

EZ5

Syslog Watcher

Version 7.0, 2026-10-16



Table of Contents

Introduction	1
Quick Start	2
What's New in Version 7	4
Syslog Watcher Manager	9
Manager Settings	11
Syslog Collector	13
Network Interfaces	14
Advanced Options	17
Syslog over TLS	19
Message Processing	22
Incoming Filter	26
Collector Service	29
Monitoring	30
Diagnostic Records	32
Performance	33
Troubleshooting	35
Syslog Storage	38
Storage Location and Limits	39
Storage Overview	40
Storage Maintenance and Archive	42
Open a Storage Folder Without a Server	44
Test Storage Speed	45
Syslog Originators	48
Managing Originators	51
Originator Groups	54
Syslog Messages	57
Formatting	58
Message Fields	59
Field Modifiers	62
Date/Time Modifiers	65
Escape Modifiers	67
Field Dictionaries	70
Filtering	72
Filter Expressions	73
Filter Lists	76
Field Extraction	77
Field Collections	80
Severity and Facility Names	83

Syslog Parsers	85
Create or Edit a Parser	86
Report Incorrect Parsing	88
Viewing Messages	89
View/Search Messages	90
View Layouts	95
View/Search Presets	100
Syslog Server	104
Remote Access	105
Email Accounts	109
HTTP Endpoints	110
Secret Strings	112
TLS Certificates	114
Server Diagnostics	116
Features	119
Managing Features	120
Monitoring Features	123
Export to Files	124
Export to DB (ODBC)	129
Forward to Syslog Server	131
Send Emails	134
Send HTTP Requests	137
Execute Program/Script	140
Syslog Reports	143
Generate a Report Now	144
Scheduled Reports	145
Report Templates	149
Template Examples	152
Simple Counters	152
Advanced Counter	153
Licenses, Updates, Support	156
License Management	156
Evaluation License	159
Product Updates	161
Migrate from Version 6	161
Technical Support	164

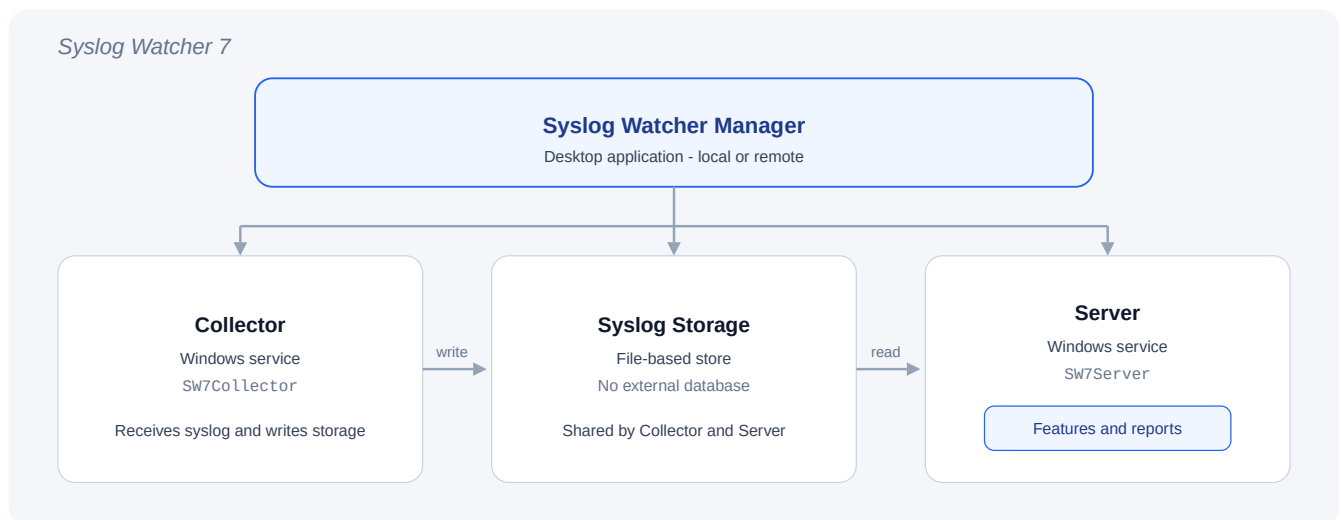
Introduction

Syslog Watcher is a syslog server for Windows. It receives syslog messages from network devices, servers, and workstations, stores them, and lets you search, process, and report on them. Messages are stored in files; no external database is needed.

To install and start collecting, follow [Quick Start](#). Upgrading from Syslog Watcher 6? See [What's New in Syslog Watcher 7](#) and [Migrate from Version 6](#).

How It Is Organized

Syslog Watcher 7 has four parts: Manager, Collector, syslog storage, and Server. The Collector writes messages to storage, and the Server reads them.



How Syslog Watcher 7 is organized

Syslog Watcher Manager

Manager is the desktop application. It connects to a local or remote server, shows status, changes the configuration, and displays stored messages. See [Syslog Watcher Manager](#).

Syslog Watcher Collector

The Collector receives syslog over the network and writes messages to syslog storage. See [Syslog Collector](#).

Syslog Storage

Syslog storage keeps all collected messages in files on disk. See [Syslog Storage](#).

Syslog Watcher Server

The Server runs features, reports, storage maintenance, and remote Manager access. See [Syslog Server](#).

Features run inside the Server. Each feature reads stored messages and sends them to files, a database, another syslog server, email, a web service, or a program. See [Features](#).

System Requirements

- Windows 8.1 or later (64-bit), or Windows Server 2012 R2 or later
- A local disk for syslog storage — an SSD for high message rates (see [Test Storage Speed](#))
- Network access from syslog originators to this computer
- Administrator privileges for installation

Where to Go Next

Receive messages	Network Interfaces (UDP, TCP, TLS), Incoming Filter , Syslog Collector
Manage originators	Syslog Originators — register, group, and select originators
Store and archive	Syslog Storage — location, retention, archive, and the Storage tab
View and search	Viewing Messages — view tabs, layouts, and presets
Fields and filters	Syslog Messages — message fields, format strings, and filter expressions
Parse messages	Syslog Parsers — built-in and custom parsers for each originator
Process messages	Features — export to files or ODBC, forward, email, HTTP, and programs
Report	Syslog Reports — generate or schedule reports
Administer	Syslog Server , Remote Access , Licenses , Updates , Support

Quick Start

Step 1: Install

1. Download the latest release from ezfive.com/syslog-watcher/downloads/.
2. Run the Syslog Watcher 7 installer and accept the [license agreement](#).
3. On the **Choose Components** page, select the components and the installation folder:
 - **Syslog Watcher Server** — the Collector and Server Windows services.
 - **Syslog Watcher Manager** — the desktop application.
4. Finish the installation.



To manage a [remote server](#) from a workstation, install only **Syslog Watcher Manager**.

▼ *After installation, depending on the selected components*

- Program files are in **C:\Program Files\Syslog Watcher 7** (or the folder chosen at install).
- **Syslog Watcher 7 Server (SW7Server)** and **Syslog Watcher 7 Collector (SW7Collector)** are registered as Windows services that start automatically with Windows.
- Windows Firewall gets inbound allow rules for both services, so originators and remote Managers can connect. Another firewall on this computer or in the network needs its own rules.
- Work files are in **C:\ProgramData\SyslogWatcher7**.
- Syslog storage is in **C:\ProgramData\SyslogStorage7**.
- Manager keeps its preferences and current state for each Windows user in **C:\Users\<user>\AppData\Roaming\SyslogWatcher7**.

Step 2: Open Manager

Start **Syslog Watcher 7 Manager** from the Start menu or the desktop shortcut. Manager connects to the local Syslog Watcher server.

Step 3: Migrate from Version 6 (if present)

If Syslog Watcher 6 data is on this computer, the **Migrate from Syslog Watcher 6** window opens. Follow [Migrate from Version 6](#): test, migrate, and turn storage retention back on.

Step 4: Check Network Interfaces

A new installation listens for UDP on all IPv4 addresses (**0.0.0.0**), port 514. Most network devices send syslog to this port by default.

To add TCP, TLS, or more UDP listeners, see [Network Interfaces](#).

Step 5: Start the Collector

The installer does not start the collector, so you can review its settings first. Start it in one of these ways:

- ▶ In the **Server** section of the main toolbar, click *** Collector** → **Start Syslog Collector**.
- ▶ On the [Server tab](#), click **Start Collector** under **Syslog Collector** in the diagram.

Step 6: Point Devices at This Computer

Configure each network device, server, workstation, or software source to send syslog to this computer's IP address and the port from Step 4.

Each new sender is added as an [originator](#) when its first message arrives.

Step 7: Check That Messages Arrive

1. In Manager, select the [Storage tab](#).
2. Click  **Refresh**; today's counts grow as messages arrive.
3. Click a count to see those messages in a [view tab](#).

If no messages arrive, see [Collector Troubleshooting](#).

Work Without Internet Access

Syslog Watcher does not need Internet access to collect, store, and view syslog messages, so it can run in a closed network. For the tasks that involve EZ5, use another computer or a phone with Internet access:

- **License:** install a license or request an evaluation license with a request link or a QR code. See [Offline Installation](#).
- **User Guide:** install the [offline User Guide](#), so that [Help](#) opens pages from disk.
- **Updates:** download the new installer on another computer, copy it over, and [run it](#).
- **Support:** save the [support data file](#) and attach it to a ticket from another computer.

Related Topics

- [Syslog Collector](#) — pipeline, service, and monitoring
- [License Management](#) — install, select, or evaluate a license

What's New in Version 7

This page lists the main changes in Syslog Watcher 7 since version 6.5.

Architecture

Dedicated Collector Service

The syslog collector is now a separate Windows service, independent of Syslog Watcher Server and Manager. Incoming messages are written to storage even while the Server is stopped — for example during an upgrade.

See [Syslog Collector](#).

Upgraded Storage Structure

The new storage layout handles higher message rates than version 6.5 and handles time zones better.

See [Syslog Storage](#).

Remote Access

Manager can connect over the network to a Syslog Watcher Server to configure it, view stored messages, and work with reports. The connection can be encrypted. Role-based accounts can be limited to read-only access, with no permission to change the configuration.

See [Remote Access](#).

Working with Messages

Storage Tab with Calendar

The Storage tab shows how many messages arrived each hour and day, by originator and severity. Use it to find when and where a problem started.

See [Storage Overview](#).

View Tabs

View tabs keep their request and layout when Manager restarts.

See [View/Search Messages](#).

Filter Row

The message grid has a filter row: each column can be filtered on its own.

View Presets

View/Search presets save frequently used searches and open them in one click.

See [View/Search Presets](#).

Syslog Parsers

Parsers are redesigned: they have more section types, and the editor has live testing. Built-in parsers cover Cisco, Fortinet, Juniper, NETGEAR, Palo Alto, SonicWall, Sophos, and Ubiquiti.

See [Syslog Parsers](#).

Field Collections

Many vendors do not put field names in the syslog text; the payload is only a list of values. A field collection names those values by message type, so they can be used in filters, exports, and views.

See [Field Collections](#).

Field Modifiers and Escape Modifiers

New [field modifiers](#) extract and transform message data, and new [escape modifiers](#) prepare values for CSV, JSON, SQL, HTML, URLs, command lines, and file names. Escaping keeps special characters in syslog text from breaking those outputs.

Customizable Severity and Facility Names

You can rename severities and facilities; the syslog numbers stay the same.

See [Severity and Facility Names](#).

Faster Regular Expression Engine

A new regular expression engine makes filters, field extraction, and parsers faster. Existing expressions do not have to be rewritten.

Collection

Incoming Filter

The incoming filter still discards traffic before storage by severity and keywords. It now also accepts a regular expression on the raw line, as an allow-list or a deny-list.

See [Incoming Filter](#).

TLS Certificates

The Server has a certificate store that generates, imports, and exports certificates. TLS settings select a certificate by name instead of a file path.

