



INTELLIGENT EVENT MODULE BASICS

The Microsoft Windows Intelligent Event Module (IEM) enables you to automate real-time monitoring of Microsoft® Windows® operating system and capture the critical information you need for effective enterprise management.

The Microsoft Windows IEM provides ConsoleWorks® with a watch-list of text messages, including error codes, status warnings, and system alerts, produced by Windows NT®, Windows 2000®, and Windows XP®. ConsoleWorks watches for these messages, called Events, in the data streams of your managed assets.

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.

MICROSOFT WINDOWS IEM AT A GLANCE

Events:	1043
Scans:	1 Master 5 Event Severity
Filename:	<code>cw_iem-microsoft_windows-0002.bin</code>
License Required:	<code>CONWRKS-DB-MSWINDOWS.lic</code>
Connector Required:	Syslog

USING THE MICROSOFT WINDOWS IEM

To use this IEM, complete the following tasks:

1. Download the IEM from the TDI website.
2. Import the IEM into ConsoleWorks.
3. Associate the Scans from the IEM with the systems you want to manage.

Download the IEM

1. Install the license for the Microsoft Windows IEM. To obtain this license, contact TDI (sales@tditx.com).
2. Connect to the TDI website (www.tditx.com/support_iemdownloads.asp).
3. On the Product Downloads page, locate and click **Microsoft Windows**.
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-microsoft_windows-0002.bin`) to a directory accessible from your client workstation.

Import the IEM

1. On the main menu:
 - (ConsoleWorks 3) click **Admin > Database > Import IEM**.
 - (ConsoleWorks 4) click **EVENTS > IEMs**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-microsoft_windows-0002.bin`.
4. On the Import IEM page, click **Import IEM**, and wait for the **IEM import completed** or the **Import Successful** message to appear before attempting to associate the IEM's Scans.

Associate the Scans

Associate the Scans with the systems you want ConsoleWorks to monitor. When you associate Scans with a system, you are specifying that ConsoleWorks scan the data streams of that system for the Events contained in the Scans.

Example: To associate Scan MSWINDOWS-ERROR (ConsoleWorks 3)


1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **MSWINDOWS-ERROR**.



- On the Scan: MSWINDOWS-ERROR page, in the Unassociated Consoles column, select the check boxes next to the names of the systems you want to associate with the Scan.
- Click **Update Scan**.

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

Example: To associate Scan MSWINDOWS-ERROR (ConsoleWorks 4)

- On the main menu, click **EVENTS > Scans > Edit**.
The Edit Scan page appears.
- On the Name drop-down list, click **MSWINDOWS-ERROR**.
- Click , then click **Add**.
The Add Consoles selector appears.
- Select the Consoles you want associated with the Scan, review your choices in the Selected Consoles window, and click **OK**.
- Click **Save**.

SCANS AVAILABLE IN THE MICROSOFT WINDOWS IEM

The Microsoft Windows IEM contains a Master Scan and five Event Severity Scans.

Master Scan

The Master Scan, **MSWINDOWS**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with a system, you are specifying that ConsoleWorks scan the data streams of that system for any of the IEM's 1,043 Events.

Event Severity Scans

The Microsoft Windows IEM contains five Event Severity Scans. Use one or more of these Scans to monitor Windows systems for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- MSWINDOWS_ERROR 548 Events
- MSWINDOWS_FAILUREAUDIT 26 Events
- MSWINDOWS_INFORMATION 192 Events
- MSWINDOWS_SUCESSAUDIT 56 Events
- MSWINDOWS_WARNING 221 Events

SAMPLE MICROSOFT WINDOWS IEM EVENTS

The Microsoft Windows IEM provides you with names, message texts, Severity ratings, explanations, causes, recommended responses, and sources of more information for Events produced by Windows.

This section displays samples of the information you receive for each Event in the Microsoft Windows IEM.

Sample Event 1

Name: WIN_1101_MICROSOFT

Message: Source. * Microsoft *
EventID: 11001\$

Severity: ERROR

Explanation: Microsoft Firewall failed. The failure occurred during Initialization of reverse Network Address Translation (NAT).

Causes: The error is generated only if you are publishing any servers. It is looking for a registry key called "ClientSetsExcluded" which it does not create when you create the publishing rule.

Response: To fix it, go into the properties of every one of your published servers and click the "Applies To" tab. In the "Exceptions" area, add a dummy client set to the exceptions. Hit **OK** and wait a few seconds, then go back in and remove the exception. Adding and removing the exception creates the registry key that it is looking for and the errors stop. To check that the registry has been successfully modified, look in the event viewer, make a reference of the number after PNATServerMappings, go in the registry, look for the matching number and see if ClientSetsExcluded has been created under the number. For example, for the above error I would make a reference of {E1F6B393-EF5A-4870-FF9-0AFA3DAFBF9D} in the event viewer and see if ClientSetsExcluded has been created under it in the registry and then move to next occurrence of the error in the event viewer.

Further Discussion: *Microsoft Internet Security and Acceleration Server 2000*



© 2007–2010 TDI. The information in this document is provided by TDI as-is without warranty of any kind and is subject to change without notice. The warranties for TDI 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 TDI.