

# Symantec™ Incident Manager Security Update 3 Release Notes

Security release for Symantec Incident Manager 3.0.



# SYMANTEC INCIDENT MANAGER 3.0

## Security Update 3 Release Notes

The software described in these Release Notes is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version [SU 3](#)

Copyright Notice

Copyright © 2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation. NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

### Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. Symantec Incident Manager, LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other product names that are mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. Technical Support's primary role is to respond to specific questions on product feature and function, installation, and configuration, as well as to author content for the Knowledge Base. Technical Support works in collaboration with the other areas within Symantec to answer your questions in a timely fashion.

Symantec Technical Support offers:

- A range of support options that gives you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week, worldwide, in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, that offer enhanced response and proactive security support

Please visit our Web site for current information on support programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

## Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to go to the Symantec licensing and registration site at: [www.symantec.com/certificate](http://www.symantec.com/certificate)

Alternatively, you may go to: [www.symantec.com/techsupp/ent/enterprise.html](http://www.symantec.com/techsupp/ent/enterprise.html)

Select the product that you wish to register and, from the Product Home Page, select the Licensing and Registration link.

## Contacting Technical Support

Customers with a current support agreement may contact Technical Support by phone or online at: [www.symantec.com/techsupp](http://www.symantec.com/techsupp)

Customers with Platinum support agreements may contact Platinum Technical Support by phone or online at: [www-secure.symantec.com/platinum/](http://www-secure.symantec.com/platinum/)

When contacting Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

## Customer Service

To contact Enterprise Customer Service online, go to [www.symantec.com](http://www.symantec.com), select the Global Site for your country, then choose Service and Support. 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 vendors)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

# Symantec Corporation Software License Agreement Symantec Incident Manager

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES (“SYMANTEC”) IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS “YOU” OR “YOUR”) ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING THE “AGREE” OR “YES” BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK THE “I DO NOT AGREE” OR “NO” BUTTON OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

## 1. License:

The software and documentation that accompanies this license (collectively the “Software”) is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a “License Module”) that accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Software, Your rights and obligations with respect to the use of this Software are as follows.

You may:

- A. use the number of copies of the Software as have been licensed to You by Symantec under a License Module. If the Software is part of a suite containing multiple Software titles, the number of copies You may use may not exceed the aggregate number of copies indicated in the License Module, as calculated by any combination of licensed Software titles. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software You are authorized to use on a single computer;
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;

- C. use the Software on a network, provided that You have a licensed copy of the Software for each computer that can access the Software over that network;
- D. use the Software in accordance with any written agreement between You and Symantec; and
- E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees in writing to the terms of this license.

You may not:

- A. copy the printed documentation that accompanies the Software;
- B. sublicense, rent, or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- C. use the Software as part of a facility management, timesharing, service provider, or service bureau arrangement;
- D. use a previous version or copy of the Software after You have received and installed a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;
- E. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;
- F. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received permission in a License Module; nor
- G. use the Software in any manner not authorized by this license.

## 2. Content Updates:

Certain Software utilize content that is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as “Content Updates”). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates that Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on

the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit the licensee to obtain and use Content Updates.

### 3. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to You. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money You paid for the Software. Symantec does not warrant that the Software will meet Your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

### 4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT, OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether or not You accept the Software.

### 5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items," as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

### 6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see [www.bxa.doc.gov](http://www.bxa.doc.gov)). Violation of U.S. law is strictly prohibited. You agree to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

### 7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America.

Otherwise, this Agreement will be governed by the laws of England and Wales. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals, and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment, or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module that accompanies this license or by a written document that has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland , or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

decrease utility of Content Updates subsequently provided to Licensee in accordance with Section 2, above.

## 8. Additional Uses and Restrictions:

The following terms and conditions supersede any conflicting terms and conditions above.

A. Permission to use the software to monitor Workstations, Servers or Network Devices does not constitute permission to make additional copies of the Software;

B. You may use the Software to monitor no more than the number of Workstations set forth under a License Module. "Workstation" means a desktop central processing unit primarily serving a single user.

C. You may use the Software to monitor no more than the number of Servers set forth under a License Module. "Server" means a central processing unit that acts as a server for other central processing units;

D. You may use the Software to monitor no more than the number of Network Devices set forth under a License Module. "Network Device" means a network-based intrusion detection system, firewall, router, switch or other similar network device.