See [TLS Certificates](#).

Client Certificate Names and Fingerprints

The collector records the certificate fingerprints and names of new TLS clients. Allow a client by checking its entry in the list, instead of copying values by hand.

See [Client Certificate Validation](#).

Built-in Storage Speed Test

A built-in test measures how fast a disk can write syslog storage. Use it to estimate hardware requirements.

See [Test Storage Speed](#).

Processing

Feature Suspend and Resume

Each feature can be suspended and resumed. On resume, a feature continues from where it stopped (including the backlog), skips to new messages, or starts from a chosen date and time. New features start suspended, so nothing is exported until you click **Resume**.

See [Managing Features](#).

Execute Program/Script

A new feature type starts a program or script for each matching message, with message fields on the command line.

See [Execute Program/Script](#).

Send HTTP Requests

A new feature type sends an HTTP request (POST or PUT) for each matching message. Named HTTP endpoints hold the host, TLS, headers, and authentication; the feature supplies the path and the body, including JSON.

See [Send HTTP Requests](#).

Scheduled Syslog Reports

Reports can run on a schedule: once, recurring, weekly, or monthly. The Server generates them without Manager running; open the results in Manager later.

See [Syslog Reports](#).

Administration

Secret Strings

Passwords and other private values are stored as encrypted secret strings and referred to as **%Name%** in the configuration.

See [Secret Strings](#).

Storage Archive

The storage archive keeps a compressed, optionally encrypted copy of the storage, daily or hourly, in a local or network folder. A command can run after each sync — for example to copy the archive to cloud storage.

See [Storage Maintenance and Archive](#).

Email Notification of Problems

The Server can email new warnings and errors from its own and the collector's diagnostic records, so you can fix problems before they stop collection or leave gaps in the log.

See [Server Diagnostics](#).

Migration from Version 6

Syslog Watcher 7 migrates a version 6 installation on the same computer: license, configuration, forwarders (as features), knowledge-base files, filter lists, view layouts, and report templates. It keeps using the version 6 syslog storage, so existing messages are not copied.

See [Migrate from Version 6](#).

Syslog Watcher Manager

Syslog Watcher Manager is the Syslog Watcher desktop application. Use it to view messages, check status, and change settings. It connects to one Syslog Watcher Server at a time, on this computer (local) or on another computer (remote). The Collector and the Server are Windows services and keep running after you close Manager.

Connect to the Local Server

By default, Manager connects to the local server when it starts (**Auto-connect to local server** in [Manager Settings](#)). Otherwise, in the **Server** section of the main toolbar, click  **Local**. The button appears only when the Server is installed on this computer.

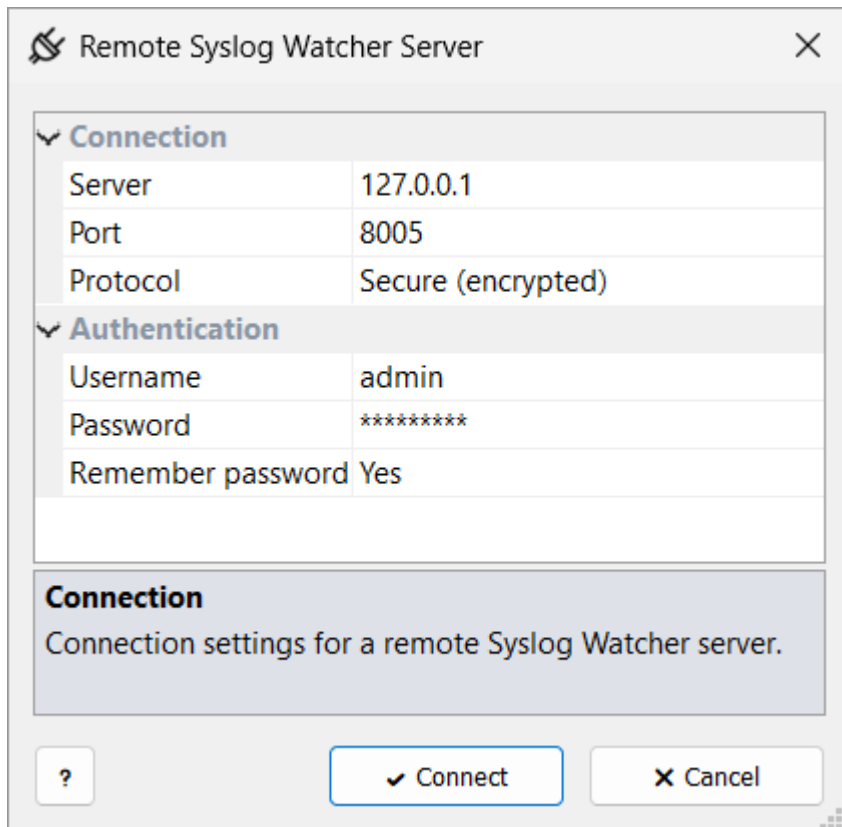


[Roles](#) do not apply to Manager on the server computer. What it can do depends on the Windows account that runs it.

Connect to a Remote Server

The remote server must have [remote access](#) enabled and a user account for you.

1. If Manager is connected to a server, [disconnect](#) first.
2. In the **Server** section of the main toolbar, click  **Remote**.
3. In the **Remote Syslog Watcher Server** window, fill in the connection settings.
4. Click **Connect**.



Connection	
Server	127.0.0.1
Port	8005
Protocol	Secure (encrypted)

Authentication	
Username	admin
Password	*****
Remember password	Yes

Connection
Connection settings for a remote Syslog Watcher server.

?

Server	IP address or host name of the Syslog Watcher Server computer.
Port	The Port set on the server.
Protocol	The same as Connection on the server.
Username	A remote access user on the server.
Password	That user's password.
Remember password	Yes saves the password for the next connection. It is stored encrypted for your Windows account.

Work in a Remote Session

In a remote session, you work with the server's syslog storage, features, originators, and configuration, within the limits of your [role](#).

Some actions run on the server computer, not on the Manager computer, for example, test emails, test HTTP requests, and storage maintenance. [Generate Report Now...](#) is not available remotely. [Schedule](#) the report instead.

Disconnect

In the **Server** section of the main toolbar, click  **Server** → **Disconnect** and confirm. The **Local** and **Remote** buttons appear again.

Use Manager as a Storage Reader

Manager can also work with no server at all, as a reader for syslog storage. It opens a storage folder directly, for example an extracted [storage archive](#), a storage copied from another computer, or a Syslog Watcher 6 storage. You can view and search messages and generate reports.

See [Open a Storage Folder Without a Server](#).

General Section

 Manager	Open the Manager settings .
 Updates	Check for newer product versions. See Product Updates .
 Support	Open Product Support .

Help

Click ? in a tab or window to open the User Guide page about it. Press  in the main window to open the User Guide start page.

If the [offline User Guide](#) is installed, Help opens its pages from disk, with no Internet access needed. Otherwise, Help opens the online guide.

Related Topics

- [Remote Access](#)

Manager Settings

To open Manager settings, in the **General** section of the main toolbar, click  **Manager**.

Settings

Behavior

Auto-connect to local server	When Manager starts, connect to the Syslog Watcher Server installed on this computer. Windows may ask for administrator rights.
Check for updates	When Manager starts, check for a newer product version. If there is one, Manager tells you. Open Updates for details.
Warn if versions differ	After connecting to a local or remote server, warn if the server version differs from the Manager version.
Confirm closing a view tab	Ask for confirmation when you click a view tab's close button.
Confirm closing Manager	Ask for confirmation when you close Manager while it is connected to a server.

Storage Tab

Maximum selected days	The most days you can select at once on the Storage tab calendar (1–999).
------------------------------	---

Appearance

Server tab scale	Size of the Server tab , as a percentage of the Windows display scale (50–200). You can also change it with  + mouse wheel on the Server tab.
UI language	Language of the Manager user interface. Only English is available in this version.
Long date format, Short date format, Long time format, Short time format	How Manager shows dates and times. System settings (an empty value) uses the Windows regional format. To use your own format, type a

[format string](#). Restart Manager to apply a change.

Date and Time Formats

Letters	Shows
yyyy / yy	Year: 2026 / 26
MMMM / MMM / MM	Month: October / Oct / 10
dddd / ddd / dd	Day: Saturday / Sat / 10
HH	Hour: 00–23
hh	Hour: 01–12
mm	Minute: 00–59
ss	Second: 00–59
tt	AM or PM

For example, `yyyy-MM-dd` shows 2026-10-10, and `HH:mm:ss` shows 14:05:09.

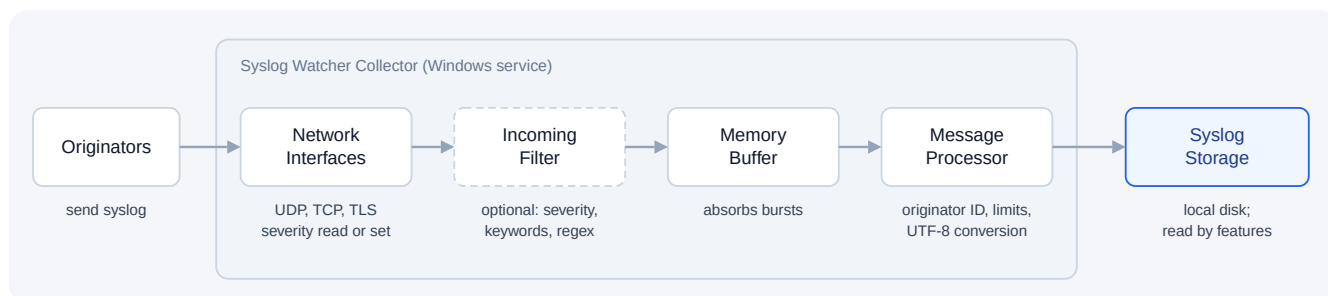
Syslog Collector

The collector receives syslog messages from the network and writes them to syslog storage. Without a running collector, no new messages are accepted.

The collector runs as a [Windows service](#), independent of Syslog Watcher Server and Manager. It keeps collecting while the Server is stopped — for example during Server updates and security patches.

How It Works

Each message passes through these stages before it is written to syslog storage:



Syslog message collection pipeline

Network Interfaces	UDP, TCP, and TLS listeners receive messages from originators. The collector reads the severity of each message, or assigns the default severity when the message has none. See Network Interfaces .
Incoming Filter	Optional (off by default). Discards unwanted messages by severity, keywords, or a regular expression, before they take space in the buffer. See Incoming Filter .
Memory Buffer	Holds messages until they are written, so bursts are not lost while storage catches up. See Memory Buffer .
Message Processor	Assigns the originator ID , checks the originator and license limits, and converts the message text to UTF-8. See Message Processing .
Syslog Storage	Processed messages are written to the file-based syslog storage . Features (export, forward, email, HTTP, scripts) read from this storage later; they are not part of the collector.

The Server tab shows how many messages were discarded and why; see [Discarded Messages](#).

Collector Topics

- [Network Interfaces](#) — configure UDP, TCP, and TLS listeners
 - [Advanced Options](#) — message length, buffers, framing, timeouts
 - [Syslog over TLS](#) — server certificates and client authentication

- [Message Processing](#) — preprocessor, originator ID rules, and memory buffer
- [Incoming Filter](#) — discard unwanted messages before storage
- [Collector Service](#) — start and stop the collector, startup type, recovery
- [Monitoring](#) — collector status, interfaces, and discarded messages on the Server tab
- [Diagnostic Records](#) — the collector's own log for startup, license, and interface errors
- [Performance](#) — storage speed, buffer sizing, and high-volume tips
- [Troubleshooting](#) — common collector problems by symptom

Network Interfaces

A **network interface** is a listener on a local IP address that accepts syslog messages. Each interface uses one transport: UDP, TCP, or TLS. Several interfaces can run at once, for example UDP for older originators and TLS for originators that must encrypt their logs.

