



Sentinel SBC Notifications

Technical Bulletin

Table of Contents

Basic Concepts	3
How a notification OID is built	3
Essential Notifications	3
Required Information	10
Configuration Tasks	11
Setting the severity per service	11
Notification rules routing	12
Configuring the destinations	14
Example: alarms via SNMP, call events via syslog	15
Configuration script	15
Verifying the configuration	18
Basic Tasks	18
Disabling a notification rule entry without deleting it	18
Deleting a notification rule entry	18
Adding or removing a notification rule	18
Changing the severity of a service	18
Copyright Notice	19

Basic Concepts

A notification is a text message a service on the unit issues to signal something of interest to the administrator: a failed power supply, a link going down, a rejected call. Each one has a source service, a **NumKey** that identifies it within that service, and a severity.

Out of roughly 1,400 notifications documented across 42 services, this Technical Bulletin selects the **76** that tell a NOC whether the SBC is alive, carrying calls and not compromised, and describes how to configure the unit to send exactly those to the monitoring tools in place: an SNMP manager, a syslog server, or the logs of the unit itself.

Before leaving the unit, every notification goes through two consecutive filters. If it does not pass the first, the second never sees it:

- **Minimum severity per service.** Each service has a threshold, **MinSeverity**, which is *Warning* by default. Anything below it is not issued. In the web interface this is the **Service Notification Configuration** table.
- **Event notification rules.** Of what is issued, only notifications matching an **Nlm.Events** notification rule leave the unit. Each notification rule pairs a criteria expression with a destination. In the web interface this is the **Notification Events** table.

Note: The SIP endpoint and SIP proxy services (**SipEp**, **SipProxy**) are out of the scope of this document, and the firewalls (**Nfw**, **Lfw**) are not monitored. Signaling is covered by the **Sbc** service itself.

How a notification OID is built

Each notification sent via SNMP goes out as a trap whose OID is built from the service NumKey and the notification NumKey:

OID	Services	Service	Notifications	NumKey
.1.3.6.1.4.1.4935	.1000.100.200.100	.4400	.200.300	.740

The example resolves to **Sbc** (service 4400), notification 740, “*A limit is enforced*”. The one exception is the **Hardware** service, which hangs off .1.3.6.1.4.1.4935.1000.100.200.500.40000.200.300.

Important: Unit performance depends on the number of notifications it issues. Lowering a service to *Info* or *Debug* multiplies the events, so do it only where needed, as described in Setting the severity per service.

Essential Notifications

The notifications are grouped by domain and ranked by how the NOC should react. Messages are quoted exactly as the unit issues them, so they match the text received with the trap.

Priority	Meaning	Expected action	Count
P1	Service is down or about to be.	Page the on-call.	34
P2	Degraded, misconfigured or at risk.	Open a ticket, act within hours.	31

Priority	Meaning	Expected action	Count
P3	Trends, clear events and planned-change markers.	Context for troubleshooting.	11

Platform

If the chassis or its processes fail, the rest of the monitoring means nothing. Watch these on every physical unit, always.

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Dcm	30	The Power Supply Unit #%1\$d is in fault state. Power supply in fault. The chassis loses redundancy: a second failure takes the SBC out of service. Needs on-site intervention now.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.30
P1	Dcm	100	Critical fan fault(s) detected. All fans in fault, or the fan controller is not responding. Risk of thermal shutdown within minutes.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.100
P1	Dcm	70	Warning, disk wear level is at %1\$d percent. Storage wear at a critical level. Precedes loss of configuration, CDRs and logs. Plan a replacement.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.70
P1	Dcm	90	Temperature fault detected: %1\$s. Temperature above the configured threshold at the reported location. Check cooling and airflow before it escalates.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.90
P2	Dcm	80	Fan fault detected: %1\$s. A single fan in fault. There is still thermal margin, but it should open a ticket.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.80
P2	Dcm	10	The activation of a license for the unit with MAC address %1\$s has failed. License not activated: firmware too old, key built for another unit, or corrupted key. Can leave SBC capacity disabled.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.10
P3	Dcm	95	Temperature OK: %1\$s. Clears the temperature alarm. Map it as the clear event for 90.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.95
P3	Dcm	40	The Power Supply Unit #%1\$d recovered from the previous fault state. Clears the power supply alarm. Map it as the clear event for 30.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.2000.200.300.40
P1	All	60010	The service is no longer responding. Triggering the system watchdog. Watchdog triggered: the service hung and forces a restart of the service or the whole unit. The most important generic trap; subscribe it at least for Sbc, Scm, Bni, Eth and Hoc.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.<service>.200.300.60010
P1	All	60020	An internal error was encountered. Error code: %1\$s. Internal error in a software module. It can change system behaviour with no visible outage. Open a support case with the error code.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.<service>.200.300.60020

