



INTELLIGENT EVENT MODULE BASICS

The Juniper Networks Netscreen ScreenOS 5.1 Intelligent Event Module (IEM) enables you to automate real-time monitoring of Juniper Networks® Netscreen ScreenOS and capture the critical information you need for effective enterprise security management.

The Juniper Networks Netscreen ScreenOS 5.1 IEM provides *ConsoleWorks*® with a watch-list of text messages, including attack alerts, threat warnings, and system status signals, produced by version 5.1 of the Netscreen ScreenOS operating system. *ConsoleWorks* watches for these messages, called Events, in the data streams of your managed firewall/IPSec VPN 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.

JUNIPER NETWORKS NETSCREEN SCREENOS 5.1 IEM AT A GLANCE

Events:	1129
Scans:	1 Master 7 Event Severity
Filename:	<code>cw_iem-juniper_netscreen-0002.bin</code>
License Required:	<code>CONWRKS-DB-NETSCREEN.lic</code>
Connector Required:	Syslog

USING THE JUNIPER NETWORKS NETSCREEN SCREENOS 5.1 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.

To Download the IEM

1. Install the license for the Juniper Networks Netscreen ScreenOS 5.1 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 **Juniper Networks Netscreen ScreenOS 5.1**.
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-juniper_netscreen-0002.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-juniper_netscreen-0002.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 firewalls and devices you want *ConsoleWorks* 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 NETSCR_CRITICAL Scan

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

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

SCANS AVAILABLE IN THE JUNIPER NETWORKS NETSCREEN SCREENOS 5.1 IEM

The Juniper Networks Netscreen ScreenOS 5.1 IEM contains a Master Scan and seven Event Severity Scans.

Master Scan

The Master Scan, **NETSCR**, 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 1129 Events.

Event Severity Scans

The Juniper Networks Netscreen ScreenOS 5.1 IEM contains seven Event Severity Scans. Use one or more of these Scans to monitor devices running Netscreen ScreenOS for Events based on their Severity level.

The IEM provides the following Event Severity Scans:

- NETSCR_EMERGENCY 3 Events
- NETSCR_ALERT 55 Events
- NETSCR_CRITICAL 116 Events
- NETSCR_ERROR 29 Events
- NETSCR_WARNING 50 Events
- NETSCR_NOTIFICATION 710 Events
- NETSCR_INFORMATIONAL 166 Events

SAMPLE JUNIPER NETWORKS NETSCREEN SCREENOS 5.1 IEM EVENTS

The Juniper Networks Netscreen ScreenOS 5.1 IEM provides you with names, message texts, Severity ratings, and affected subsystems for Events produced by Netscreen ScreenOS.

This section displays samples of the information you receive for each Event in the Juniper Networks Netscreen ScreenOS 5.1 IEM.

Sample Event 1

Name: NETSCR_PINGDEATHPROTO
Message: Ping of Death! From * to *, proto 1 (zone *, int *). Occurred * times.
Severity: EMERGENCY
Subsystem: ATTACKS

Sample Event 2

Name: NETSCR_CONNREFUSEDDNS
Message: Connection refused by the DNS server.
Severity: Critical
Subsystem: DNS

© 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.