The collector needs at least one interface; without one it receives nothing. A new installation has one UDP interface on all IPv4 addresses (**0.0.0.0**), port 514.

Managing Network Interfaces

Network interfaces are configured in **Syslog Collector Configuration**:

1. In the **Server** section of the main toolbar, click **✳ Collector** → **Syslog Collector Configuration...** The **Collector** button is shown when Manager is connected to a local or remote server.
2. Open the **Network Interfaces** tab.
3. Add, change, or delete interfaces. To remove an interface, click **Delete Interface** in its header.
4. Click **Apply**.

Network Interfaces

Message Processing

Syslog Storage

> Interface: UDP/0.0.0.0/514
 [Delete Interface](#)

> Interface: TCP/0.0.0.0/514
 [Delete Interface](#)

> Interface: TLS/0.0.0.0/6514
 [Delete Interface](#)

Local IP address	All local IPv4 addresses (0.0.0.0)
Syslog port	6514
> Maximum concurrent connections	1000
> TLS Options	
Minimum protocol version	TLS 1.2
Certificate	Certificate1
Private key password	%TLCERT%
> Client certificates	Require, validate
> Allow self-signed certificates	Yes
Certificate Authority (CA)	
> Advanced	

[Add UDP Interface](#), [Add TCP Interface](#), [Add TLS Interface](#)

Interface: TLS/0.0.0.0/6514
 The network interface receives syslog messages from the network using the selected protocol.

?
 Import / Export

✓ Apply

✕ Cancel

If you are not allowed to change the configuration, the window title ends with **(Read Only)** and **Apply** is disabled. This happens when:

- ▶ Local server: Manager is not running as Administrator, so it cannot save the configuration file.
- ▶ Remote server: your account's role does not allow changing the collector configuration. By default, only the **Admin** role does.

Leave the [advanced settings](#) unchanged unless a specific problem requires a change.

UDP Interface

UDP is the usual syslog transport. It is connectionless: originators send datagrams with no session. Port **514** is the IANA default (RFC 5426).

UDP is simple and widely supported, but delivery is not guaranteed and the payload is not encrypted. Use it when compatibility matters more than reliable, encrypted delivery.

Adding a UDP Interface

1. Click **Add UDP Interface**.
2. In **Local IP address**, select **All local IPv4 addresses (0.0.0.0)** or **All local IPv6 addresses (::0)**, or enter one address of this computer.
3. In **Syslog port**, keep **514** or set the port the originators send to.
4. Click **Apply**.

▼ Interface: UDP/192.168.30.1/514 Delete Interface	
Local IP address	192.168.30.1
Syslog port	514
▼ Advanced	
Maximum message length	10000
Socket buffer size (bytes)	2000000

TCP Interface

TCP adds a persistent connection, ordered delivery, and flow control. Port **514** is the IANA default (RFC 6587) — the same number as UDP, but a different protocol.

The originator must support syslog over TCP. TCP does not encrypt the data. Use it when message loss on the network path is not acceptable.

Adding a TCP Interface

1. Click **Add TCP Interface**.
2. Set **Local IP address** and **Syslog port** as for a [UDP interface](#).
3. If needed, adjust **Maximum concurrent connections** (see [TCP and TLS Connections](#)).
4. Click **Apply**.

▼ Interface: TCP/0.0.0.0/514 Delete Interface	
Local IP address	All local IPv4 addresses (0.0.0.0)
Syslog port	514
> Maximum concurrent connections	100
▼ Advanced	
Maximum message length	10000
Socket buffer size (bytes)	2000000
Octet-counting detection	Yes
Split stream using CR/LF	Yes
Inactive client timeout	Disabled

TLS Interface

TLS encrypts syslog over TCP. Port **6514** is the IANA default (RFC 5425).

The collector presents a server certificate; originators can be required to present client certificates. Use TLS when logs must not cross the network in clear text.

Adding a TLS Interface

1. Click **Add TLS Interface**.
2. Set address, port, and connections as for a [TCP interface](#). The initial port is **6514**.
3. Under **TLS Options**, select a **Certificate**, as described in [Syslog over TLS](#).
4. Click **Apply**.

If no certificate is selected, **Apply** offers to generate a self-signed one.

TCP and TLS Connections

TCP and TLS interfaces limit how many originators can be connected at the same time.

Maximum concurrent connections	Maximum number of syslog clients connected at the same time (1–59999). The operating system can set a lower limit.
Replace older connections	When the limit is reached, Yes disconnects the oldest client so the new one can connect. No refuses the new client.

Choosing Port Numbers

The usual ports are **514** for UDP and TCP, and **6514** for TLS. The collector must listen on the same port and transport the originators send to. Firewalls on the path must allow that port and protocol.

A UDP interface can share an address and port with a TCP or TLS interface, because they are different transports. Example: UDP **514** and TCP **514** together.



TCP and TLS interfaces cannot share an address and port, because TLS runs over TCP. Two interfaces of the same transport cannot share them either.

Related Topics

- [Advanced Interface Options](#)
- [Syslog over TLS](#)
- [Monitoring](#) — interface status and counters
- [Troubleshooting](#) — no messages arrive

Advanced Options

Each network interface (UDP, TCP, or TLS) has an **Advanced** section with low-level transport settings. The initial values suit most cases; change them only to solve a specific problem.

Open the interface in [Syslog Collector Configuration](#), then expand **Advanced**.

Any Interface

Field	Initial	Description
Maximum message length	10000	Maximum length of one syslog message, in bytes (3–65515). UDP: a longer datagram is dropped. TCP and TLS: a longer message is truncated, and the client is disconnected to resynchronize the stream; a warning is written to Diagnostic Records .
Socket buffer size (bytes)	2000000	Size of the operating system receive buffer for this listener, used to absorb data bursts (0–268435455). 0 uses the system default.

When to Adjust

If messages are cut off or missing, or TCP/TLS clients are disconnected with a truncation warning, increase **Maximum message length**. Originators that send large structured data or verbose application payloads can exceed the initial limit.

Change **Socket buffer size** only when the server receives more than about 10,000 messages per second over UDP and messages are lost during bursts. Contact technical support before changing it: the right size depends on Windows limits, available memory, and the message rate.

Streaming (TCP/TLS) Interface

These settings apply only to TCP and TLS. UDP has no byte stream and no client sessions.

Field	Initial	Description
Octet-counting detection	Yes	Detect RFC 6587 octet-counting framing (each message prefixed with its length). With Yes , both octet-counted and delimiter-separated streams are accepted. Turn it off only for compatibility with legacy equipment.
Split stream using CR/LF	Yes	Yes splits the stream into messages on CR, LF, and \0 . No splits on \0 only — for originators that send multi-line messages terminated by \0 .
Inactive client timeout	Disabled	Disconnect clients that send nothing for this many seconds. 0 (shown as Disabled) keeps idle clients connected.

When to Adjust

Keep **Octet-counting detection** and **Split stream using CR/LF** on unless messages arrive merged together or split in the wrong places.

Inactive client timeout helps when many originators connect and disconnect over time, so that idle sessions do not fill up [Maximum concurrent connections](#). For a fixed set of originators, leave it disabled.

Related Topics

- [Network Interfaces](#)
- [Performance](#)
- [Monitoring](#) — connected clients per interface

Syslog over TLS

Syslog over TLS (RFC 5425) sends syslog over an encrypted TCP connection, usually to port **6514**. The collector presents a server certificate and can require client certificates.

In Syslog Watcher this is a [TLS network interface](#). You do not point the interface to certificate files. Instead, you add the certificate once to the Syslog Watcher Server's certificate store, and then select it by name in the interface settings. To manage the store, use [TLS Certificates](#) (**More** → **TLS Certificates...** in the **Server** section of the main toolbar).

TLS Options

The **TLS Options** section of a TLS interface has these settings:

Setting	Description
Minimum protocol version	Lowest TLS version the collector accepts: TLS 1.0 , TLS 1.1 , TLS 1.2 , or TLS 1.3 . The initial value is TLS 1.2 . Lower it only when an older originator cannot connect otherwise.
Certificate	Server certificate and private key, chosen by name from TLS Certificates . The button next to the list opens TLS Certificates , where you can generate or import a certificate.
Private key password	Password for an encrypted private key. Use a secret string (% SECRET %) instead of the actual password. When you select a Certificate , Manager fills in the secret string stored for it, if there is one; otherwise it clears the field. Leave it empty for an unencrypted key.
Client certificates	Do not request (initial value), Request , validate if received , or Require, validate . See Client Certificate Validation .

If **Certificate** is empty when the configuration is applied, Manager offers to generate a self-signed certificate and selects it. A TLS interface does not work without a certificate.

Server Certificate

Originators check the collector's certificate when they connect. The name they use to reach the collector (host name or IP address) must appear in the certificate, and the certificate must be trusted by the originator.

There are two ways to get a certificate into the store:

- **Generate Self-signed Certificate** — quick to set up; every originator must be configured to trust that certificate (or to skip verification). Add the collector host name and, if originators

connect by IP, its IP address as **Subject Alternative Names (SAN)**.

► **Import** — a certificate issued by the organization's CA (or a public CA), with its private key, in PEM format. Include the chain in the certificate file: server certificate first, then intermediate CAs.

Both are described in [TLS Certificates](#).



A certificate can also be created outside Syslog Watcher, for example with OpenSSL, and then imported:

```
openssl req -x509 -newkey rsa:2048 -sha256 -days 365 -nodes -keyout
server.key -out server.crt -subj "/CN=syslog-collector.example.com"
-addext "subjectAltName=DNS:syslog-collector.example.com,IP:192.0.2.10"
```

Replace the DNS name and IP with the values originators use, then import `server.crt` and `server.key` with **Import** → **From PEM File....**

Client Certificate Validation

By default, only the originator checks the other side: it verifies the collector's server certificate. The connection is encrypted, but the collector does not check who connects.

With client certificate validation (mutual TLS), the collector accepts connections only from authorized originators.

Client Certificates Mode

Mode	Behavior
Do not request	No client certificate is requested. Any client that trusts the server certificate can connect.
Request, validate if received	 Rarely needed. Example: during a gradual rollout of client certificates, originators that already have one are validated, while the others keep sending until they get theirs. Then switch to Require, validate. A client certificate is requested. If the client sends one, it must pass validation. A client that sends none is still accepted.
Require, validate	A client certificate is required and must pass validation. Clients without one are refused.

When the mode is not **Do not request**, two validation methods appear. A client is accepted if it passes either method.

Setting	Description
Allow self-signed certificates	Yes accepts a client certificate whose fingerprint is allowed in Certificate fingerprints . The certificate does not need to be issued by a CA.

Setting	Description
Certificate Authority (CA)	CA certificate, by name, from TLS Certificates . Client certificates must be issued by this CA. Blank turns CA validation off.



If neither method is on, every client certificate is refused.

Certificate Fingerprints

Use fingerprints for a small set of originators, or for originators with self-signed certificates and no shared CA.

1. Set **Allow self-signed certificates** to **Yes**.
2. Let the originator try to connect once. The collector refuses it and records the certificate fingerprint. When **Certificate Authority (CA)** is blank, it also writes a warning to [Diagnostic Records](#).
3. Double-click **Certificate fingerprints**, or click its ... button. The value shows how many fingerprints are allowed.
4. In the **Certificate fingerprints** window, check the row for that originator and click **Apply**.

Each row shows **From IP**, **Algorithm**, and **Fingerprint**; the window title shows the allowed and total counts. A checked row is allowed; an unchecked row is known but refused. An allowed fingerprint is valid only for the IP address it came from.

The list is saved when you click **Apply** in that window, separately from the interface settings; the collector picks up the change without a restart.



With no allowed fingerprints, every self-signed client is refused.

CA Validation, IP, and Names

Use a CA when originators share an internal PKI.

