

Intelligent Event Module Basics

The NetScreen® ScreenOS® Intelligent Event Module (IEM) enables you to automate real-time monitoring of Juniper® Networks' NetScreen ScreenOS. Use the NetScreen ScreenOS IEM to keep aware of ScreenOS alerts, respond automatically to network attacks, and capture the critical information you need for effective enterprise security management.

Events

The NetScreen ScreenOS IEM provides *ConsoleWorks*® with a watch-list of messages produced by NetScreen ScreenOS. These messages, called *Events*, include error codes, system warnings, and status alerts. *ConsoleWorks* uses these Events as the targets that it scans for in the data streams of your managed systems.

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 and 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.

NetScreen ScreenOS IEM at a Glance

Product version:	5.1
Events:	1129
Scans:	1 Master 169 Event
Filename:	cw_scan-netscreen-v1_0.bin
License required:	CONWRKS-DB-NETSCR.lic
Connector required:	Syslog

Using NetScreen ScreenOS IEM

To use this IEM, perform 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 system running NetScreen ScreenOS.

Note: You must obtain a license for the NetScreen ScreenOS IEM prior to using the module. To obtain the license, contact your TDi sales team manager (sales@tditx.com).

Download IEM

1. On the main menu of the TDi web site (www.tditx.com), click **Support > Product Downloads**.
2. On the Connect to www.tditx.com dialog box, enter your User name and Password. To obtain a User name and Password, contact TDi Support (support@tditx.com).
3. On the Support page, in the Product Downloads section, click the *ConsoleWorks* link appropriate for your version of *ConsoleWorks*.
4. On the Support page, in the *ConsoleWorks* Downloads section, under the Add-Ons heading, click **Intelligent Event Modules**.
5. On the Support page, in the *ConsoleWorks* Add-Ons section, locate and double-click **Juniper Networks NetScreen ScreenOS 5.1**.
6. Save the file (cw_scan-netscreen-v1_0.bin) to a directory accessible from your client workstation.

Import 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_scan-netscreen-v1_0.bin**.
4. On the Import IEM page, click **Import IEM**.

Associate Scan

When you associate a Scan with a system running NetScreen ScreenOS, you are specifying that *ConsoleWorks* monitor the NetScreen ScreenOS data stream from this system for the Events contained in that Scan.

ConsoleWorks offers you the following options for associating Scans:

- Associate individual Scans with one or more systems.
- Associate multiple Scans with one or more systems.
- Create a Scan containing only the Events you want monitored and associate this customized Scan with one or more systems.

Note: While you can associate any Scan with any application, system, or device, only associate a Scan with the application, system, or device appropriate for that Scan. For instance, associate only Cisco Scans with Cisco switches and McData Scans with McData switches.

Note: For detailed instructions on associating Scans, please refer to *ConsoleWorks 3.0 User Guide*.

Scans Available in the NetScreen ScreenOS IEM

The NetScreen ScreenOS IEM contains a Master Scan and 169 Event 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 system, you are specifying that *ConsoleWorks* scan this system for all 1129 Events contained in the IEM.

Event Scans

The NetScreen ScreenOS IEM contains 169 Event Scans organized into three configurations. You can have *ConsoleWorks* monitor for Events according to:

- Subsystem (51 Scans)
- Event Severity (7 Scans)
- Combination of subsystem and Severity (111 Scans)

Review the following Scan configurations to help you select Scans to associate with the systems in your enterprise.

Subsystem Scans

Use these Scans to monitor NetScreen ScreenOS 5.1 systems for Events messages sent from or to their components.

The IEM provides the following Scans for subsystems:

- NETSCR_ADDRESSES 3 Events
- NETSCR_ADMIN 38 Events
- NETSCR_ANTIVIRUS 27 Events
- NETSCR_ARP 6 Events
- NETSCR_ATTACKS 39 Events
- NETSCR_ATTACK_DATABASE 7 Events
- NETSCR_AUTH 70 Events
- NETSCR_BGP 15 Events
- NETSCR_DEVICE 33 Events
- NETSCR_DHCP 32 Events
- NETSCR_DIP 6 Events
- NETSCR_DNS 33 Events
- NETSCR_ENTITLEMENT 9 Events
- NETSCR_FLOW 7 Events
- NETSCR_HDLC 3 Events
- NETSCR_HIGH_AVAILABILITY 72 Events
- NETSCR_IGMP 22 Events