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	All	60200	The configuration is lost because the file is too big. The service configuration could not be loaded and is lost. The service starts without it.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.<service>.200.300.60200
P2	All	60210	The configuration will be lost because the file is too big. Early warning: the configuration will be lost at the next service restart unless it is reduced. This is the window to act before the incident.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.<service>.200.300.60210
P2	Scm	110	Service <%1\$s> has not responded to the last Start request within the allowed delay. A service did not start within the allowed time. Typical sign of a degraded start after a restart or an update.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.400.200.300.110
P2	Scm	40	Service <%1\$s> is stopped. Service stopped. When the service is Sbc, all traffic is down: treat it as an outage, not as information.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.400.200.300.40
P3	Scm	120	Service <%1\$s> has not responded to the last Stop request within the allowed delay. A service did not stop cleanly. Useful to correlate abnormal restarts.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.400.200.300.120
P3	Scm	20	Service <%1\$s> started successfully. Reveals unplanned restarts and clears service-down alarms.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.400.200.300.20

SBC service

The core of the unit: media and signaling interfaces, configuration apply, session limits and TLS transport. This is where an SBC stops carrying calls while still answering ping.

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Sbc	500	Internal error '%1\$d'. Internal error in the SBC service. Usually needs a unit restart. Escalate immediately.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.500
P1	Sbc	510	Invalid interfaces configuration. A MediaInterface or SignalingInterface problem keeps the SBC from starting fully: the unit is up but carries no traffic.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.510
P1	Sbc	1300	An internal error has occurred. Please restart the SBC service. The SBC service took too long to start and will not work properly until it is restarted.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1300
P1	Sbc	40	The %1\$s Network Interface used by the Media Interface %2\$d ('%3\$s') is not ready. The network interface of the media plane is not ready: disconnected or address unresolved. Audio is lost. Can be transient, so alarm after a 1–2-minute delay.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.40
P1	Sbc	130	The %1\$s Network Interface used by the Signaling Interface %2\$d ('%3\$s') is not ready. The network interface of the signalling plane is not ready. The SBC stops receiving SIP on that interface.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.130

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Sbc	730	An error during session creation: source=%1\$s:%2\$s, ruri=%3\$s, from=%4\$s, to=%5\$s, call-id=%6\$s, reason=%7\$s. Call failed because of a system error, typically routing. Alarm on rate, not on single events: it is the most direct indicator of calls failing.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.730
P1	Sbc	740	A limit is enforced: source=%1\$s:%2\$s, ruri=%3\$s, from=%4\$s, to=%5\$s, call-id=%6\$s, reason=%7\$s. Session rejected by a limit (CAC, rate limit or license); the reason field says which. Alarm on a rate threshold: a sign of saturation or of an attack.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.740
P1	Sbc	800	Alert. Reason=%1\$s. Generic SBC engine alert: the channel for abnormal conditions detected in real time. The Reason field carries the detail.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.800
P1	Sbc	1320	Cannot use the network address of the '%1\$s' Call Agent as a registration contact because the network is down. The network of a Call Agent used as a registration contact macro is down: registrations towards that side stop working.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1320
P2	Sbc	520	The Apply command was attempted on the configuration but failed. The configuration change was not applied. The SBC keeps running the previous one: what you see may differ from what runs.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.520
P2	Sbc	560	Invalid Configuration. No attempt to apply the configuration. Configuration validation failed and no apply was even attempted.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.560
P2	Sbc	10	Port conflict detected on Media Interface %1\$d ('%2\$s'). The RTP port range overlaps one already in use. The media plane cannot come up.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.10
P2	Sbc	100	Port conflict detected on Signaling Interface %1\$d ('%2\$s'). The signalling port is already in use. The SIP interface cannot come up.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.100
P2	Sbc	150	Signaling Interface at index %1\$d is not in Client mode, and no host certificate is available. Without a host certificate, TLS cannot run in Server or Both mode: secure signalling is down.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.150
P2	Sbc	820	A Tls connection to %1\$s:%2\$s was refused. The TLS peer is unreachable or not listening on that port. Secure trunk down.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.820
P2	Sbc	830	A Tls connection to %1\$s:%2\$s failed because the received certificate is not trusted. Peer certificate not trusted: malformed, expired, or CA not installed. Classic cause of a trunk outage after a certificate renewal.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.830
P2	Sbc	850	Tls connection to %1\$s:%2\$s was unexpectedly terminated. An established TLS connection dropped unexpectedly. Points to network or peer instability.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.850