When **Certificate Authority (CA)** is set, the client certificate chain must lead to that CA. Two more settings can then tie the certificate to the connecting client:

Setting	Description
Allow clients by IP	Yes accepts the client when its certificate has the client's source IP address in a SAN IP entry.
Allow clients by name	Allow any name (no check) (initial value) accepts every certificate from the CA. N allowed accepts only certificate names (CN or DNS SAN) that are allowed in the Client names list.



With both left off (**No** and **Allow any name**), any certificate from the CA is accepted.

With either on, the client must match at least one of them; otherwise it is refused and a name check

warning is written to Diagnostic Records.

Troubleshooting

Symptom	What to check
TLS handshake failed	The originator does not trust the server certificate, or the name it connects with is not in the certificate. Add the right SAN entries, or import a CA-issued certificate. With client certificates on: the client certificate is not from the configured CA, or no validation method is on.
TLS handshake failed with a protocol version error	The originator's TLS version is below Minimum protocol version . Update the originator if possible; lower the minimum only if needed.
The received client certificate is unknown	Self-signed client not allowed yet. Allow it in Certificate fingerprints .
Client certificate name check failed	CA-issued client certificate does not match Allow clients by IP or Allow clients by name . Allow the name in Client names , or add the client IP to its certificate SAN.

See also [Troubleshooting](#).

Related Topics

- [Network Interfaces](#)
- [TLS Certificates](#)
- [Secret Strings](#)
- [Diagnostic Records](#)

Message Processing

The **Message Processing** tab of **Syslog Collector Configuration** sets how the collector assigns a severity, converts the encoding, filters messages, and assigns each message to an originator.

To open it, click **✱ Collector** → **Syslog Collector Configuration...** in the **Server** section of the main toolbar, then **Message Processing**.

Network Interfaces

→

Message Processing

→

Syslog Storage

Preprocessor

If a message has no severity, assign	(7) Debug
Message body encoding	UTF-8

Filter

Originator IDs

Default originator ID rule	ID = IP address of the message sender
Resolve name (reverse DNS lookup)	Yes
If originator ID is unknown	Add new originator

Originator ID Rules (2)

IP Range Rule

IP range start	10.20.0.15
IP range end	
Originator ID	Extract as RFC5424:HOSTNAME
If unable to extract ID	Apply the default rule
If originator ID is unknown	Add new originator

Filter

The preliminary filter discards unnecessary syslog messages at an early stage, before they are written to syslog storage.

?

Import / Export ▼

✓ Apply

✗ Cancel

Syslog Collector Configuration: Message Processing

Preprocessor

The preprocessor settings apply at two points of the [pipeline](#):

- The severity is assigned as soon as a message is received, before the [Incoming Filter](#).
- The encoding is converted after the memory buffer, just before the message is written to storage.

If a message has no severity, assign

Every message in syslog storage has a severity. The severity is carried in the **<PRI>** part at the start of the message. Some originators omit it, although the syslog standards require it. Such messages get the severity selected here, and facility 16 (local0).

Message body encoding

Syslog Watcher stores all messages in UTF-8. Most current devices and software send UTF-8, so the default **UTF-8** needs no conversion.

If originators send another encoding, enter its name, for example **windows-1252**, **Latin1**, **Shift-JIS**, or **ISO-8859-8**. The collector converts each message from that encoding to UTF-8.

- Messages that contain only ASCII characters are not converted.
- Messages that contain a UTF-8 byte order mark are treated as UTF-8 regardless of this setting; the mark is removed.
- If the conversion fails (for example, the encoding name is not recognized), the message is stored unconverted. An error is written to **Diagnostic Records** once per encoding name until the collector restarts.



The encoding applies to all originators; it cannot be set per originator. For mixed encodings, configure the originators to send UTF-8.

Originator IDs

The collector assigns an originator ID to every message and uses it to find the originator in syslog storage. To learn how IDs work and when to change the default rule, with examples, see [Originator ID](#).

Originator IDs	
Default originator ID rule	ID = IP address of the message sender
Resolve name (reverse DNS lookup)	Yes
If originator ID is unknown	Add new originator

Originator IDs settings

Default originator ID rule	ID = IP address of the message sender. Applies when no originator ID rule matches the sender.
Resolve name (reverse DNS lookup)	With Yes , a new originator is named after the sender's host name when its ID is the sender's IP address. With No , the name is the same as the ID. See How Originators Are Registered .
If originator ID is unknown	Add new originator registers the originator and stores the message, within the license limit. Discard messages drops the message; it is counted as Unknown originator in Monitoring .

Originator ID Rules

A rule takes the ID from the message itself for senders in an IP range, for example a syslog relay. To learn when to use rules and which rule applies when several match, see [Originator ID Rules](#).

1. Click **Add Rule** next to **Originator ID Rules (N)**.
2. Set **IP range start** and, for a range, **IP range end**.
3. Select how to get the **Originator ID** (see below).
4. Click **Apply**.

To remove a rule, click **Delete** in its header.

▼ Originator ID Rules (2) Add Rule	
▼ IP Range Rule Delete	
IP range start	10.20.0.15
IP range end	
Originator ID	Extract as RFC5424:HOSTNAME
If unable to extract ID	Apply the default rule
If originator ID is unknown	Add new originator

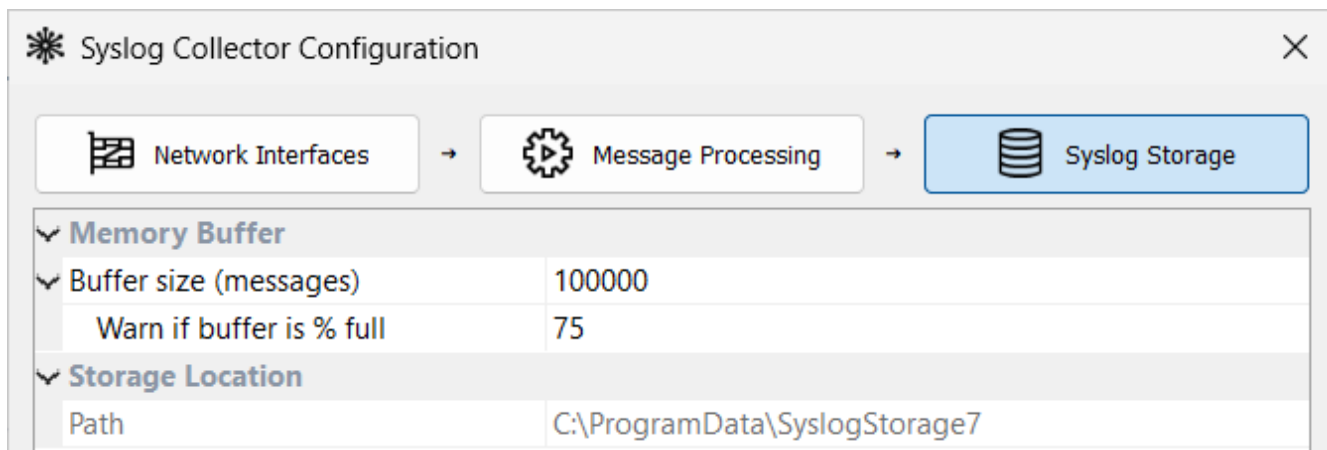
Originator ID rule

IP range start	First IP address of the range, for example 192.168.0.1 or ::1 . Required.
IP range end	Last IP address of the range (inclusive). Leave it blank for a single address.
Originator ID	Extract as RFC5424:HOSTNAME , Extract as RFC5424:HOSTNAME/APPNAME , or Extract with regular expression (enter it in Regular expression). The RFC 5424 options work only for messages in RFC 5424 format; for other formats, use a regular expression. IDs longer than 255 characters are truncated.
If unable to extract ID	Apply the default rule uses the sender IP address. Discard messages drops the message; it is counted as No originator ID in Monitoring .
If originator ID is unknown	Add new originator or Discard messages , for this range only.

Memory Buffer

The memory buffer sits between the network interfaces and the storage writer. It holds messages so that short bursts are not lost when storage cannot keep up.

The buffer is set on the **Syslog Storage** tab of **Syslog Collector Configuration**.



The image shows the 'Syslog Collector Configuration' window. It has three tabs: 'Network Interfaces', 'Message Processing', and 'Syslog Storage'. The 'Syslog Storage' tab is selected. Under this tab, there are two sections: 'Memory Buffer' and 'Storage Location'. The 'Memory Buffer' section has two rows: 'Buffer size (messages)' with a value of '100000' and 'Warn if buffer is % full' with a value of '75'. The 'Storage Location' section has one row: 'Path' with a value of 'C:\ProgramData\SyslogStorage7'.

Syslog Collector Configuration: Syslog Storage

Buffer size (messages)	Maximum number of messages held in memory before they are written (1,000–10,000,000). A larger buffer covers longer bursts and uses more RAM.
Warn if buffer is % full	At this fill level (10–99), a warning is written to Diagnostic Records and Buffer Usage on the Server tab turns red.

When the buffer is full, new messages are discarded and counted as **Buffer overflow** in [Monitoring](#).

Size the buffer for the longest burst it must absorb: at 5,000 messages per second, 100,000 messages cover about 20 seconds. A larger buffer helps only with bursts; if **Buffer Usage** stays high, storage is too slow for the sustained rate. For monitoring and other tuning, see [Performance](#).

The **Syslog Storage** tab also shows the storage folder (read-only); change it as described in [Storage Location](#).

Related Topics

- [Incoming Filter](#)
- [Syslog Originators](#) — registered originators, groups, and selection
- [Monitoring](#) — buffer usage and discarded messages on the Server tab
- [Performance](#)

Incoming Filter

The **Filter** section on the [Message Processing](#) tab discards unwanted messages as soon as they are received — before the memory buffer and before syslog storage.

While no criterion is set, the filter is off and the section header reads **Filter [OFF]**.

When It Runs

Most filtering in Syslog Watcher uses the [message filter](#) on stored messages (features, views, reports). The incoming filter runs **before** storage:

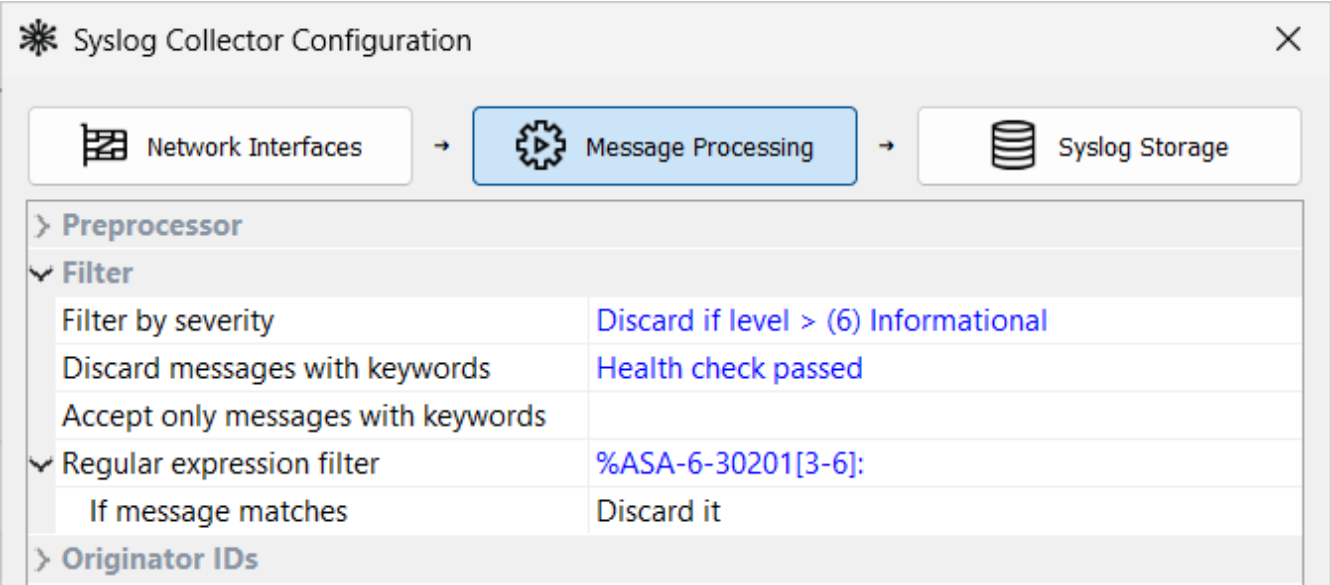
- Discarded messages take no storage space and no place in the memory buffer.
- Discarded messages get no further processing (originator handling, features).
- Only simple criteria are available: the message is not parsed at this stage.

