



INTELLIGENT EVENT MODULE BASICS

The ISS® (Internet Security Systems) IDS (Intrusion Detection System) Intelligent Event Module (IEM) enables you to automate real-time monitoring of ISS IDS products and capture the critical information you need for effective enterprise management.

The ISS IDS IEM provides ConsoleWorks® with a watch-list of SNMP trap IDs produced by ISS IDS products. ConsoleWorks watches for these IDs, called *Events*, in the data streams of your managed devices.

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.

ISS IDS IEM AT A GLANCE

Events:	5
Scans:	1
Filename:	<code>cw_iem-iss_ids-0001.bin</code>
License Required:	<code>CONWRKS-DB-ISIDSM50.lic</code>
Connector Required:	SNMP Trap Receiver

USING THE ISS IDS 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 Scan from the IEM with the devices you want to manage.

To Download the IEM

1. Install the license for the ISS IDS IEM. To obtain this license, contact your TDi Solutions Team Manager (sales@tditx.com).
2. Move to the TDi web site (www.tditx.com/support_iemdownloads.asp).
3. On the Product Downloads page, locate and click **ISS Intrusion Detection System**.
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).
5. Save the file (`cw_iem-iss_ids-0001.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-iss_ids-0001.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 Scan.

To Associate the Scan

Associate the Scan with the ISS IDS devices you want ConsoleWorks to monitor. When you associate a Scan with a device, you are specifying that ConsoleWorks scan the data streams of that device for the Events contained in the Scan.

Example: To associate ISSIDS Scan

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

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



SCAN AVAILABLE IN THE ISS IDS IEM

The ISS IDS IEM contains a single Scan, `ISSDS`. When you associate this Scan with a device, you are specifying that *ConsoleWorks* scan the data stream of that device for any of the IEM's five Events.

SAMPLE ISS IDS IEM EVENTS

The ISS IDS IEM provides you with names, SNMP trap IDs, Severity ratings, causes, objects, statuses, and explanations for Events produced by ISS IDS products.

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

Sample Event 1

Name: ISSIDS_HIGHPRIORITYEVENT
Trap ID: 1249903
Severity: MAJOR
Cause: A high-priority Event was encountered by the RealSecure engine.
Status: Current
Objects:
 Trap Name: `eventEntryName25`
 Time Event Discovered: `eventEntryTime25`
 Protocol Type: `eventEntryProtocol125`
 Source IP Address: `eventEntrySourceIpAddress25`
 Destination IP Address: `eventEntryDestinationIpAddress25`
 ICMP Type: `eventEntryIcmpType25`
 ICMP Code: `eventEntryIcmpCode25`
 Source Port: `eventEntrySourcePort25`
 Destination Port: `eventEntryDestinationPort25`
 Actions: `eventEntryUserActionList25`
 Variables/Values: `eventEntryEventSpecificInfo25`

Explanation: This trap is sent from a RealSecure engine whenever a high priority Event is encountered that the RealSecure engine is configured to send traps for. The details of the Event are contained in the trap.

Sample Event 2

Name: ISSIDS_LOGDATATRAP
Trap ID: 1249902
Severity: INFORMATIONAL
Cause: Configured log data was sent to the log file.
Status: Current
Objects:
 Time Log Entry Created: `logEntryTime`
 Sending Application: `logEntrySource`
 Object not described: `logEntryCategory`
 Object not described: `logEntryEventId`
 Object not described: `logEntryDescription`
 Object not described: `logEntryData`

Explanation: This trap is sent for certain types of log data, i.e., the configured types of log data that are sent as a trap.

© 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.