- NETSCR_IKE 67 Events
- NETSCR_INTERFACE 30 Events
- NETSCR_L2TP 23 Events
- NETSCR_LOGGING 19 Events
- NETSCR_MIP 1 Event
- NETSCR_MULTICAST 20 Events
- NETSCR_NSM 25 Events
- NETSCR_NSIRD 6 Events
- NETSCR_NTP 17 Events
- NETSCR_OSPF 15 Events
- NETSCR_PIM 41 Events
- NETSCR_PKI 121 Events
- NETSCR_POLICIES 8 Events
- NETSCR_PPP 4 Events
- NETSCR_PPPOE 17 Events
- NETSCR_RIP 9 Events
- NETSCR_ROUTE 20 Events
- NETSCR_SCHEDULE 1 Event
- NETSCR_SERVICE 3 Events
- NETSCR_SIP 24 Events
- NETSCR_SNMP 12 Events
- NETSCR_SSHV1 23 Events
- NETSCR_SSHV2 26 Events
- NETSCR_SSL 10 Events
- NETSCR_SYSLOG_AND_WEBTRENDS 20 Events
- NETSCR_SYSTEM 41 Events
- NETSCR_TRAFFIC_SHAPING 2 Events
- NETSCR_URL_FILTERING 37 Events
- NETSCR_USER 2 Events
- NETSCR_VIP 5 Events
- NETSCR_VIRTUAL_ROUTER 20 Events
- NETSCR_VPNS 21 Events
- NETSCR_VSYS 8 Events
- NETSCR_ZONE 9 Events

Severity Scans

Use these Scans to monitor NetScreen ScreenOS 5.1 for messages based on the Severity level of the Event.

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

- NETSCR_DNS_CRITICAL 3 Events
- NETSCR_DNS_NOTIFICATION 27 Events
- NETSCR_DNS_INFORMATIONAL 3 Events
- NETSCR_ENTITLEMENT_ALERT 6 Events
- NETSCR_ENTITLEMENT_NOTIFICATION 3 Events
- NETSCR_FLOW_NOTIFICATION 7 Events
- NETSCR_HDLC_NOTIFICATION 3 Events
- NETSCR_HIGH_AVAILABILITY_CRITICAL 36 Events
- NETSCR_HIGH_AVAILABILITY_NOTIFICATION 35 Events
- NETSCR_HIGH_AVAILABILITY_INFORMATIONAL 1 Event
- NETSCR_IGMP_NOTIFICATION 22 Events
- NETSCR_IKE_ALERT 2 Events
- NETSCR_IKE_CRITICAL 1 Event
- NETSCR_IKE_NOTIFICATION 3 Events
- NETSCR_IKE_INFORMATIONAL 61 Events
- NETSCR_INTERFACE_CRITICAL 2 Events
- NETSCR_INTERFACE_NOTIFICATION 28 Events
- NETSCR_L2TP_ALERT 3 Events
- NETSCR_L2TP_NOTIFICATION 14 Events
- NETSCR_L2TP_INFORMATIONAL 6 Events
- NETSCR_LOGGING_CRITICAL 3 Events
- NETSCR_LOGGING_WARNING 4 Events
- NETSCR_LOGGING_NOTIFICATION 11 Events
- NETSCR_LOGGING_INFORMATIONAL 1 Event
- NETSCR_MIP_NOTIFICATION 1 Event
- NETSCR_MULTICAST_ALERT 6 Events
- NETSCR_MULTICAST_CRITICAL 5 Events
- NETSCR_MULTICAST_NOTIFICATION 9 Events
- NETSCR_NSM_NOTIFICATION 21 Events
- NETSCR_NSM_INFORMATIONAL 4 Events
- NETSCR_NSRD_ERROR 1 Event
- NETSCR_NSRD_WARNING 3 Events
- NETSCR_NSRD_INFORMATIONAL 2 Events
- NETSCR_NTP_NOTIFICATION 17 Events
- NETSCR_OSPF_CRITICAL 5 Events
- NETSCR_OSPF_NOTIFICATION 3 Events
- NETSCR_OSPF_INFORMATIONAL 7 Events
- NETSCR_PIM_ALERT 10 Events
- NETSCR_PIM_NOTIFICATION 31 Events

Combination (subsystem & Severity) Scans

Use these Scans to monitor NetScreen ScreenOS 5.1 for messages associated with a specific subsystem and Severity level.

The IEM provides the following Scan combinations:

- NETSCR_ADDRESSES_NOTIFICATION 3 Events
- NETSCR_ADMIN_ALERT 15 Events
- NETSCR_ADMIN_WARNING 1 Event
- NETSCR_ADMIN_NOTIFICATION 12 Events
- NETSCR_ADMIN_INFORMATIONAL 10 Events
- NETSCR_ANTIVIRUS_ERROR 11 Events
- NETSCR_ANTIVIRUS_WARNING 6 Events
- NETSCR_ANTIVIRUS_NOTIFICATION 10 Events
- NETSCR_ARP_CRITICAL 2 Events
- NETSCR_ARP_NOTIFICATION 4 Events
- NETSCR_ATTACKS_EMERGENCY 3 Events
- NETSCR_ATTACKS_ALERT 8 Events
- NETSCR_ATTACKS_CRITICAL 18 Events
- NETSCR_ATTACKS_NOTIFICATION 10 Events
- NETSCR_ATTACK_DATABASE_NOTIFICATION 7 Events
- NETSCR_AUTH_WARNING 20 Events
- NETSCR_AUTH_NOTIFICATION 50 Events
- NETSCR_BGP_ALERT 1 Event
- NETSCR_BGP_NOTIFICATION 13 Events
- NETSCR_BGP_INFORMATIONAL 1 Event
- NETSCR_DEVICE_ALERT 2 Events
- NETSCR_DEVICE_CRITICAL 17 Events
- NETSCR_DEVICE_NOTIFICATION 14 Events
- NETSCR_DHCP_ALERT 1 Event
- NETSCR_DHCP_CRITICAL 1 Event
- NETSCR_DHCP_WARNING 1 Event
- NETSCR_DHCP_NOTIFICATION 14 Events
- NETSCR_DHCP_INFORMATIONAL 15 Events
- NETSCR_DIP_NOTIFICATION 6 Events