Use it to drop high-volume, low-value traffic (for example debug-level noise) before it reaches storage. It is the cheapest way to reduce storage load; see [Performance](#).

Discarded messages are counted on the Server tab as **Filtered (severity)** or **Filtered (content)**; see [Monitoring](#).

Filter Settings

A message must pass every criterion that is set. The criteria are checked in this order: severity, **Accept only messages with keywords**, **Discard messages with keywords**, regular expression.



Syslog Collector Configuration: Filter

Filter by severity	Do not discard (accept all levels), or Discard if level > (N) <name>. For example, Discard if level > (4) Warning discards (5) Notice, (6) Informational, and (7) Debug messages from all originators.
Discard messages with keywords	Deny list: a message that contains any of the keywords is discarded.
Accept only messages with keywords	Allow list: a message that contains none of the keywords is discarded.
Regular expression filter	Pattern searched for anywhere in the message. Leave it blank to turn this criterion off.
If message matches	Accept it: only matching messages are kept; all others are discarded. Discard it: matching messages are discarded.



Enter one keyword per line; press **Ctrl** + **Enter** for a new line. An empty list turns that criterion off.

How Text Is Matched

Keywords and the regular expression are matched against the message as received:

- The **<PRI>** part is removed; the rest of the syslog header (timestamp, host name) is included.
- Matching is case-sensitive. In a regular expression, **(?i)** at the start makes it case-insensitive.
- Text is matched before the **encoding conversion**, in the encoding the originator sent, while keywords are saved in UTF-8.
- The regular expression uses Perl syntax.

Example: a Cisco ASA firewall logs every connection it opens and closes at **(6) Informational**, often thousands of messages per second:

```
Oct 12 2026 08:15:00: %ASA-6-302013: Built outbound TCP connection 4711 for
outside:203.0.113.10/443 (203.0.113.10/443) to inside:10.1.1.25/51544
(10.1.1.25/51544)
Oct 12 2026 08:15:04: %ASA-6-302014: Teardown TCP connection 4711 for
outside:203.0.113.10/443 to inside:10.1.1.25/51544 duration 0:00:04 bytes 5120 TCP
FINs
```

To drop these messages and keep all other **Informational** messages from the firewall, set **Regular expression filter** to **%ASA-6-30201[3-6]:** and **If message matches** to **Discard it**. The pattern matches message IDs 302013–302016: TCP and UDP connections built and torn down.



Discarded messages are lost. After changing keywords or the pattern, watch **Filtered (content)** on the Server tab.

Incoming Filter and Message Filter

	Incoming Filter	Message Filter
When it runs	When a message is received, before storage	After the message is in storage
Available criteria	Severity, keywords, regular expression on the raw message	All parsed fields (originator, facility, message body, timestamps, custom fields)
Effect	The message is never stored	Features, views, and reports include or exclude the message
Use for	High-volume noise reduction	Fine-grained routing, export, and reporting

Related Topics

- [Message Processing](#)
- [Filtering](#)
- [Performance](#)
- [Monitoring](#)

Collector Service

The collector runs as its own Windows service, **Syslog Watcher 7 Collector** (SW7Collector), separate from Manager and from **Syslog Watcher 7 Server** (SW7Server).

Starting and Stopping the Collector

Start or stop the collector in one of these ways:

- ▶ In the **Server** section of the main toolbar, click **✳ Collector** → **Start Syslog Collector** or **Stop Syslog Collector**.
- ▶ When the collector is stopped, click **Start Collector** on the [Server tab](#).
- ▶ In **Services** ([services.msc](#)), select **Syslog Watcher 7 Collector** and click **Start** or **Stop**.
- ▶ In a Command Prompt run as Administrator, run `net start SW7Collector` or `net stop SW7Collector`.

The **Start**, **Stop**, and **Startup Type** commands appear in the **Collector** drop-down only when you can control the collector:

- ▶ Local server: always. Manager runs as Administrator and asks for elevation when it starts.
- ▶ Remote server: only for the **Admin** role (see [Remote Access](#)).

Startup Type

The installer registers the collector with startup type **Automatic**, but does not start it. Start it once after the initial configuration; after that it starts with Windows.

To change the startup type, click **✳ Collector** → **Startup Type: <current>** → **Switch to Manual** or **Switch to Automatic**.

Startup type	Behavior
Automatic	Starts with Windows. Usual setting for a production collector.
Manual	Does not start with Windows. Start it from Manager or Windows Services when collection is needed.

Automatic (Delayed Start) can be set in Windows Services; Manager shows it as **Automatic**.

Recovery After a Failure

If the collector service stops unexpectedly, Windows restarts it after the first and the second failure. After a third failure within one hour, it stays stopped.

After an unexpected restart, open [Diagnostic Records](#) and check the records of the run that failed.

Storage Location

The collector writes to syslog storage, which must be on a **local** disk. Network folders (mapped drives and UNC paths) are rejected as a storage location.

To keep a copy of collected messages on a network or cloud location, use the [storage archive](#).

Related Topics

- [Diagnostic Records](#) — startup and shutdown events
- [Monitoring](#) — collector status on the Server tab
- [Troubleshooting](#)
- [Syslog Server](#) — the other Syslog Watcher service

Monitoring

The [Server tab](#) in Manager shows live collector statistics. For the collector's own log, see [Diagnostic Records](#).



The counters are kept by the collector service and cover only its current run. They start at zero whenever the collector starts, for example after it is restarted or the computer reboots.

Collector in the Diagram

The [message flow diagram](#) at the top of the Server tab shows the collector at a glance:

- The **Syslog Collector** card lists the network interfaces: green for working ones, red for ones that could not start.
- **Messages between Originators and Syslog Collector:** messages received on all interfaces.
- **Discarded:** messages received but not stored, for all reasons. It turns red when the last discard was less than an hour ago, and orange when it was less than 24 hours ago.
- **Messages between Syslog Collector and Syslog Storage:** messages written to syslog storage.

Click **Syslog Collector** in the diagram to show the sections below it.

Syslog Collector

Status	Meaning
Collecting	The collector is running. Uptime shows how long it has been running. Buffer Usage shows how full the memory buffer is, for example 2% of 100,000.
Not Collecting	The collector service runs but cannot collect. Reason explains why: No network interfaces in the collector configuration .
Stopped	The collector service is stopped. Stopped At shows when. See Collector Service .

Buffer Usage turns red when it reaches **Warn if buffer is % full**. A short peak is normal during a burst. Usage that stays high means storage cannot keep up; see [Performance](#).

Network Interfaces

The table has one row for each configured [network interface](#).

Column	Description
Protocol/IP/Port	Transport, local address, and port of the listener. 0.0.0.0 is shown as AnyIPv4(0.0.0.0) , and ::0 as AnyIPv6(::0) .
Connected Clients	TCP and TLS: clients connected now and the limit, for example 3 / 100 . The limit is Maximum concurrent connections in the interface settings . UDP has no connections, so the column shows —.
Received	Total size of the syslog messages received on this interface.
Messages	Syslog messages received on this interface, before any are discarded.
Last Message	How long ago the last message arrived.

An interface that could not start is shown in red, with the error instead of counters — for example when another program already uses the port.

Discarded Messages

The table counts messages that the collector received but did not store, by reason. **Last Discarded** is red when the last discard was less than an hour ago, and orange when it was less than 24 hours ago.

Reason	Cause
License limit	The license limit on originators or messages per hour was reached.
Filtered (content)	Dropped by keywords or the regular expression of the Incoming Filter . Expected when that filter is set.
Filtered (severity)	Dropped by Filter by severity of the Incoming Filter . Expected when that filter is set.
Unknown originator	New originator ID while If originator ID is unknown is Discard messages . See Originator IDs .

Reason	Cause
Inactive originator	The originator exists but Active is No . See Inactive Originators .
No originator ID	An originator ID rule could not extract an ID, and If unable to extract ID is Discard messages .
Storage failure	A new originator could not be registered in syslog storage.
Buffer overflow	The memory buffer was full.

For what to do about each reason, see [Troubleshooting](#).

Stored Messages by Severity

Click **Syslog Storage** in the diagram to see the messages written to storage by severity, for the **Current Clock Hour**, the **Previous Clock Hour**, and **Since Collector Startup**.



A large share of **Debug** messages that nobody needs is a candidate for the [Incoming Filter](#).

Related Topics

- [Server Tab](#) — the whole dashboard, including features and archive
- [Diagnostic Records](#) — the collector's own log
- [Troubleshooting](#)
- [Performance](#)

Diagnostic Records

Diagnostic records are the collector's own log: startup, license, network interfaces, configuration changes, storage, and shutdown. They do not contain the syslog messages received from the network.

Viewing Diagnostic Records

In the **Server** section of the main toolbar, click **Collector** → **Diagnostic Records (Collector)**. The **Collector** button is shown when Manager is connected to a local or remote server.

Server Storage Last 15 Minutes Firewall denies Diagnostics (Collector)			
? Prev. Records Started: 10/10/2026 2:25:40 AM Next Records Refresh Show DEBUG records Save to File...			
Level	Timestamp (ISO Format)	Component	Diagnostic record
Info	2026-10-10 02:25:40-07:00	Main	>>> Syslog Watcher Collector version 1.0.5, Windows OS 602931718
Info	2026-10-10 02:25:40-07:00	Receiver	(Interface UDP/0.0.0.0/514) Network interface created. Maximum message length = 10000.
Info	2026-10-10 02:25:40-07:00	Main	Collector started successfully. Syslog storage: C:\ProgramData\SyslogStorage7

Diagnostics (Collector)

The tab shows the records of one collector run at a time, from the moment the collector started until it stopped. It opens on the latest run; the **Started:** drop-down shows its start time. To see earlier runs, use **Prev. Records** or the **Started:** drop-down.

The toolbar has these controls:

◀ Prev. Records	Show the records of the previous (older) collector run.
Started: drop-down	Jump to a run by its start time. The list holds the latest 200 runs.
▶ Next Records	Show the records of the next (newer) collector run.
↻ Refresh	Reload the records of the selected run.
Show DEBUG records	Show all records, including Debug and Trace , or only the important ones.
💾 Save to File...	Save the records of the selected run to a .log file.



The record files are kept in **C:\ProgramData\SyslogWatcher7\collector\logs** on the server computer.

Related Topics

- [Monitoring](#) — live collector statistics on the Server tab
- [Server Diagnostics](#) — the same kind of log for Syslog Watcher Server
- [Collector Service](#) — start and stop the collector
- [Troubleshooting](#)

Performance

The collector receives messages, processes them, and writes them to syslog storage. Storage write speed is the usual limit. When messages arrive faster than storage can write them, the [memory buffer](#) fills; once it is full, new messages are discarded as **Buffer overflow**.

Storage Write Speed

Syslog storage must be on a local disk; network folders are not accepted.

- Prefer an SSD (NVMe or SATA) over a spinning disk.
- Keep storage on a different volume from the operating system and the page file when the traffic is high.
- Exclude the storage folder from real-time antivirus scanning if the security policy allows it.

To measure what the disk can do, run the [storage speed test](#). It writes test data the same way the collector does and reports messages per second. Compare that rate with the peak rate at which your originators send messages.

Memory Buffer

The memory buffer absorbs bursts while storage catches up. Watch **Buffer Usage** in the [Syslog Collector](#) section of the Server tab.

