM 6.0 HP-UX 11i Itanium-based Systems Agent Setup

<<http://securityresponse.symantec.com/avcenter/security/ESM/esmSU21/hpux-ia64-setup.tgz>>