### sendsyslog

Sends syslog message to the specified IP address.

#### Syntax

sendsyslog [OPTIONS] dst=IP\_ADDR

Required Parameter

**dst=IP\_ADDR**

IP address of syslog server

Optional Parameter

**format=json|txt**

Format of the log to be sent: either json or txt (default: txt).

* json: Converts all data received as input into JSON format and transmits it
* txt: Transmits the string value of the **line** field as it is.

**port=INT**

Port number of syslog server (default: 514). This designates a value from 1 to 65535 for the port number.

**pri=INT**

PRI constant value defined in RFC 5424: <https://tools.ietf.org/html/rfc5424> (default: 134, meaning Facility: local0, Severity: Info).

The PRI constant is calculated as a value that adds SEVERITY to a value multiplied by 8 in FACILITY. The following table is a table that is configured as a value calculated according to the calculation formula.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Facility(↓)<br />Severity(→) | 0/Emer | 1/Alert | 2/Crit | 3/Error | 4/Warn | 5/Notice | 6/Info | 7/Debug |
| 0 / kern | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 / user | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 / mail | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 3 / deamon | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
| 4 / auth | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 |
| 5 / syslog | 40 | 41 | 42 | 43 | 44 | 45 | 46 | 47 |
| 6 / lpr | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 |
| 7 / news | 56 | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| 8 / uucp | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 |
| 9 / clock | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 |
| 10 / authpriv | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 |
| 11 / ftp | 88 | 89 | 90 | 91 | 92 | 93 | 94 | 95 |
| 12 / ntp | 96 | 97 | 98 | 99 | 100 | 101 | 102 | 103 |
| 13 / audit | 104 | 105 | 106 | 107 | 108 | 109 | 110 | 111 |
| 14 / alert | 112 | 113 | 114 | 115 | 116 | 117 | 118 | 119 |
| 15 / solaris-cron | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| 16 / local0 | 128 | 129 | 130 | 131 | 132 | 133 | **134** (default) | 135 |
| 17 / local1 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| 18 / local2 | 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 |
| 19 / local3 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| 20 / local4 | 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 |
| 21 / local5 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| 22 / local6 | 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 |
| 23 / local7 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |

**src=IP\_ADDR**

Replaces the source IP address with an arbitrary IP instead of the Logpresso IP address

To replace the source IP address and transmit it, the 'libpcap' library must be installed on your operating system. You may also need to recompile the 'araqne-pcap' library for your operating system. Use PCAP to create and transmit readdressed packets only when specifying the source IP address other than Logpresso IP address. Note that if the packet size exceeds the MTU, the transmission fails.