- Short peaks that fall back to a low value are normal.
- Usage that stays high, or **Buffer overflow** in [Discarded Messages](#), means storage is too slow for the sustained rate. A larger buffer only helps with bursts, not with a sustained rate that storage cannot write.

Size the buffer for the longest burst it must absorb: at 5,000 messages per second, the initial buffer of 100,000 messages covers about 20 seconds. The buffer holds messages in RAM, so a larger value needs more memory.

Incoming Filter

Discarding unwanted messages before storage is the cheapest way to cut load. If much of the traffic is never used (for example **Debug** from verbose originators), the [Incoming Filter](#) removes it before it enters the memory buffer.

The [stored messages by severity](#) on the Server tab help to choose a severity threshold.

Character Encoding

Converting messages from another encoding adds a small cost per message; messages with only ASCII characters are not converted. Keep **UTF-8** when originators already send UTF-8, as most do today. See [Preprocessor](#).

Transport

UDP has the lowest cost per message. TCP adds connection handling, and TLS adds encryption on top of that. Use TLS where messages must be encrypted; its CPU cost matters only with very high message rates or many connections.

For bursts on UDP, increase **Socket buffer size** in [Advanced Options](#) only after the storage and buffer checks above, and preferably with technical support.

High-Volume Checklist

1. Run the [storage speed test](#) and move storage to a faster local disk if needed.
2. Drop unneeded traffic with the [Incoming Filter](#).
3. Size the memory buffer for bursts.
4. If one server still cannot keep up, split the load: install Syslog Watcher on a second server and point some of the originators to it.

Related Topics

- [Monitoring](#)

- [Memory Buffer](#)
- [Incoming Filter](#)
- [Test Storage Speed](#)

Troubleshooting

When the collector misbehaves, first check these two places in Manager:

- The collector sections of the [Server tab](#) — see [Monitoring](#).
- [Diagnostic Records](#) — look for the first **Error** of the latest collector run.

No Messages Arrive

Symptom	Likely cause	Resolution
Collector status Stopped	Collector service not running	Click Start Collector on the Server tab, or * Collector → Start Syslog Collector in the Server section of the main toolbar. See Collector Service .
Status Not Collecting , reason No network interfaces in the collector configuration .	No listener configured	Add one in Network Interfaces .
Interface row in red: Another service or application uses this protocol/network address/port .	Another program already uses the address and port	The error names the program after Occupied by: . If it does not, find the program with <code>netstat -ano</code> , or with <code>Get-NetUDPEndpoint</code> / <code>Get-NetTCPConnection</code> in PowerShell. Stop it, or change the port in Network Interfaces . The collector retries every 5 seconds, so the interface starts once the port is free.
Interface Messages = 0, no errors	Traffic does not reach the collector	Check that the originator sends to this computer's IP address, the same port, and the same transport (UDP vs TCP). Allow the port in Windows Defender Firewall, for example: <code>netsh advfirewall firewall add rule name="Syslog UDP 514" dir=in action=allow protocol=UDP localport=514</code>
Interface Messages > 0, but nothing in views	Messages are discarded, or the view filters them out	Check Discarded Messages . If nothing is discarded, check the view's time range and filter.

Messages Are Discarded

The **Discarded Messages** table on the Server tab names the reason.

Reason	Resolution
License limit	The license limit on originators or messages per hour is reached. The Free License allows 3 originators and 5000 messages per hour. See License Management .
Filtered (content) / Filtered (severity) higher than expected	Review the Incoming Filter . Matching is case-sensitive and includes the syslog header. With If message matches set to Accept it , messages that do not match the regular expression are discarded.
Unknown originator	If originator ID is unknown is Discard messages . Add the originator manually in Syslog Originators , or switch the setting to Add new originator .
Inactive originator	Set Active to Yes on that originator .
No originator ID	An IP range rule cannot extract the ID from these messages. Fix the rule, or set If unable to extract ID to Apply the default rule .
Storage failure	A new originator could not be registered in syslog storage. Read the Failed to register syslog originator record in Diagnostic Records . Check free disk space and permissions on the storage folder .
Buffer overflow	Messages are not written to storage fast enough, or not at all. If writes fail (disk full, storage folder unavailable), the collector keeps retrying and the buffer fills up; check Diagnostic Records . If storage is too slow: for bursts, increase Buffer size (messages) in Memory Buffer ; for sustained load, see Performance .

TLS Connection Issues

See [Syslog over TLS — Troubleshooting](#) for handshake, fingerprint, and name check errors.

Other Problems

Symptom	Likely cause	Resolution
Start Syslog Collector fails	The configuration cannot be loaded, or another error during startup	Open Diagnostic Records and read the first Error of the latest collector run.
The collector runs but stores nothing; Diagnostic Records show Collector started without syslog storage; not accepting syslog .	Storage folder missing or not accessible	Check the path in Syslog Storage , then restart the collector.
Diagnostic Records show [License] Failed to load license ; License limit discards	The license file cannot be loaded; the collector uses the Free License limits	See License Management .

Symptom	Likely cause	Resolution
Collector stops unexpectedly	The collector failed while running	Windows restarts it; see Recovery After a Failure . Compare with the last good run (Prev. Records), click Save to File... , and contact technical support .

Related Topics

- [Monitoring](#)
- [Diagnostic Records](#)
- [Network Interfaces](#)
- [Syslog over TLS](#)
- [Performance](#)
- [Technical Support](#)

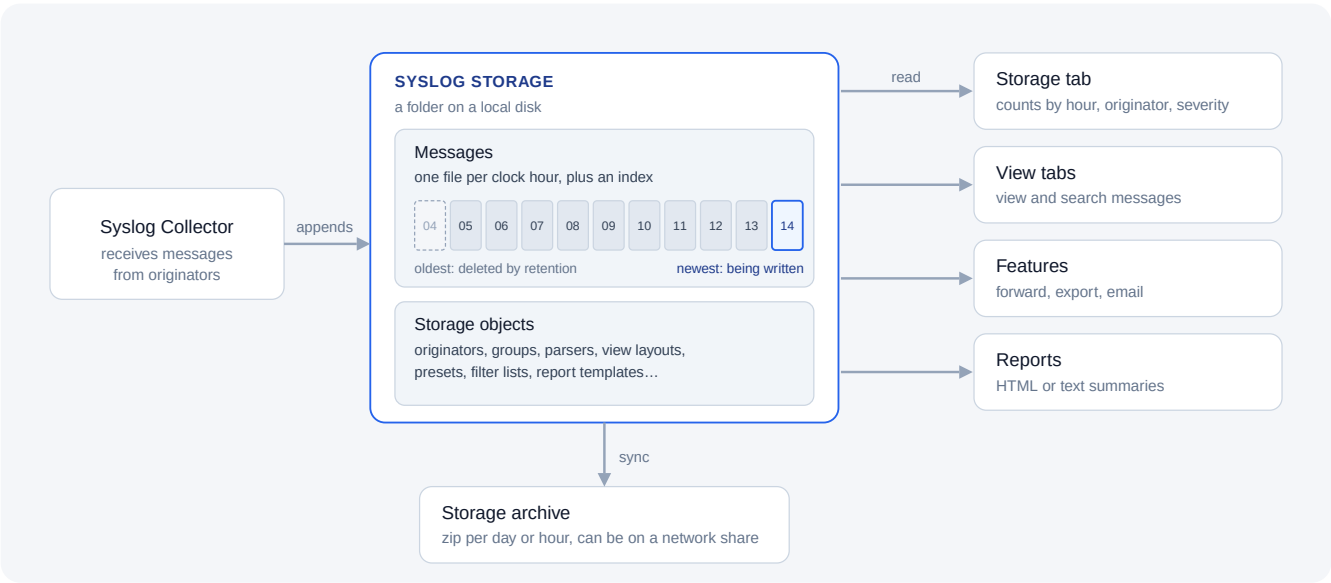
Syslog Storage

Syslog storage is the local file-based database where the **collector** writes every message it receives. No external database is required.

View tabs, features, and reports all read from the storage. The collector only appends to it, so the storage works as a large buffer: collection continues even when a feature or report is slow or stopped.

The storage holds two kinds of data:

- **Messages** — one file per clock hour, plus an index.
- **Storage objects** — **originators**, **groups**, **parsers**, **view layouts**, **View/Search presets**, **filter lists**, **field collections**, **field dictionaries**, **report templates**, and **severity and facility names**.



What writes to syslog storage and what reads from it (simplified schematic)

Storage Button

What the  **Storage** button in the **Storage** section of the main toolbar does depends on what Manager is connected to:

Manager is	The Storage button
Connected to the local server	Opens a drop-down with Syslog Storage Location... , Storage Settings... , and Test Storage Speed...
Connected to a remote server	Opens Storage Settings .
Not connected to a server	Opens a drop-down with Open Storage Folder... , or Close Storage when a storage folder is open.

Time Zone

Calendar days on the **Storage tab** and the **RECEIVED** field use the time zone of the Syslog Watcher

Server computer. When Manager [opens a storage folder without a server](#), it uses the time zone of the Manager computer. The Storage tab status bar shows the time zone in use. Use `RECEIVED_UTC` when a value must follow UTC.

The server reads the time zone when its service starts. After changing the Windows time zone, restart the Syslog Watcher Server service.

Each storage also records the server time zone when it is created, and [daily archive](#) files use that recorded time zone. It differs from the current server time zone when the storage was created in another time zone: on another computer, before the computer's time zone was changed, or by Syslog Watcher 6 (after a [migration from version 6](#)).

In This Section

- [Storage Location and Limits](#) — move the storage, set retention limits
- [Storage Overview](#) — what the storage contains, by day, hour, and originator
- [Storage Maintenance and Archive](#) — enforce retention, keep a compressed copy
- [Open a Storage Folder Without a Server](#) — view an extracted archive or a copied storage
- [Test Storage Speed](#) — measure the disk write rate

Related Topics

- [Memory Buffer](#)
- [Performance](#)

Storage Location and Limits

[Syslog storage](#) is a folder on a local disk. Without a server, Manager can also open a storage folder directly; see [Open a Storage Folder Without a Server](#). What the  **Storage** button offers depends on the connection; see [Storage Button](#).

Storage Location

The default location is `C:\ProgramData\SyslogStorage7`.

To change it:

1. Make sure Manager is connected to the local server.
2. In the **Storage** section of the main toolbar, click  **Storage** → **Syslog Storage Location...**
3. Set **Path** to a folder on a local disk, and click **Apply**.
4. Manager disconnects from the server to apply the change; connect again.

Network folders (mapped drives and UNC paths) are rejected. To keep a copy of messages on a network or cloud location, use the [storage archive](#).



A new syslog storage is created in the new folder. Messages and storage objects in the old folder are not moved; the old folder stays on disk.



Check the disk with [Test Storage Speed](#) before moving the storage to it.

Storage Settings

Storage settings are the retention limits. They are saved in the storage itself, not in the server configuration.

Open them in one of these ways:

- ▶ Connected to the local server: in the **Storage** section of the main toolbar, click  **Storage** → **Storage Settings...**
- ▶ Connected to a remote server: in the **Storage** section of the main toolbar, click  **Storage**.

On a remote server, only users with the **Admin role** can change them; for other users the window opens as **Storage Settings (Read Only)**.

Setting	Initial	Description
Delete files older than	3650 days	Maximum age of stored messages, in hours or days.
Maximum storage size (GB)	10000	Maximum total size of the storage. When it is exceeded, the oldest files are deleted.

Files are deleted by clock hour, oldest first.



The limits are applied only when **Enforce storage limits** is on in [Storage Maintenance](#). It is off by default, so nothing is deleted until you turn it on.

Related Topics

- [Syslog Storage](#)
- [Open a Storage Folder Without a Server](#)
- [Storage Maintenance and Archive](#)
- [Test Storage Speed](#)

Storage Overview

The **Storage** tab gives a high-level view of what syslog storage contains: how many messages arrived in each hour and from each originator, by severity. Use it to find when a problem started, or which originator suddenly sends more (or fewer) messages.