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P2	Sbc	840	A Tls connection to %1\$s:%2\$s failed for unspecified reason. Unclassified TLS failure. Group it with 820, 830 and 850 into a single secure-trunk alarm.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.840
P2	Sbc	1360	The Sbc service has received too many events. The events queue will be truncated. The event queue is being truncated: notifications and call traces are being lost. Undermines the monitoring itself.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1360
P2	Sbc	1380	Tls is disabled. Host Validation is required but there are no CA certificates. CertificateValidation is set to HostName, but no CA is loaded, so TLS is disabled. A silent security exposure.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1380
P2	Sbc	1260	License activation parameters changed for the SBC service. License change: licensed capacity (sessions, registrations) may have changed. Review limits before the next busy hour.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1260
P3	Sbc	1290	802.1Q parameters changed for SBC service. 802.1Q change pending an SBC service restart to take effect.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.1290
P3	Sbc	770	Registration expired. aor=%1\$s, to=%2\$s, contact=%3\$s, source=%4\$s:%5\$s, from-ua=%6\$s. Registration expired in the cache or at the registrar. On its own it is noise; on rate it reveals mass loss of client registrations.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.770
P3	Sbc	710	Call Attempt: call-id=%1\$s, from=%2\$s, to=%3\$s ruri=%4\$s, res=%5\$s, src=%6\$s:%7\$s. Call failed or cancelled before being established. Basis for ASR. Send via syslog, not as a trap.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.710
P3	Sbc	720	Call End: call-id=%1\$s, from=%2\$s, to=%3\$s ruri=%4\$s, src=%5\$s:%6\$s, duration=%7\$s, reason=%8\$s. Call ended, with its cause: reply, rtp-timer-terminated, session-timer-terminated, no-ack. Basis for ACD and for detecting audio loss. Via syslog.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.4400.200.300.720

Network

Physical link, addressing, default route, DNS and clock. An SBC with a drifting clock or no DNS fails in ways that look like SIP problems.

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Eth	80	%1\$s link down detected. Physical link down with redundant ports enabled. Signals the loss of a network path.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.2400.200.300.80
P1	Eth	100	Switching over from %1\$s to redundant port %2\$s. Switched over to the redundant port: the unit keeps running but without protection. Repair the primary.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.2400.200.300.100

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Bni	120	DHCP lease expired for address %1\$s on the Network Interface %2\$s. The unit could not renew its lease and loses its IP address: outage on that interface.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.120
P1	Bni	270	Error: cannot enable network interface %1\$s because link %2\$s does not exist. The network interface cannot be enabled because the configured link does not exist. Configuration or hardware error.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.270
P1	Bni	285	Error: cannot enable network interface %1\$s because IP address %2\$s is already used on the network. Duplicate IP on the network. Causes intermittent outages that are hard to diagnose; always alarm.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.285
P1	Hoc	78	System clock is desynchronised. Clock out of sync. Breaks TLS certificate validation, CDRs and log correlation.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.78
P1	Hoc	85	Current default router is invalid. The default router is unreachable: no way out to networks that are not directly connected.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.85
P1	Hoc	88	No current default router defined. No default router defined. Same effect as the previous one.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.88
P1	Hoc	115	Current DNS configuration is invalid. Therefore, no DNS request will be issued. Without DNS, proxies, registrars and trap destinations cannot be resolved.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.115
P2	Bni	280	Error: cannot enable network interface %1\$s because IP address %2\$s is already used on network interface %3\$s. Address overlap between the unit's own interfaces.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.280
P2	Bni	110	DHCP lease refused for the Network Interface %1\$s. The DHCP server answered NAK. The interface is left without an address.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.200.200.300.110
P2	Eth	110	Switching back from %2\$s to primary port %1\$s. Back on the primary port. Closes the episode opened by event 100.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.2400.200.300.110
P2	Hoc	77	System clock is resynchronized from %1\$s to %2\$s. Clock jump. A large jump invalidates timestamps and can break TLS sessions.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.77
P2	Hoc	45	Current SNTP configuration is invalid. Therefore, no SNTP request will be issued. Invalid SNTP configuration: the unit stops synchronising and will drift towards event 78.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.700.200.300.45
P2	IpRouting	5	Unable to add route to %1\$s via %2\$s on link %3\$s. Route not installed in the routing table. Traffic to that destination has no path.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.3500.200.300.5
P3	Eth	90	%1\$s link up detected. Link recovered. Map it as the clear event for 80.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.2400.200.300.90

Security

Management access and certificates. Includes the trap that warns when the traps themselves cannot leave the unit.