- NETSCR_PKI_NOTIFICATION 121 Events
- NETSCR_POLICIES_NOTIFICATION 8 Events
- NETSCR_PPP_NOTIFICATION 4 Events
- NETSCR_PPPOE_NOTIFICATION 17 Events
- NETSCR_RIP_CRITICAL 5 Events
- NETSCR_RIP_NOTIFICATION 3 Events
- NETSCR_RIP_INFORMATIONAL 1 Event
- NETSCR_ROUTE_CRITICAL 5 Events
- NETSCR_ROUTE_NOTIFICATION 15 Events
- NETSCR_SCHEDULE_NOTIFICATION 1 Event
- NETSCR_SERVICE_NOTIFICATION 3 Events
- NETSCR_SIP_NOTIFICATION 24 Events
- NETSCR_SNMP_NOTIFICATION 4 Events
- NETSCR_SNMP_INFORMATIONAL 8 Events
- NETSCR_SSHV1_CRITICAL 4 Events
- NETSCR_SSHV1_ERROR 4 Events
- NETSCR_SSHV1_WARNING 7 Events
- NETSCR_SSHV1_INFORMATIONAL 8 Events
- NETSCR_SSHV2_CRITICAL 4 Events
- NETSCR_SSHV2_ERROR 8 Events
- NETSCR_SSHV2_WARNING 7 Events
- NETSCR_SSHV2_NOTIFICATION 2 Events
- NETSCR_SSHV2_INFORMATIONAL 5 Events
- NETSCR_SSL_NOTIFICATION 7 Events
- NETSCR_SSL_INFORMATIONAL 3 Events
- NETSCR_SYSLOG_AND_WEBTRENDS_WARNING 1 Event
- NETSCR_SYSLOG_AND_WEBTRENDS_NOTIFICATION 19 Events
- NETSCR_SYSTEM_CRITICAL 2 Events
- NETSCR_SYSTEM_NOTIFICATION 16 Events
- NETSCR_SYSTEM_INFORMATIONAL 23 Events
- NETSCR_TRAFFIC_SHAPING_NOTIFICATION 2 Events
- NETSCR_URL_FILTERING_ALERT 1 Event
- NETSCR_URL_FILTERING_ERROR 5 Events
- NETSCR_URL_FILTERING_NOTIFICATION 31 Events
- NETSCR_USER_NOTIFICATION 2 Events
- NETSCR_VIP_CRITICAL 1 Event
- NETSCR_VIP_NOTIFICATION 4 Events

- NETSCR_VIRTUAL_ROUTER_NOTIFICATION 20 Events
- NETSCR_VPNS_CRITICAL 2 Events
- NETSCR_VPNS_NOTIFICATION 12 Events
- NETSCR_VPNS_INFORMATIONAL 7 Events
- NETSCR_VSYS_NOTIFICATION 8 Events
- NETSCR_ZONE_NOTIFICATION 9 Events

Sample Events

The NetScreen ScreenOS IEM provides you with names, messages, explanations, and recommended responses for NetScreen ScreenOS 5.1 Events.

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

Sample Event 1

Event Name:	NETSCR_UNEXPTERRMAIL
Event Message:	Unexpected error from e-mail server (state= <i>id_num</i>): <i>string</i>
Event Severity:	Warning
Explanation:	An e-mail server generated an error condition with the specified ID number. The NetScreen device typically generates this message when the mail server does not accept SMTP messages from the NetScreen device.
Response:	Check if the mail server is allowed to receive messages from the IP address of the NetScreen device. Add the IP address of the NetScreen device to the mail server application, if necessary.

Sample Event 2

Event Name:	NETSCR_CELLOBJNAME
Event Message:	cell_obj_name was { added deleted } policy <i>id_num</i> cell_name.
Event Severity:	Notification
Explanation:	An admin added or deleted an attack object from the specified policy.
Response:	Confirm that the action was appropriate and performed by an authorized admin.

Sample Event 3

Event Name:	NETSCR_DNSCACHETBL_REF
Event Message:	DNS cache table entries have been refreshed as result of external event.
Event Severity:	Notification
Explanation:	DNS entries were refreshed in the DNS cache table. This message may occur in response to an automatic update or other action by external sources, which may use configuration protocols like DHCP or PPPoE.
Response:	No recommended action.

Additional Information

For additional product information or to receive a free, live ConsoleWorks demonstration, please call 1.800.695.1258 or visit our web site at www.tditx.com.