Click any count to see those messages in a view tab.

Calendar

The calendar on the left shows days that have messages in bold on a blue background; the more messages, the darker the blue. Select a day or a range of days; the table shows message counts for the selected days.

The number of days you can select together is set by **Maximum selected days** (1–999) in [Manager Settings](#).



Days follow the [server time zone](#).

Tab Toolbar

○ Refresh	Reload the counts now.
Auto: OFF	Auto-refresh drop-down: Every 5 sec , Every 10 sec , Every 15 sec , Every 30 sec , Every 60 sec , or Auto: OFF .
Distribution:	Table layout: 🕒 Time range or 🎯 Originators ; see Distribution below.
Show:	In Time range mode only: count messages from ALL ORIGINATORS , one originator group (Group: <name>), or <select originators> .

Distribution

Mode	Rows
🕒 Time range	One row per clock hour of the selected days, grouped by Date . Columns: Time range , Disk size , ALL LEVELS , and one column per severity.
🎯 Originators	One row per originator that has messages in the selected days. Columns: Originator ID , Originator name , ALL LEVELS , and one column per severity.

When the selection has messages, a summary row on top totals it: **ENTIRE RANGE** in **Time range** mode, with the total **Disk size**, or **ALL ORIGINATORS (N)** in **Originators** mode.

Messages from deleted originators are combined into one **<deleted>** row, and from disabled originators into one **<disabled>** row. These rows have no **Originator ID**, and their counts do not open a view tab.

Open Messages from a Cell

Click a message count to open a new [view tab](#) with exactly those messages. The tab opens right away, without the **New View Tab** window.

The new tab loads:

- the row's hour (in **Time range** mode) or originator (in **Originators** mode); a count in the

summary row covers all rows

- the column's severity, or all severities for **ALL LEVELS**
- the selected days, and the **Show:** filter in **Time range** mode

Related Topics

- [Syslog Storage](#)
- [View/Search Messages](#)
- [Server Tab](#)

Storage Maintenance and Archive

On the **Storage Maintenance** page of **Server Configuration**, you turn on storage retention and set up the **storage archive**. The **Syslog Watcher Server** service does both.

In the **Server** section of the main toolbar, click  **Server** →  **Server Configuration...**, then open **Storage Maintenance**.

Syslog Storage Retention

Setting	Initial	Description
Enforce storage limits	Disabled	Delete files that exceed limits — the server checks the storage size and file age, and deletes files beyond the limits. Disabled — nothing is deleted.

The limits themselves (**Delete files older than**, **Maximum storage size (GB)**) are set in [Storage Settings](#).



After a [migration from version 6](#), retention is off so that you can review the migrated limits first.

Storage Archive

The **storage archive** is a periodically synchronized, compressed copy of the syslog storage. Compression gives up to 10× longer retention for the same disk space, and the archive can be on a remote disk or network share.

Each sync writes zip files for the hours or days that have closed since the previous sync. Each zip holds a copy of the storage index and the message files for its period.

Setting	Description
Synchronize archive	Disabled — no archive; the other archive settings are hidden. Daily — one zip per calendar day (storage time zone), written shortly after midnight. Hourly — one zip per clock hour, written shortly after the hour ends.
Archive location	Folder for the archive files. Required when sync is on. It can be a network path if the server service account can write to it.
Protect files with password	Optional password for the zip files. Use a secret string (%EXAMPLE%) instead of the actual password. The files use standard ZIP password protection, so Windows Explorer can extract them.
Limit archive retention	Yes, delete older archive files deletes archive files older than Keep archive files for (days) (1–36500, initial 365). It only deletes old archive files; it does not limit what the next sync writes.
Execute command after syncing	Optional command line run after each sync. See Command After Sync .



Daily and hourly archives use different file names and folder layouts. Do not switch an existing archive folder between them; use a new folder, or delete the files in the folder first.

Command After Sync

Use the command to process new archive files, for example to copy them to cloud storage. `{ARCHIVE_DIR}` in the command line (and in **Work folder**) is replaced with the archive folder.

Setting	Description
Execute command after syncing	Command line. Example: <code>powershell.exe -File C:\Scripts\Upload-Archive.ps1 "{ARCHIVE_DIR}"</code>
Work folder	Working folder for the process.
Run as	Windows account that runs the command: <code>DOMAIN\user</code> , <code>user@domain</code> , or a local name. Leave empty to run the command as the server service account.
Password	Password for Run as . Use a secret string .
Command timeout	Seconds to wait (1–86400). A command that runs longer is stopped.

The command result is written to [Server Diagnostics](#).

Archive Status

Click **Syslog Storage** on the [Server tab](#) diagram. The **Syslog Archive** section shows the archive folder and:

Last Sync When the last sync ran.

Next Sync	When the next sync is due.
Duration	How long the last sync took.
Synced	Storage size → archive size written by the last sync (for example 1.2 GB → 140 MB), or Up to date when nothing new had to be archived.

A sync error is shown in red under the list. When the archive is off, the section shows **Storage archive is disabled**.

Viewing Archived Messages

To view messages from an archive file, extract it to an empty folder and open that folder in Manager without a server. See [Open a Storage Archive File](#).

Related Topics

- [Syslog Storage](#)
- [Syslog Server](#)
- [Secret Strings](#)

Open a Storage Folder Without a Server

When Manager is not connected to a server, it can open a [syslog storage](#) folder directly and read the storage files itself.

Use this to:

- ▶ View messages from a [storage archive](#) file after you extract it.
- ▶ View a storage copied from another computer.
- ▶ Generate reports from a storage opened this way.
- ▶ View a Syslog Watcher 6 storage that was not migrated.

Open a Storage Folder

1. If Manager is connected to a server, in the **Server** section of the main toolbar, click  **Server** → **Disconnect** and confirm.
2. In the **Storage** section of the main toolbar, click  **Storage** → **Open Storage Folder...**
3. In the **Select Storage Folder** window, select the folder that contains the storage index file: **storage7.index**, or **storage.index** for a version 6 storage.

Manager opens the [Storage tab](#), and the window title shows the folder path. Changes to storage objects (originators, groups, parsers, view layouts, and so on) are saved in the opened folder.



By default, Manager connects to the local server when it starts. To start without a server, set **Auto-connect to local server** to **No** in [Manager Settings](#).

Open a Storage Archive File

Each [archive file](#) is a zip with a copy of the storage index and the message files for its hour or day.

1. Copy the zip file to a local disk.
2. Extract it to an empty folder.
3. Open the folder as described in [Open a Storage Folder](#).



To view several archive files together, extract them into the same folder from oldest to newest, replacing existing files. Each archive file holds a copy of the storage index from its sync, and only the newest copy covers all extracted hours.

Read-Only Storage

Manager opens the storage for viewing only when:

- ▶ it cannot write to the folder, or
- ▶ the folder holds a version 6 storage (`storage.index`).

Manager then shows **Syslog storage is open for viewing only (read-only)**.

To edit a version 7 storage, restart Manager as Administrator, and make sure the storage files are not marked read-only. A version 6 storage always opens read-only.

Time Zone

Without a server, calendar days on the Storage tab and the **RECEIVED** field use the time zone of the Manager computer, not the time zone recorded in the storage. The Storage tab status bar shows it. Exception: for a version 6 storage, **RECEIVED** uses the time zone saved in that storage, if it has one. See [Time Zone](#).

Close the Storage

In the **Storage** section of the main toolbar, click  **Storage** → **Close Storage** and confirm. The **Server** section appears again.

Related Topics

- [Syslog Storage](#)
- [Storage Maintenance and Archive](#)
- [Syslog Watcher Manager](#)

Test Storage Speed

Test Storage Speed measures how many messages per second syslog storage can write to a disk. The test writes generated messages the same way the collector writes received ones.



The test generates messages of all eight severity levels, which is rare in practice: most originators send only two or three. Fewer severity levels make indexing faster, so real performance is usually noticeably higher than the test result.

Use it to:

- ▶ Check a disk before moving the [storage location](#) to it.
- ▶ Estimate hardware for an expected message rate.
- ▶ Find out whether storage is the bottleneck when the [buffer usage](#) stays high.

Run the Test

1. Make sure Manager is connected to the local server.
2. In the **Storage** section of the main toolbar, click  **Storage** → **Test Storage Speed...**
3. Set the [test parameters](#).
4. Click ▶ **Start Test**. The first results appear after about 5 seconds.
5. Let it run for a minute or more, then click ■ **Stop Test**. The test waits for queued messages to be written and deletes the test files.

 Test Storage Speed

▼ Test Parameters

Location	C:\ProgramData\SyslogStorage7
Number of syslog originators	10
Average message length	250

Test Parameters

Parameters for the storage write throughput test. The test writes into a `_speed_test_` folder under Location and deletes it when the test stops.

Writing to C:\ProgramData\SyslogStorage7_speed_test_
Originators: 10, average message length: 250
Waiting for the first results (about 5 seconds)...

[5 sec]	speed=154,613 msg/s	avg=154,613 msg/s	total=774,224	184 MB
[10 sec]	speed=144,394 msg/s	avg=149,503 msg/s	total=1,497,562	356 MB
[15 sec]	speed=142,182 msg/s	avg=147,064 msg/s	total=2,208,848	526 MB
[20 sec]	speed=141,925 msg/s	avg=145,780 msg/s	total=2,919,030	695 MB
[25 sec]	speed=140,432 msg/s	avg=144,710 msg/s	total=3,622,103	863 MB
[30 sec]	speed=137,564 msg/s	avg=143,518 msg/s	total=4,311,378	1,027 MB
[35 sec]	speed=154,514 msg/s	avg=145,091 msg/s	total=5,086,162	1,212 MB
Stopping: waiting for the queue to drain...				
[37 sec]	speed=141,226 msg/s	avg=144,900 msg/s	total=5,344,053	1,274 MB

Stopped.

?

▶ Start Test

■ Stop Test

Close

Test Storage Speed window



The test writes real data to the disk, which slows down other work on that disk. Run it outside busy hours when testing the disk that holds the live storage.

Test Parameters

Setting	Initial	Description
Location	Storage folder	Folder on the disk to test. The test creates a <code>_speed_test_</code> subfolder there and deletes it when the test stops.
Number of syslog originators	10	Rough estimate of the real number of originators (1–100000). Storage writes per originator, so this value affects the result.
Average message length	250	Average message body length in bytes (50–10000).

Messages get random severities, weighted toward the less important levels.

Results

A new result line appears every 5 seconds:

Value	Meaning
<code>[N sec]</code>	Time since the start.
<code>speed</code>	Messages per second in the last interval.
<code>avg</code>	Average messages per second since the start.
<code>total</code>	Messages written, followed by the data size.

Read `avg` once it stops changing much. Keep the peak incoming message rate well below it: the collector also parses messages, and features and view tabs read from the same disk.

Related Topics

- [Performance](#)
- [Syslog Storage](#)

Syslog Originators

A **syslog originator** is the device, server, or application that generates a syslog message — not a relay or proxy that only forwards it. Syslog Watcher links each stored message to its originator.

Each originator is a record in syslog storage with:

- **ID** — identifies which originator sent a message; in simple cases, the sender's IP address
- **Name** — a human-readable name; in simple cases, the host name resolved by reverse DNS lookup
- **Parser** — extracts fields from the originator's messages (see [Syslog Parsers](#))
- **Groups** — the [originator groups](#) it belongs to
- **Active** — whether the originator is in use; see [Inactive Originators](#)

The [collector](#) adds originators automatically when the first message from a new ID arrives. You can also add, edit, and delete them in Manager.

To manage originators, in the **Storage** section of the main toolbar, click  **Originators** (see [Managing Originators](#)). To manage groups, click  **Groups** (see [Originator Groups](#)).



In Syslog Watcher 5 and earlier, an originator was called a **syslog source**.