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Snmp	50	The FQDN '%1\$s' cannot be resolved. The SNMP traps could not be sent to this destination. The SBC cannot send traps to that destination: monitoring goes blind. Also watch the unit with an external heartbeat.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.900.200.300.50
P1	Aaa	120	User %1\$s has been temporarily locked due to excessive login failures. Account locked after repeated login failures: a sign of a brute-force attack on management access.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.1000.200.300.120
P1	Aaa	110	The default users have been restored. The users table went back to defaults after a partial or factory reset. Default credentials are active: a security incident.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.1000.200.300.110
P1	Aaa	40	Radius server at %1\$s is unreachable. Without RADIUS there is no central authentication or accounting; the unit falls back to local users.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.1000.200.300.40
P2	Snmp	60	SNMPv3 authentication failed for user %1\$s. SNMPv3 authentication failed: unauthorised polling, or wrong credentials on the manager.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.900.200.300.60
P2	Cert	110	Transferred certificate is invalid. The downloaded certificate does not validate. The unit keeps the previous certificate, or none.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.2300.200.300.110
P2	Aaa	10	Authentication failed for user %1\$s. Failed login attempt. A single one is noise; on rate it feeds brute-force detection together with 120.	Info	.1.3.6.1.4.1.4935.1000.100.200.100.1000.200.300.10

Firmware and configuration

Updates, backups and storage. They catch the unit that booted degraded and the change that was left half done.

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Fpu	1000	Executing on recovery firmware. The unit booted on the recovery firmware after repeated failures. It runs degraded and needs an update.	Critical	.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.1000
P1	Fpu	3100	Firmware recovery required. Restarting system. Failure during an update; the unit is about to restart to recover. Imminent outage.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.3100
P1	Fpu	1400	Installation operation could not complete successfully. Maximum retries reached and the installation is aborted. The unit stays on the previous version.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.1400

Pri	Service	NumKey	Message and why it matters	Severity	Full OID
P1	Fpu	1100	Bad signature, bad construction, or corruption for file %1\$s in MFP %2\$s. Invalid signature or corrupted file. Besides the failed update, check the integrity of the source.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.1100
P1	Conf	10300	No restore data found for service %1\$s, a factory default reset will be performed. No restore data for the service: it will be reset to factory defaults. Configuration loss.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.10300
P2	Fpu	4200	Rollback operation could not complete successfully. The rollback failed and is aborted. The unit may be left in a mixed state.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.1300.200.300.4200
P2	Conf	10500	Restore Configuration Command failed. The configuration restore did not complete.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.10500
P2	Conf	5400	Backup Configuration Command failed. The backup was not created: there is no restore point before a change.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.5400
P2	Conf	3475	Scripts execution will not start again automatically after the reboot process. Reboot-loop protection triggered: provisioning scripts will not resume on their own, and the unit may be left half configured.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.3475
P2	File	20	Not enough space to store file. File system full. Affects captures, backups, certificates and firmware.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.2600.200.300.20
P3	Conf	3425	Reboot initiated to apply hardware settings. Reboot triggered by the RebootIfNeeded command. Helps tell planned restarts from crashes.	Warning	.1.3.6.1.4.1.4935.1000.100.200.100.800.200.300.3425
P3	Nlm	2500	Diagnostic logs transfer failed due to insufficient storage space. Diagnostic logs could not be saved for lack of space: evidence for the post-mortem is lost.	Error	.1.3.6.1.4.1.4935.1000.100.200.100.1100.200.300.2500

Required Information

Complete the following table to make sure you have the information required to complete the configuration steps.

Information	Value	Used in Step
Destination for each notification	For example, SNMP for alarms, syslog for call traces	Routing the notifications
SNMP manager address and port, if Send via SNMP is used	NMS_IP:162	Configuring the destinations
Syslog server address and port, if Send via Syslog is used	SYSLOG_IP:514	Configuring the destinations
Free rows in the Nlm.Events table	1 to 5, plus one per additional destination	Routing the notifications

Configuration Tasks

Setting the severity per service

With the default value, the **8 Info notifications** on the list are never issued: the hardware alarm clears, service starts and stops, call traces and authentication failures. Lower the services that issue them to *Info* and leave the rest at *Warning*.

