

Symantec Enterprise Security Manager Denial-of-Service Fix Update Guide

This document contains the procedures for updating Symantec ESM managers and agents to fix the race condition, denial-of-service issue. For detailed information about this issue see the *Enterprise Security Manager Denial-of-Service Security Advisory*.

Downloading the updates

Download the following archives as necessary, to update Symantec ESM 6.0 and 6.5.x managers and agents to fix the race condition issue.

- ESM60RaceConditionFix.zip (Symantec ESM 6.0)
- ESM65xRaceConditionFix.zip (Symantec ESM 6.5.x)

Extract the archive to a local directory. Each update package will contain an agent folder (ESM60RaceConditionFix\agent) and a manager folder (ESM60RaceConditionFix\manager). In each agent and manager folder are platform folders (for example: d:\download\ESM65\ESM65RaceConditionFix\agent\w3s-ix86) that contain the update files for each supported platform.

When manually updating ESM managers and ESM agents you will need to locate and copy update files from the appropriate platform folder (for example: d:\download\ESM65\ESM65RaceConditionFix\agent\w3s-ix86\esmagent.exe).

NOTE: Before remotely updating ESM 6.0 or 6.5.x agents you must move the manager folder out of the main folder (for example: d:\download\ESM65\ESM65RaceConditionFix\manager to d:\download\ESM65\manager). If the manager folder is not moved, it may interfere with the remote update of ESM agents.

Updating ESM managers manually

The following procedures describe the process of manually updating Symantec ESM managers on Windows and UNIX to fix the race condition issue. Each manager must be manually updated.

To update an ESM manager on Windows

- For example: Update an ESM 6.5 manager for Windows 2003 where the manager folder was extracted and moved to d:\download\ESM65\manager.
1. Stop the ESM Manager Service in Windows Service Manager.
 2. Rename the current esmmanager.exe file in c:\program files\symantec\esm\bin\w3s-ix86 if you want to save the old file.
 3. Copy the new esmmanager.exe file from d:\download\ESM65\manager\w3s-ix86.
 4. Paste the new esmmanager.exe file into c:\program files\symantec\esm\bin\w3s-ix86.
 5. Restart the ESM Manager Service.

To update an ESM manager on UNIX

- For example: Update an ESM 6.5 manager for Solaris 2.9 (SPARC) where the manager directory was extracted and moved to /myfix/esm65/manager.
1. Stop the ESM process using the esmsetup program.
 2. To rename the current esmd file, type the following command:
mv /esm/bin/solaris-sparc/esmd /esm/bin/solaris-sparc/esmd-before-race-fix
 3. To copy the new esmd file to the manager, type the following command
cp /myFix/esm65/manager/solaris-sparc/esmd /esm/bin/solaris-sparc/
- NOTE:** If you have an ESM agent on the same system as the manager, refer to the section below entitled, “Updating ESM agents manually” for directions on how to copy the version.dat file manually.
4. Restart the ESM process using the esmsetup program.

Remotely updating ESM agents

The following procedure describes the process of remotely updating Symantec ESM agents to fix the race condition issue for all supported ESM platforms.

NOTE: Before remotely updating ESM 6.0 or 6.5.x agents you must move the manager folder out of the main folder (for example: d:\download\ESM65\ESM65RaceConditionFix\manager to d:\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 LiveUpdate will update with the files necessary for the Race Condition Fix.
2. In the Symantec ESM console, in the Enterprise tree, locate an agent you wish to update.
3. Right click the agent, and then click **Enable LiveUpdate** to enable the agents that you wish to update.
4. Group ESM 6.0 agents and 6.5 agents into separate domains.
5. Click **LiveUpdate**, and then do one of the following:
 - In the ESM 6.0 console click **LiveUpdate from a CD or network path**.
 - In the ESM 6.5 console click **LiveUpdate from a directory**
6. Browse to the directory that contains the updated agent directory.

Make sure that you select the directory just above the **agent** folder. For example, if you are updating ESM 6.0 agents, select the **ESM60RaceConditionFix** directory.