E. If specified in a License Module, You may use the Software to monitor only the type of technology (e.g. antivirus, network intrusion detection, firewall) set forth under that License Module.

F. When an upgrade to the Software is made available to Licensee, Licensee must install such upgrade to use subsequently provided Content Updates. Failure to install any such Software upgrade(s) may impair or



# Security Update 3

## Release Notes

### **About Security Update 3**

Use this release to update Symantec Incident Manager 3.x. Symantec Incident Manager is a security management solution that correlates security events from Symantec and third-party products, manages all aspects of the incident life cycle, and helps focus resources on the highest priority incidents based on business impact.

Symantec Incident Manager contains a state-based Rules engine that reduces false positives and operational costs. The Rules engine correlates incoming attacks and automatically checks against known vulnerabilities that are identified by Symantec Vulnerability Assessment.

## What's new in Symantec Incident Manager

Security Update 3 includes updated support for the Symantec Event Manager for AntiVirus and Symantec™ Event Collector for CheckPoint 2.5 as well as updated tables, rules, and normalizer packages and Manhunt signatures. Mappings of SANS Top 20 events to the associated vulnerabilities are improved.

### Supported products

With the application of this security update, Symantec Incident Manager processes events from the following supported products:

- Symantec Event Manager for AntiVirus 2.0  
This is supported on SESA 2.0.1 and later. It is not supported on SESA 2.0.
- Symantec Event Collector for CheckPoint 2.5  
This is supported on SESA 2.0.1 and later.

### Correlation manager

Security Update 3 makes the following updates to the tables, rules, and normalizer files (TRN, KBT) in the Correlation manager/Rules engine:

- Adds new functionality to allow severity override.
- Updates values in the IP WatchList.tab file as of September 20, 2004.
- Adds VendorSeverity normalization support for SiteProtector, Snort, Manhunt, and RealSecure.

### Security content

Security Update 3 makes the following updates to the security content in Symantec Incident Manager:

- Adds support for updated Manhunt signatures.
- Adds support for improved SANS Top 20 coverage.
- Adds support for improved malicious code coverage.
- Includes mitigating strategies for exposures.

## Resolved issues

Security Update 3 resolves the following issues:

- Adds functionality that allows vendor severity override.
- Normalizes the vendor severity value consistently.
- Processes CheckPoint 2.0 and 2.5 events regardless of the SESA version.
- Runs the `lusim.bat -cm` command properly.
- `Virus_Outbreak` correctly increments counts of existing incidents without declaring new incidents.

## New Normalizer.properties

When an event is routed to Symantec Incident Manager 3.x, it first reaches the `Normalizer.properties` file. The `Normalizer.properties` file contains three sections and products that are integrated into Symantec Incident Manager. Incident Manager must be defined within both sections for the product events to be recognized.

The first section is an event source list. This section lists all of the products that pass events recognized by Incident Manager. When integrating products built with the Universal Collector for testing purposes, entries should be entered at the top of the event source list, followed by a `,\`. The entry should contain the product name. The following is correct when adding a product to the first section, where `NewCollectorName` is the name of the product to be integrated.

```
eventSourceList=\
    NewCollectorName,\
    ESM, \
```

The second section lists which fields from the product are available to be used to determine which normalizer to use for an event. This section starts with the line `'eventNormalizerIdentifier'` and contains a comma-separated list of schema fields.

The third section determines which normalizer should be used to process an event. When integrating Universal Collector entries for testing purposes, these entries should be added at the bottom of the normalizer file, in the appropriate section.

The following is an example of an appropriately integrated product.

```
NewCollector.product_id=30xx
NewCollector.Passthrough=false
NewCollector.TranslatorFile=NewCollector/NewCollector.trn
NewCollector.AlertTableFile=NewCollector/NewCollector.kbt
NewCollector.Validating=true
#####End of SUEC entries
```

As this file may be updated when Incident Manager liveupdates, it is important to break these entries into the appropriate sections. When the file is liveupdated, any entries that you added will be missing. Once the liveupdate is applied, locate the version of the normalizer.properties file with your edits in the file (Normalizer.bak). In a text editor, cut the sections containing your edits from the bottom and top of the file and place them in the designated area within the new normalizer.properties file, located in the Normalizer directory. Restart Apache Tomcat for your edits to take effect.