Steps

- 1) Go to **System / Event Log**.
 - 2) In the **Service Notification Configuration** table, click + next to **Service** to expand the list of services.
 - 3) Set **Severity** for each service to the value in the table below. Services not listed stay at **Warning**.
- Note:** This setting only allows the service to issue the notification. A matching event notification is still needed for it to reach the destination.
- 4) Click **Apply**.

Result

Service Notification Configuration		
Service	Severity	
Authentication, Authorization, and Accounting (AAA):	Info	
Basic Network Interface (BNI):	Warning	
Certificate Manager (CERT):	Warning	
Command Line Interface (CLI):	Warning	
Configuration Manager (CONF):	Warning	
Device Control Manager (DCM):	Info	
Element Management System for Virtuo (EMS):	Warning	
Ethernet Manager (ETH):	Warning	
File Manager (FILE):	Warning	
Firmware Pack Updater (FPU):	Warning	
Host Configuration (HOC):	Warning	
IP Routing (IPROUTING):	Warning	
Local Quality Of Service (LQOS):	Warning	
Local Firewall (LFW):	Warning	
Notifications and Logging Manager (NLM):	Warning	
Process Control Manager (PCM):	Warning	
Session Border Controller (SBC):	Info	
Service Controller Manager (SCM):	Info	
Web (WEB):	Warning	

Figure 1 – Service Notification Configuration table with factory values. Change AAA, DCM, SBC and SCM to Info.

Service	NumKey	Severity	Reason
Authentication, Authorization, and Accounting (AAA)	1000	Info	Aaa.10
Basic Network Interface (BNI)	200	Warning	Default value: enough for what is monitored
Certificate Manager (CERT)	2300	Warning	Default value: enough for what is monitored
Configuration Manager (CONF)	800	Warning	Default value: enough for what is monitored
Device Control Manager (DCM)	2000	Info	Dcm.40, Dcm.95
Ethernet Manager (ETH)	2400	Warning	Default value: enough for what is monitored
File Manager (FILE)	2600	Warning	Default value: enough for what is monitored
Firmware Pack Updater (FPU)	1300	Warning	Default value: enough for what is monitored
Host Configuration (HOC)	700	Warning	Default value: enough for what is monitored
IP Routing (IPROUTING)	3500	Warning	Default value: enough for what is monitored
Notifications and Logging Manager (NLM)	1100	Warning	Default value: enough for what is monitored
Service Controller Manager (SCM)	400	Info	Scm.20, Scm.40
Session Border Controller (SBC)	4400	Info	Sbc.710, Sbc.720, Sbc.770
Snmp (set by script)	900	Warning	Default value: enough for what is monitored

CLI, EMS, LQOS, LFW, PCM and WEB appear in the web interface table but are not monitored: leave them at *Warning*.

Notification rules routing

The 76 notifications are routed with 5 notification rules, one per domain. Each notification rule pairs a criteria expression, which selects the notifications, with an action, which sets where they are sent. The criteria of each notification rule lists every NumKey in the group as service.notification, comma-separated with no spaces. The **Criteria** field accepts at most 512 characters.

Choosing a destination

The unit offers five destinations. Choose, for each notification rule, the one that fits the monitoring tools in place:

Action	Where the notifications go	Typical use
Send via SNMP	Traps to the SNMP managers set in Snmp.TrapDest .	Real-time alarms on an NMS.
Send via Syslog	Messages over UDP to the syslog server set in Nlm.SyslogRemoteHost .	Central log collection, SIEM, history, and high-volume events such as call traces.
Log Locally	The Local Log table of the unit (System / Local Log). Limited size, erased when the unit restarts.	Troubleshooting on the unit itself.
Log to File	A file in the file system of the unit.	Keeping a record on the unit across restarts.
Send via SIP	SIP NOTIFY messages through the SIP endpoint service.	Collecting events over SIP. The SIP endpoint service is out of the scope of this document.

Note: A notification can reach more than one destination: add one notification rule per destination with the same criteria, for example one with **Send via SNMP** for the NMS and another with **Send via Syslog** for the history. Each notification rule takes one of the 100 rows of the **Notification Events** table.

Adding the notification rules

Steps

- 1) Go to **System / Event Log**.
- 2) In the **Notification Events** table, paste the criteria of the first notification rule in the table below into **Criteria**.

Note: Choosing a **Service** and **Notification** from the selection lists fills in **Criteria** automatically, but for a single service per row. These notification rules combine several services, so pasting the full criteria is faster.

