



# Intelligent Event Module™ for Tripwire® 2.3

## INTELLIGENT EVENT MODULE BASICS

The Tripwire 2.3 Intelligent Event Module (IEM) enables you to automate real-time monitoring of Tripwire® 2.3-47 and capture the critical information you need for effective enterprise security management.

The Tripwire 2.3 IEM provides ConsoleWorks® with a watch-list of text messages, including integrity violation alarms, policy update alerts, and system status warnings, produced by Tripwire. ConsoleWorks watches for these messages, called Events, in the data streams of your Tripwire installations.

### Events

When ConsoleWorks detects an Event, it alerts you to the Event as it is happening, records the circumstances surrounding the Event, and automatically performs the default or customer-configured responses associated with that Event.

### Scans

IEMs come with Events pre-arranged in logical groupings, called Scans™. Working with a Scan—or a combination of Scans—instead of hundreds of individual Events simplifies managing Events across your enterprise.

## TRIPWIRE 2.3 IEM AT A GLANCE

Events:	16
Scans:	1 Master 4 Event Severity 1 SNMP Trap
Filename:	<code>cw_iem-tripwire_tripwire-0004.bin</code>
License Required:	<code>CONWRKS-DB-TRIPWIRE.lic</code>
Connector Required:	Syslog
Optional Connector:	SNMP Trap Receiver

## USING THE TRIPWIRE 2.3 IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDi web site.
2. Import the IEM into ConsoleWorks.
3. Associate the Scans from the IEM with the Tripwire installations you want to monitor.

### To Download the IEM

1. Install the license for the Tripwire 2.3 IEM. To obtain this license, contact your TDi Solutions Team Manager ([sales@tditx.com](mailto:sales@tditx.com)).
2. Move to the TDi web site ([www.tditx.com/support\\_iemdownloads.asp](http://www.tditx.com/support_iemdownloads.asp)).
3. On the Product Downloads page, locate and click **Tripwire 2.3**.
4. In the Connect to support2.tditx.com dialog box, enter your User name and Password, and click **OK**. To obtain a User name and Password, contact TDi Support ([support@tditx.com](mailto:support@tditx.com)).
5. Save the file (`cw_iem-tripwire_tripwire-0004.bin`) to a directory accessible from your client workstation.

### To Import the IEM

1. On the ConsoleWorks main menu, click **Admin > Database > Import IEM**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-tripwire_tripwire-0004.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM import completed** message to appear on the page before associating the IEM's Scans.

### To Associate the Scans

Associate the Scans with the Tripwire installations you want ConsoleWorks to monitor. When you associate Scans with an application, you are specifying that ConsoleWorks scan the data streams of that application for the Events contained in the Scans.

#### Example: To associate the TRIPWIRE\_CRITICAL Scan

1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **TRIPWIRE\_CRITICAL**.
3. On the Scan: TRIPWIRE\_CRITICAL page, in the Unassociated Consoles column, select the check boxes next to the names of the Tripwire installations you want to associate with the Scan.
4. Click **Update Scan**.

For detailed instructions on associating Scans, please refer to the ConsoleWorks user's guide.



## SCANS AVAILABLE IN THE TRIPWIRE 2.3 IEM

---

The Tripwire 2.3 IEM contains a Master Scan and four Event Severity Scans and one SNMP trap Scan.

### Master Scan

The Master Scan, **TRIPWIRE**, is a container Scan. It references all the Event Severity Scans in the IEM. When you associate the Master Scan with an application, you are specifying that *ConsoleWorks* scan the data streams of that application for any of the IEM's 15 Severity-based Events.

### Event Severity Scans

The Tripwire 2.3 IEM contains four Event Severity Scans. Use one or more of these Scans to monitor Tripwire for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- TRIPWIRE\_CRITICAL 4 Events
- TRIPWIRE\_MAJOR 5 Events
- TRIPWIRE\_WARNING 2 Events
- TRIPWIRE\_INFORMATIONAL 4 Events

### SNMP Trap Scans

The Tripwire 2.3 IEM contains one SNMP trap Scan. Use this Scan to capture the SNMP trap triggered when Tripwire completes a host integrity check ([refer to Sample Event 2](#)).

## SAMPLE TRIPWIRE 2.3 IEM EVENTS

---

The Tripwire 2.3 IEM provides you with names, message texts, Severity ratings, explanations, and recommended responses for Events produced by Tripwire.

The following section displays samples of the information you receive for each Event in the Tripwire 2.3 IEM.

### Sample Event 1

**Name:** TRIPWIRE\_ICHECK\_FAIL  
**Message:** Integrity Check Failed:  
**Severity:** CRITICAL  
**Explanation:** Tripwire has failed its file integrity check.  
**Response:** Re-run the command with the `--verbose` option, examine the error status, fix the problem, then re-run the command.

### Sample Event 2

**Name:** TRIPWIRE\_000\_VIOLATION\_SNMP  
**Message:** Enterprise: 1.3.6.1.4.1.6818.1.1\$  
Tag Value: \*  
Specific Value: 0\$  
**Severity:** WARNING  
**OID:** 1.3.6.1.4.1.6818.1.0  
**Explanation:** This trap indicates that Tripwire has completed an integrity check.  
**Variables:** This trap reports 1 variable.  
**tripwireReportDetails** (DisplayString) (Binding #1) is a string with the format of:

- The text 'TWRReport',
- *hostname* of the machine on which the integrity check was run,
- *date* and *time* of report generation,
- total number of violations (V),
- maximum severity of violations (S),
- number of objects added, removed, and changed (A, R, C),
- number of low, medium, and high severity violations (L, M, H)

### Sample Event 3

**Name:** TRIPWIRE\_RPT\_MODOBJ  
**Message:** Modified object name:  
**Severity:** CRITICAL  
**Explanation:** A discrepancy has been detected by Tripwire. The resulting Tripwire report lists each object that has been modified. Note: This is not a Tripwire event. It is generated internally by a *ConsoleWorks* automated Action.  
**Response:** Examine the report and determine whether the discrepancy indicates the host has been compromised.

---

© 2007 TECSys Development, Inc. The information in this document is provided by TECSys Development, Inc. as-is without warranty of any kind and is subject to change without notice. The warranties for TECSys Development, Inc. solutions are set forth in the limited warranty statements accompanying such solutions. Nothing herein shall be construed as constituting an additional warranty. All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners. Portions of the technology within the *ConsoleWorks* server are protected under US Patent number 6,505,245. *ConsoleWorks* is a registered trademark of TECSys Development, Inc.