



Intelligent Event Module™ for Cisco® ASA 8.1

INTELLIGENT EVENT MODULE BASICS

The Cisco ASA 8.1 Intelligent Event Module (IEM) enables you to automate real-time monitoring of the Cisco® ASA 5500 series of network security devices and capture the critical information you need for effective and secure enterprise management.

The Cisco ASA 8.1 IEM provides ConsoleWorks® with a watch-list of text messages, including error codes, system warnings, and status alerts, produced by ASA 8.1. ConsoleWorks watches for these messages, called Events, in the data streams of your managed hardware 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.

CISCO ASA 8.1 IEM AT A GLANCE

Events:	1546
Scans:	1 Master 7 Event Severity
Filename:	<code>cw_iem-cisco_asa81-0002.bin</code>
License Required:	<code>CONWRKS-DB-CISCOASA.lic</code>
Connector Required:	Serial, Telnet or Telnet on Demand

USING THE CISCO ASA 8.1 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 devices you want to manage.

Download the IEM

1. Obtain a license for the Cisco ASA 8.1 IEM. To obtain this license, contact TDI (sales@tditx.com).
2. Connect to the TDI web site: (www.tditx.com/support_iemdownloads.asp).
3. On the Product Downloads page, locate and click **Cisco ASA 8.1**.
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-cisco_asa81-0002.bin`) to a directory accessible from your client workstation.

Import the IEM

1. On the main menu:
 - (*ConsoleWorks 3.x*) click **Admin > Database > Import IEM**.
 - (*ConsoleWorks 4.x*) click **Events > IEMs**.
2. On the Import IEM page, click **Browse**.
3. On the Choose file dialog box, locate and double-click `cw_iem-cisco_asa81-0002.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 Scans.

Associate the Scan


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

Example: To associate Scan ASA81_CRITICAL (ConsoleWorks 3.x)

1. On the ConsoleWorks main menu, click **Manage > Scans > Show Scans**.
2. On the Show Scans page, in the Scans column, click **ASA81_CRITICAL**.
3. On the Scan: ASA81_CRITICAL 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**.



Example: To associate Scan ASA81_CRITICAL (ConsoleWorks 4.0)

1. On the main menu, click **Events > Scans > Edit**.
The Edit Scan page appears.
2. On the Name drop-down list, click **ASA81_CRITICAL**.
3. Click , then click **Add**.
The Add Consoles selector appears.
4. Select the Consoles you want associated with the Scan, review your choices in the Selected Consoles window, and click **OK**.
5. Click **Save**.

SCANS AVAILABLE IN THE CISCO ASA 8.1 IEM

The Cisco ASA 8.1 IEM contains a Master Scan and seven Event Severity Scans.

Master Scan

The Master Scan, **ASA81**, is the top-level Scan. It references all the other Scans in the IEM. When you associate the Master Scan with a device, you are specifying that ConsoleWorks scan the data streams of that device for any of the IEM's 1,546 Events.

Event Severity Scans

The Cisco ASA 8.1 IEM contains seven Event Severity Scans. Use one or more of these Scans to monitor devices for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

• ASA81_ALERT	72 Events
• ASA81_CRITICAL	67 Events
• ASA81_ERROR	315 Events
• ASA81_WARNING	281 Events
• ASA81_NOTIFICATION	218 Events
• ASA81_INFORMATIONAL	343 Events
• ASA81_DEBUGGING	250 Events

SAMPLE CISCO ASA 8.1 IEM EVENTS

The Cisco ASA 8.1 IEM provides you with names, message texts, Severity ratings, causes, explanations, and responses for Events produced by Cisco devices.

The following section displays samples of the information you receive for each Event in the Cisco ASA 8.1 IEM.

Sample Event 1

Name: ASA81_101002
Message: %ASA-1-101002
Severity: ALERT
Cause: Failing primary or secondary failover cable.
Explanation: This is a failover message. This message reports that the failover cable is present but not functioning correctly. *Primary* can also be listed as *Secondary* for the secondary unit.
Response: Replace the failover cable.

Sample Event 2

Name: ASA81_106017
Message: %ASA-2-106017
Severity: CRITICAL
Cause: Denied IP because of Land Attack from *IP_address* to *IP_address*.
Explanation: This security appliance received a packet with the IP source address equal to the IP destination, and the destination port equal to the source port. This message indicates a spoofed packet designed to attack systems. This attack is referred to as a Land Attack.
Response: If this message persists, an attack may be in progress. However, the packet does not provide enough information to determine where the attack originates.

©2007–2009 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.