- 3) From the **Action** selection list, choose the destination for that group, as described in Choosing a destination.
- 4) Click **+** to add the row.
- 5) Repeat steps 2 to 4 for each notification rule, and for each additional destination of a notification rule.
- 6) Click **Apply**.

Result

Index	Group	Notif.	Criteria
1	Platform	18	4400.C,2000.C,400.C,200.C,2400.C,700.C,1300.C,1000.C,900.C,2300.C,3500.C,800.C,1100.C,2600.C,400.20,400.40,400.110,400.120,2000.10,2000.40,2000.80,2000.90,2000.95

Index	Group	Notif.	Criteria
2	SBC service	24	4400.10,4400.40,4400.100,4400.130,4400.150,4400.510,4400.520,4400.560,4400.710,4400.720,4400.730,4400.740,4400.770,4400.800,4400.820,4400.830,4400.840,4400.850,4400.1260,4400.1290,4400.1300,4400.1320,4400.1360,4400.1380
3	Network	16	200.110,200.120,200.270,200.280,200.285,700.45,700.77,700.78,700.85,700.88,700.115,2400.80,2400.90,2400.100,2400.110,3500.5
4	Security	7	900.50,900.60,1000.10,1000.40,1000.110,1000.120,2300.110
5	Firmware and configuration	11	800.3425,800.3475,800.5400,800.10300,800.10500,1100.2500,1300.1100,1300.1400,1300.3100,1300.4200,2600.20

Note: The Platform notification rule uses <service>.C instead of listing each Critical notification. In the 14 monitored services every Critical notification is on the list, so this selects exactly the same set with 14 criteria instead of 60. Listed one by one, they would exceed the 512-character limit.

Configuring the destinations

Configure only the destinations chosen for the notification rules.

SNMP

Notifications routed with **Send via SNMP** go out as traps to the destinations in **Snmp.TrapDest**: up to five, comma-separated, port optional. Each trap carries the OID of its notification, as described in How a notification OID is built.

Steps

- 1) Set **Snmp.TrapDest** to the SNMP manager address and port, for example **NMS_IP:162**.
- 2) Make sure **Snmp.EnableTrap** is set to **Enable**.

Important: The trap queue holds 100 notifications per second, and once it is full, new traps replace older ones. On an SBC carrying traffic, per-call traces can push out a critical trap. Keep high-volume notifications, such as call traces, out of the SNMP notification rules.

Note: If a destination in **Snmp.TrapDest** is an FQDN that does not resolve, that destination stops receiving traps. The unit reports it with **Snmp.50**, which is on the list as P1.

Syslog

Notifications routed with **Send via Syslog** are sent over UDP to the server set in **Nlm.SyslogRemoteHost**, or in **Syslog Configuration / Remote Host** on the **System / Event Log** page. With no port, 514 is used. The layout of each message is set with **Nlm.SyslogMessageFormat**.

Local log

Notifications routed with **Log Locally** are kept in the Local Log table, shown in **System / Local Log**. Click **Refresh Local Log** to see the latest entries and **Clear Local Log** to empty it. When the table is full, the oldest entry is erased to make room for the new one, and the whole table is erased when the unit restarts.

File

Notifications routed with **Log to File** are written to a file in the file system of the unit. The file name, maximum size and number of files are set with **Nlm.LogFileName**, **Nlm.LogFileMaxSize** and **Nlm.LogFileMaxNb**.

Note: Log to File is not available on the 4102S and C7 Series.

Example: alarms via SNMP, call events via syslog

A common split sends the alarms to the SNMP manager and the high-volume call events to syslog. **Sbc.700** (Call Start), **Sbc.710** (Call Attempt), **Sbc.720** (Call End) and **Sbc.770** (Registration expired) are issued once per call or registration: they feed the ASR and ACD metrics, but on an SBC with real traffic they would compete with the alarms for the trap queue. Remove them from the SBC service notification rule and add a second notification rule that sends them via syslog:

```
# SBC service rule, without the call event
Nlm.insertEvent index=1
Nlm.Events[Index=1].Activation = Enable
Nlm.Events[Index=1].Type = Notification
Nlm.Events[Index=1].Criteria =
"4400.10,4400.40,4400.100,4400.130,4400.150,4400.510,4400.520,4400.560,4400.730,4400.740,4400.800,4400.820,440
0.830,4400.840,4400.850,4400.1260,4400.1290,4400.1300,4400.1320,4400.1360,4400.1380"
Nlm.Events[Index=1].Action = SendViaSnmp

# Call event logs (syslog)
Nlm.insertEvent index=2
Nlm.Events[Index=2].Activation = Enable
Nlm.Events[Index=2].Type = Notification
Nlm.Events[Index=2].Criteria = "4400.700,4400.710,4400.720,4400.770"
Nlm.Events[Index=2].Action = SendViaSyslog

# Syslog server: fill in the real one
# Nlm.SyslogRemoteHost = "syslog.example.net:514"
```