You must update the ESM 6.0 agents and 6.5 agents in two separate passes. If you have the manager installed on c:\program files\symantec\esm, when you push each upgrade package, they go to the same directory (c:\program files\symantec\esm\update) on the manager. Before you push the second package you must rename the first, in case you need to redo the first agents again.

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 don't see the all the agent names in the left panel it means the agents must be LiveUpdate enabled.

- When the first batch of agents are successfully updated repeat steps 4 through 8 for the second agent version if necessary.

NOTE: During deployment of the Race Condition fix, traffic must be allowed on the agent on port 5599 or the firewall must be disabled. By default, Windows XP, Linux, and SuSE firewalls are enabled.

Check the status of the upgraded agents when the update is complete (see the section below).

To check the status of an agent update

- 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

In the Upgrade Status window, in the left pane 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 for UNIX and Linux or the new esmagent.exe for Windows) but that all of the other files remained the same.
Upgrade failed	If agent is for Solaris-x86 it is not supported. Solaris-x86 was released after the ESM 6.5.2 console was released.
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.
--	-------------------------------------------------------------------------------------------------------------------------------------

Updating ESM agents manually

The following procedures describe the process of manually updating Symantec ESM agents on Windows and UNIX to fix the race condition issue.

To manually update an ESM agent on Windows

- For example: Update an ESM 6.5 agent for Windows 2003 where the agent folder was extracted to d:\download\ ESM65RaceConditionFix\agent.
1. Stop the ESM Agent Service in Windows Service Manager.
 2. Rename the current esmagent.exe in c:\program files\symantec\esm\bin\w3s-ix86 if you want to save the old file.
 3. Copy the new esmagent.exe file from d:\download\ESM65RaceConditionFix\agent\w3s-ix86, and then paste it into c:\program files\symantec\esm\bin\w3s-ix86.
 4. Copy the new version.dat file from d:\download\ESM65RaceConditionFix\agent\w3s-ix86, and then paste it into c:\program files\symantec\esm\bin\w3s-ix86.
 5. Restart the ESM Agent Service.

To manually update an ESM agent on UNIX

- For example: Update an ESM 6.5 agent for Solaris 2.9 (SPARC) where the agent directory extracted to /myfix/ESM65RaceConditionFix/agent.
1. Stop the ESM process using the esmsetup program.
 2. To rename the current esmd file, type the following command:
mv /esm/bin/solaris-sparc/esmd /esm/bin/solaris-sparc/esmd-before-race-fix
 3. To copy the new esmd file to the agent, type the following command
cp /myFix/ESM65RaceConditionFix/agent/solaris-sparc/esmd /esm/bin/solaris-sparc/
 4. To copy the new version.dat file to the agent, type the following command
cp /myFix/ESM65RaceConditionFix/agent/solaris-sparc/version.dat /esm/bin/solaris-sparc/
 5. Wait for approximately 1 minute to allow the agent port to be unbound.
 6. Restart the ESM process using the esmsetup program.

Determining patch application

The following procedure describes the process of verifying that the Race Condition fix has been applied to the ESM agent.

To determine proper patch application

1. In an ESM console, after deploying the Race Condition 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 will display:

ESM60:

Windows: 6.0 (2006/02/28 16:18)
aix-rs6k: 6.0 (2006/04/18 9:43)
hpux-hppa: 6.0 (2006/06/05 16:20)
lnx-x86: 6.0 (2006/04/18 11:15)

ESM6.5.x:

Windows: 6.5 (2006/04/18 11:19)
aix-ppc64: 6.5 (2006/03/29 16:01)
aix-rs6k: 6.5 (2006/03/29 16:01)
hpux-hppa: 6.5 (2006/06/05 17:28)
hpux-ia64: 6.5 (2006/06/05 17:28)
lnx-ia64: 6.5 (2006/07/20 16:19)
lnx-x86: 6.5 (2006/05/05 11:08)
solaris-sparc: 6.5 (2006/03/29 15:52)
solaris-x86: 6.5 (2006/07/20 16:16)

For more information about installing or updating ESM components see the *Symantec Enterprise Security Manager Installation Guide*.

Copyright (c) 2006 by Symantec Corp.