

# Symantec ManHunt 3.0 or 3.0.1

## About Content Updates

Symantec ManHunt maintains the highest level of protection by periodically updating the content utilized by the software. This includes Security Updates (SUs) and Engine Updates (EUs), collectively referred to as Content Updates.

Security Updates provide the latest security content and vulnerability information, signatures, and event refinement rules. Engine Updates provide updates to the ManHunt engine and may include new supported protocols and engine enhancements.

All Content Updates are cumulative, so you need only install the latest version. If you do choose to install multiple versions, do so in the order that they become available. Never install an older, earlier update after installing a newer, later one.

## Installing Content Updates

With a SuperUser or Administrator account, you can install Content Updates (Security Updates and Engine Updates) using the ManHunt console.

### To install security updates and engine updates

- 1 Download the latest Security Update or Engine Update package from the Symantec web site, and save it on your local file system:  
<http://securityresponse.symantec.com>
- 2 In the ManHunt console, click **Update > Security Update** in the upper right corner. The history of security and engine updates is displayed.
- 3 Click **Add Update**, locate the Security Update or Engine Update file that you saved on your local file system, and select it.
- 4 Click **Add Security Update**.

The ManHunt console interprets the update file, and applies the updates to the correct files on the connected ManHunt node. ManHunt automatically propagates the changes throughout the cluster using its synchronization mechanism. Propagation causes a 30-second time lag after installation, before it is displayed on the ManHunt console.

---

**Note:** See the *Symantec ManHunt Administration Guide* to find out how to select and apply signatures to an interface (open [http://www.symantec.com/techsupp/enterprise/select\\_product\\_manuals.html](http://www.symantec.com/techsupp/enterprise/select_product_manuals.html), and click Intrusion Detection > Symantec ManHunt).

---

---

**Note:** For Engine Updates, make sure to set the binary synchronization parameter so that the Engine Update will propagate across the entire cluster.

---

## Editing the binary sync participation parameter

With a SuperUser or Administrator account, you can set the binary sync participation parameter after you have installed an Engine Update.

### To edit the binary sync participation parameter

- 1 In the ManHunt console, click **Configuration > ManHunt Node > Local Node Parameters**, and select a specific ManHunt node to configure.
- 2 In **ManHunt Configuration Parameters**, select the parameter from the scroll list in the left pane, and enter a boolean value in the lower right pane:
  - Set the value to 1 to enable binary synchronization.
  - Set the value to 0 to disable binary synchronization.
- 3 To apply changes and close the window, click **OK**.

## Restarting ManHunt sensors

The pre-update sensor runs until the next natural restart is triggered by the idle steering logic. Therefore, it is not necessary to restart the sensor process after installing Engine Updates. It is possible to do so, however, if desired.

### To restart a ManHunt sensor remotely

- 1 In the ManHunt console, right-click a monitoring or monitored interface object.
- 2 Edit the monitoring or monitored interface object.
- 3 Click **Restart Sensor**.

This restarts the sensor process without restarting other ManHunt processes or rebooting the ManHunt node.