Result

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable	4400.10,4400.40,4400.100,4400.130,4	--- Suggestion ---	v	Send Via SNMP	Valid	-
2	Enable	4400.700,4400.710,4400.720,4400.770	--- Suggestion ---	v	Send Via Syslog	Valid	-
							+

Figure 2 –Notification Events table with SBC example values.

Configuration script

The tasks above can also be applied in one go with a configuration script. This is the complete script, with the severities per service and the notification rules routing. In the script every notification rule uses **SendViaSnmp** as an example: set the **Action** of each notification rule to the destination chosen for it.

```
# =====
# SBC notifications – per-service MinSeverity and Nlm.Events notification rules
#
# 76 notifications, 5 notification rules, priorities P1,P2,P3.
# Indexes used: 1..5 of the 100 rows the table accepts.
#
# Each notification rule creates its row with "Nlm.insertEvent index=N" and is then
# addressed as "Nlm.Events[Index=N].<parameter>".
#
# Criteria syntax: (service NumKey).(notification NumKey), comma-
# separated, no spaces. Maximum 512 characters per row.
# =====

# -----
# Step 1. Minimum severity per service (Service Notification Configuration).
# Filters before Nlm.Events; Warning by default. Lowered to Info only
# where the list includes Info notifications.
# -----
Sbc.MinSeverity = Info          # Sbc.710, Sbc.720, Sbc.770
Dcm.MinSeverity = Info          # Dcm.40, Dcm.95
Scm.MinSeverity = Info          # Scm.20, Scm.40
Bni.MinSeverity = Warning
Eth.MinSeverity = Warning
Hoc.MinSeverity = Warning
Fpu.MinSeverity = Warning
Aaa.MinSeverity = Info          # Aaa.10
Snmp.MinSeverity = Warning
Cert.MinSeverity = Warning
IpRouting.MinSeverity = Warning
Conf.MinSeverity = Warning
Nlm.MinSeverity = Warning
File.MinSeverity = Warning

# -----
# Step 2. Notification rules routing (Notification Events), one per group.
# -----

# --- Platform
# 18 notifications, 23 criteria (Critical 9, Error 3, Info 4, Warning 2)
# The 9 Critical notifications of the 14 monitored services are compacted as "<service>.C".
Nlm.insertEvent index=1
Nlm.Events[Index=1].Activation = Enable
Nlm.Events[Index=1].Type = Notification
Nlm.Events[Index=1].Criteria =
"4400.C,2000.C,400.C,200.C,2400.C,700.C,1300.C,1000.C,900.C,2300.C,3500.C,800.C,1100.C,2600.C,400.20,400.40,40
0.110,400.120,2000.10,2000.40,2000.80,2000.90,2000.95"
Nlm.Events[Index=1].Action = SendViaSnmp

# --- SBC service
# 24 notifications, 24 criteria (Error 14, Info 3, Warning 7)
Nlm.insertEvent index=2
Nlm.Events[Index=2].Activation = Enable
Nlm.Events[Index=2].Type = Notification
Nlm.Events[Index=2].Criteria =
"4400.10,4400.40,4400.100,4400.130,4400.150,4400.510,4400.520,4400.560,4400.710,4400.720,4400.730,4400.740,440
0.770,4400.800,4400.820,4400.830,4400.840,4400.850,4400.1260,4400.1290,4400.1300,4400.1320,4400.1360,4400.1380
"
Nlm.Events[Index=2].Action = SendViaSnmp

# --- Network
# 16 notifications, 16 criteria (Error 7, Warning 9)
Nlm.insertEvent index=3
Nlm.Events[Index=3].Activation = Enable
Nlm.Events[Index=3].Type = Notification
Nlm.Events[Index=3].Criteria =
"200.110,200.120,200.270,200.280,200.285,700.45,700.77,700.78,700.85,700.88,700.115,2400.80,2400.90,2400.100,2
400.110,3500.5"
Nlm.Events[Index=3].Action = SendViaSnmp
```

```
# --- Security
# 7 notifications, 7 criteria (Error 2, Info 1, Warning 4)
Nlm.insertEvent index=4
Nlm.Events[Index=4].Activation = Enable
Nlm.Events[Index=4].Type = Notification
Nlm.Events[Index=4].Criteria = "900.50,900.60,1000.10,1000.40,1000.110,1000.120,2300.110"
Nlm.Events[Index=4].Action = SendViaSnmp

# --- Firmware and configuration
# 11 notifications, 11 criteria (Error 8, Warning 3)
Nlm.insertEvent index=5
Nlm.Events[Index=5].Activation = Enable
Nlm.Events[Index=5].Type = Notification
Nlm.Events[Index=5].Criteria =
"800.3425,800.3475,800.5400,800.10300,800.10500,1100.2500,1300.1100,1300.1400,1300.3100,1300.4200,2600.20"
Nlm.Events[Index=5].Action = SendViaSnmp

# -----
# Trap transport. Fill in TrapDest with the real collectors:
# up to 5 comma-separated destinations, port optional.
# -----
# Snmp.TrapDest = "10.0.0.10:162,nms.example.net:162"
# Snmp.EnableTrap = Enable

# Check after applying: every row must show
# Nlm.Events[N].ConfigStatus = Valid. Invalid means a syntax error
# in Criteria; NotSupported, a resource limitation.
```