## New severity override function

Changes to the rule and normalizer let you override the severity assigned by Symantec Incident Manager and use your own severity for the default processing of the system. This does not change the severity of the event displayed within the GUI, but it does change how the system processes the event. Rules that are written to achieve this should be entered in the CM\_CustomerRules.rule file located in CorrelationManager\KnowledgeBase\CorrelationManager\RuleFiles\CM\_CustomerRules.rule.

For example, if your system is tuned to declare an incident on severity 4 events, and correlate to incidents on level 3 events (this is out of the box settings) but there is a honeypot on your network from which you do not want to see any events declare incidents, although you would like to preserve them in SESA, you may write the following rule:

```
If {SourceIP} is "xxx.xxx.xxx.xx" Then
Assign %Severity 1;
EndIf
```

This will cause all events from SourceIP xxx.xxx.xxx.xxx (where this is the IP of your honeypot) to be processed at a severity lower than the system would use in default processing.

If a vendor point product has been tuned to declare a different severity than what is assigned by Incident Manager. This can be done on many different levels. The following is an example of a rule in which a certain event, which is normally declared as a Severity 2 would use VendorSeverity instead.

```
If {GenericAlert} is "TFTP_Get" And {VendorSeverity} isnot "null"
Then
Assign %Severity {VendorSeverity};
EndIf
```

This causes the Vendor Severity to override the severity that Incident Manager assigns.

This is also useful if the point product has signatures that may not be recognized by Incident Manager or has customer-developed signatures.

In most point products, the severity is set to 3 and the event code becomes UnknownSignature. By combining the fields that are available, a customer can

now assign the severities they wish to be processed by default processing. In the following example, by assigning a known code to the DeviceAlert, the event can be processed appropriately by default processing (assigning a 4 or a 2) in this way either preventing the signature from being correlated into existing incidents or declaring its own incident when warranted.

```
If {DeviceAlert} is "10001" And {VendorSeverity} isnot "null" Then  
Assign %Severity {VendorSeverity};  
EndIf
```

The following products assign Vendor Severity:

- Snort
- ManHunt
- ISS RealSecure SiteProtector
- ISS RealSecure Network

## Frequently asked questions

### How do I install the Security Update release?

Security Update 3 is supported on version 3.0 of Symantec Incident Manager. You can install Security Update 2 by running Symantec LiveUpdate on the Symantec Incident Manager 3.0 computer.

Security Update 3 updates the Normalizer.properties file. If you have modified this file to integrate additional collectors, you must ensure that the appropriate lines are copied from the old file that will appear in Normalizer.bak to the new Normalizer.properties file that will be copied in with this LiveUpdate. You must restart Apache tomcat for your changes to take effect.

---

**Note:** If the Rules engine component and Symantec Incident Manager are installed on separate computers, you must run LiveUpdate on both computers. To enable the fixes and new rules, LiveUpdate restarts the Rules engine computer, which deletes all events and data in memory. Consequently, LiveUpdate should be run manually on the Rules engine computer during down time.

---

#### To run LiveUpdate for Symantec Incident Manager on Windows

- 1 Open a command prompt and change to the directory.
- 2 Type the following command:  
`C:\SESA\IncidentManager\liveupdate\lusim.bat -all`  
If you installed Symantec Incident Manager to a different location than the default location mentioned above, type that location instead.
- 3 Schedule updates in Windows using the AT command or the Scheduled Tasks utility.

#### To run LiveUpdate for Symantec Incident Manager on Solaris

- 1 On the computer on which the Symantec Incident Manager component is installed, become superuser.
- 2 At the command prompt, change to the /opt/Symantec/SESA/IncidentManager/liveupdate directory and type: `lusim.sh <argument>`

The table below describes the arguments that are associated with the Symantec Incident Manager components.

Argument for each Symantec Incident Manager component to LiveUpdate.

Arguments	Description
-all	Updates all Symantec Incident Manager components installed on the computer
-sim	Updates Incident Manager
-cm	Updates Correlation Manager
-simdata	Updates Security Response Package (SRP) component

For more information about using Symantec LiveUpdate, see the *LiveUpdate Administrator's Guide*.

---

**Note:** If all of the components of your Incident Manager system do not have access to the Internet, please contact Symantec support about how to accommodate these systems through an internal Live Update mechanism.

---

## How will I be notified when new Security Update releases or Response policies become available?

Your Symantec technical point of contact will advise you of Security Update releases for Symantec Incident Manager. Security Update releases are also available on the Platinum Web site.