Important: Before applying the script, set the Action of each notification rule and configure the destinations in use. For SNMP, fill in **Snmp.TrapDest** at the end: it is commented out so that no traps go to an example address.

Note: The script uses indexes 1 to 5 of Nlm.Events, which accepts 100 rows. If the unit already has notification rules on those indexes, move the new ones to free indexes, or delete the old ones first as described in Basic Tasks.

Result

Notification Events							
#	Activation	Criteria	Service	Notification	Action	Config Status	
1	Enable	4400.C,2000.C,400.C,200.C,2400.C,70	--- Suggestion ---		Send Via SNMP	Valid	—
2	Enable	4400.10,4400.40,4400.100,4400.130,4	--- Suggestion ---		Send Via SNMP	Valid	—
3	Enable	200.110,200.120,200.270,200.280,200	--- Suggestion ---		Send Via SNMP	Valid	—
4	Enable	900.50,900.60,1000.10,1000.40,1000.	--- Suggestion ---		Send Via SNMP	Valid	—
5	Enable	800.3425,800.3475,800.5400,800.103	--- Suggestion ---		Send Via SNMP	Valid	—
							+

Figure 3 –Notification Events table with example values.

Verifying the configuration

Steps

- 1) Check the status of each notification rule in **Nlm.Events[Index=N].ConfigStatus**. It must read **Valid**.
 - **Invalid**: syntax error in **Criteria** or **Action**. The most common cause is a space inside a criterion.
 - **NotSupported**: the notification rule is valid but the unit cannot serve it, for instance because of a resource limit.
- 2) Check **<Service>.NeedRestartInfo** on the services whose severity you changed, to see whether they need a restart.
- 3) Confirm that the notifications reach the chosen destinations: traps with the prefix .1.3.6.1.4.1.4935.1000.100.200.100 on the SNMP manager, messages on the syslog server, or entries in **System / Local Log**.

Basic Tasks

Disabling a notification rule entry without deleting it

```
Nlm.Events[Index=3].Activation = Disable
```

The entry is kept and can be re-enabled with **Enable**. Useful for silencing a group during maintenance.

Deleting a notification rule entry

```
Nlm.Events[Index=3].Delete
```

Important: Run it only on rows that exist: a Delete on a missing row aborts the script.

Adding or removing a notification rule

Edit the **Criteria** of the notification rule for its domain: add or remove the service.NumKey pair, with no spaces, and keep the line within 512 characters. If the notification is Info, also check that its service is set to **Info**.

Changing the severity of a service

In **System / Event Log**, change the service **Severity** value and click **Apply**, or set **<Service>.MinSeverity**. With **Disable**, the service stops issuing notifications altogether, Critical ones included.

Copyright Notice

Copyright © 2026 M5 Technologies.

This document contains information that is proprietary to M5 Technologies.

M5 Technologies reserves all rights to this document as well as to the Intellectual Property of the document and the technology and know-how that it includes and represents.

This publication cannot be reproduced, neither in whole nor in part, in any form whatsoever, without written prior approval by M5 Technologies.

M5 Technologies reserves the right to revise this publication and make changes at any time and without the obligation to notify any person and/or entity of such revisions and/or changes



130, rue Sauvé
Sherbrooke (Québec)
J1L 0A7 Canada
m5technologies.com