Originator ID

The **originator ID** is a text string that identifies the originator of a message. The collector assigns an ID to every incoming message and uses it to find the originator record. IDs are case-sensitive and cannot be changed after the originator is created.

By default, the ID is the IP address of the message sender. This works when originators send their messages directly to Syslog Watcher and keep the same IP address.

When the Default Rule Does Not Work

When messages pass through a syslog relay or proxy, every message arrives from the relay's address, so all of them would get the same ID.

When originators get their IP addresses dynamically, for example from DHCP, an originator's address changes over time. Each new address becomes a new ID, so one originator is split into several records. If another originator later gets an old address, its messages are stored under the wrong record.

Originator ID Rules

In both cases, add [Originator ID Rules](#) in the collector settings. A rule covers a range of sender IP addresses and takes the ID from the message itself:

- **Extract as RFC5424:HOSTNAME** — the host name from the RFC 5424 header.

- **Extract as RFC5424:HOSTNAME/APPNAME** — host name and application name, for one originator per application on each host.
- **Extract with regular expression** — the text captured by the groups (...) of a regular expression, joined in order without a separator. The expression can match anywhere in the message. To group without capturing, use (?:...).

The rules are checked in order; the first rule whose range contains the sender's address applies. If the ID cannot be extracted, the rule either uses the sender IP address or discards the message.

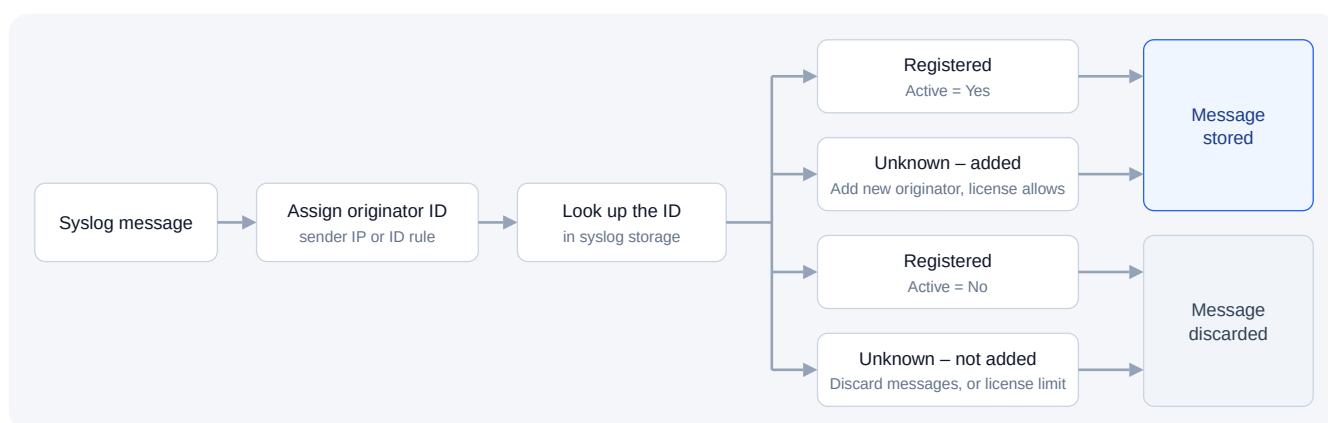
Table: Originator IDs produced by different rules

Message	Rule	Originator ID
Sent directly from 192.168.1.10	None (default)	192.168.1.10
1 2026-10-12T08:15:00Z fw01 sshd 412 - - Login failed, relayed by 10.0.0.5	Extract as RFC5424:HOSTNAME for 10.0.0.5	fw01
The same message	Extract as RFC5424:HOSTNAME/APPNAME for 10.0.0.5	fw01/sshd
site=riga dev=fw01 Login failed, relayed by 10.0.0.5	Extract with regular expression site=(\S+) dev=(\S+) for 10.0.0.5	rigafw01
1 2026-10-12T08:15:00Z laptop-17 agent - - - Started, sent directly from a DHCP address in 192.168.50.0-192.168.50.255	Extract as RFC5424:HOSTNAME for 192.168.50.0-192.168.50.255	laptop-17, whatever its current address



Changing the rules changes the IDs of new messages. Messages with a new ID go to a new originator, and the old originator stops receiving messages.

How Originators Are Registered



How the collector registers originators

The collector assigns an originator ID to every incoming message, then looks up the ID in syslog storage:

- **Registered, Active = Yes** — the message is stored.
- **Registered, Active = No** — the message is discarded.
- **Unknown ID** — the collector setting **If originator ID is unknown** decides:
 - **Add new originator** — the collector adds the originator and stores the message.

- **Discard messages** — the message is discarded and nothing is added.

A new originator gets the default parser, and its **Name** is the same as its ID. If [Resolve name \(reverse DNS lookup\)](#) is **Yes** and the ID is the sender's IP address, the collector then looks up the host name in the background. When the lookup succeeds, the name is replaced with the host name, unless someone has changed the name in the meantime.

License Limit

The [license](#) limits how many active originators the collector accepts. Inactive originators do not count.

- When the limit is reached, the collector does not add new originators; messages from unknown IDs are discarded.
- When there are more active originators than the limit allows, for example after you add them manually or the license changes, the collector stores messages only from the oldest active originators, up to the limit. Messages from the others are discarded.

[Collector monitoring](#) shows how many messages were discarded and why.

Inactive Originators

To take an originator out of use, deactivate it rather than delete it: set **Active** to **No** in the [originator properties](#). You can deactivate several originators at once.

An inactive originator is not used anywhere:

- The collector discards its new messages.
- View tabs, reports, features, and the message counts on the [Storage tab](#) skip its messages, whether the filter is **ALL ORIGINATORS**, a group, or selected originators.
- It does not count toward the [license limit](#).

Its messages stay in syslog storage, and its name, parser, and groups are kept. Set **Active** back to **Yes** to use it again; its stored messages reappear.

Inactive originators are still listed in the [Syslog Originators](#) window.

Related Topics

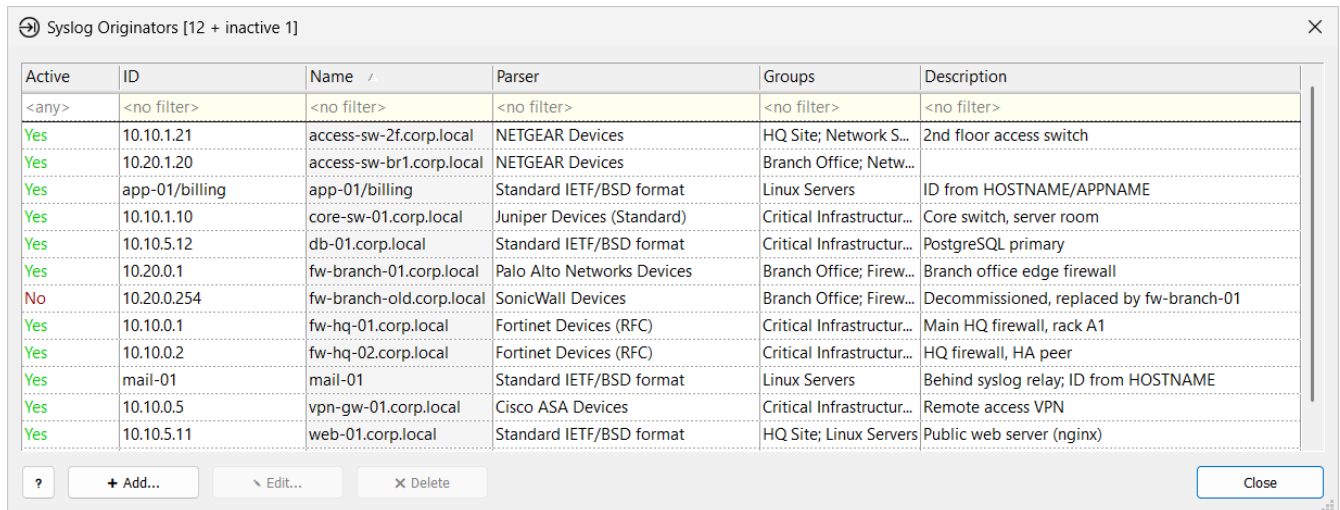
- [Managing Originators](#) — add, edit, and delete originators
- [Originator Groups](#)
- [Originator IDs](#) — how the collector assigns IDs
- [Syslog Parsers](#)

Managing Originators

The **Syslog Originators** window lists every **originator** in syslog storage. Use it to set an originator's name, parser, and groups, to deactivate originators, or, in rare cases, to add one before it starts sending.

Open it in one of these ways:

- In the **Storage** section of the main toolbar, click  **Originators**. The button is shown when Manager is connected to a server or has a storage folder open.
- On the **Server** tab, click **Originators**.



Active	ID	Name	Parser	Groups	Description
<any>	<no filter>	<no filter>	<no filter>	<no filter>	<no filter>
Yes	10.10.1.21	access-sw-2f.corp.local	NETGEAR Devices	HQ Site; Network S...	2nd floor access switch
Yes	10.20.1.20	access-sw-br1.corp.local	NETGEAR Devices	Branch Office; Netw...	
Yes	app-01/billing	app-01/billing	Standard IETF/BSD format	Linux Servers	ID from HOSTNAME/APPNAME
Yes	10.10.1.10	core-sw-01.corp.local	Juniper Devices (Standard)	Critical Infrastructur...	Core switch, server room
Yes	10.10.5.12	db-01.corp.local	Standard IETF/BSD format	Critical Infrastructur...	PostgreSQL primary
Yes	10.20.0.1	fw-branch-01.corp.local	Palo Alto Networks Devices	Branch Office; Firew...	Branch office edge firewall
No	10.20.0.254	fw-branch-old.corp.local	SonicWall Devices	Branch Office; Firew...	Decommissioned, replaced by fw-branch-01
Yes	10.10.0.1	fw-hq-01.corp.local	Fortinet Devices (RFC)	Critical Infrastructur...	Main HQ firewall, rack A1
Yes	10.10.0.2	fw-hq-02.corp.local	Fortinet Devices (RFC)	Critical Infrastructur...	HQ firewall, HA peer
Yes	mail-01	mail-01	Standard IETF/BSD format	Linux Servers	Behind syslog relay; ID from HOSTNAME
Yes	10.10.0.5	vpn-gw-01.corp.local	Cisco ASA Devices	Critical Infrastructur...	Remote access VPN
Yes	10.10.5.11	web-01.corp.local	Standard IETF/BSD format	HQ Site; Linux Servers	Public web server (nginx)

? + Add... Edit... Delete Close

The Syslog Originators window

Add an Originator

You rarely need to: the collector adds originators automatically when **If originator ID is unknown** is **Add new originator**. Add one manually when that setting is **Discard messages**, or to set the name, parser, and groups before the first message arrives.

1. Click **Add...** or press .
2. If Manager is connected to a server that adds originators automatically, it asks whether you still want to add one manually. Click **Yes**.
3. In the **New Syslog Originator** window, enter the **ID** and **Name**, and set the other **properties**.
4. Click **Create**.

The **ID** must match the ID the collector assigns to the originator's messages: in simple cases its IP address, otherwise the value extracted by an **originator ID rule**.

Edit Originators

1. Select one or more originators.
2. Click **Edit...**, double-click the row, or press .
3. Change the **properties** and click **Apply**.

When you select several originators, the **Edit Multiple Syslog Originators** window shows only **Active**, **Parser**, and **Groups**. If a value differs across the selection, it shows as **<different states>** or **<different parsers>**. A group that contains only some of the selected originators shows a mixed check box. Values you do not change are kept as they are.

Delete Originators

1. Select one or more originators.
2. Click **Delete** or press **Delete**.
3. Confirm with **OK**.



Deleting removes the originator record and its group memberships. Its messages stay in syslog storage.

If a deleted originator sends again and automatic adding is on, the collector adds it as a new originator with the default parser and no groups.



To stop storing messages but keep the settings, **deactivate** the originator instead.

Originator Properties

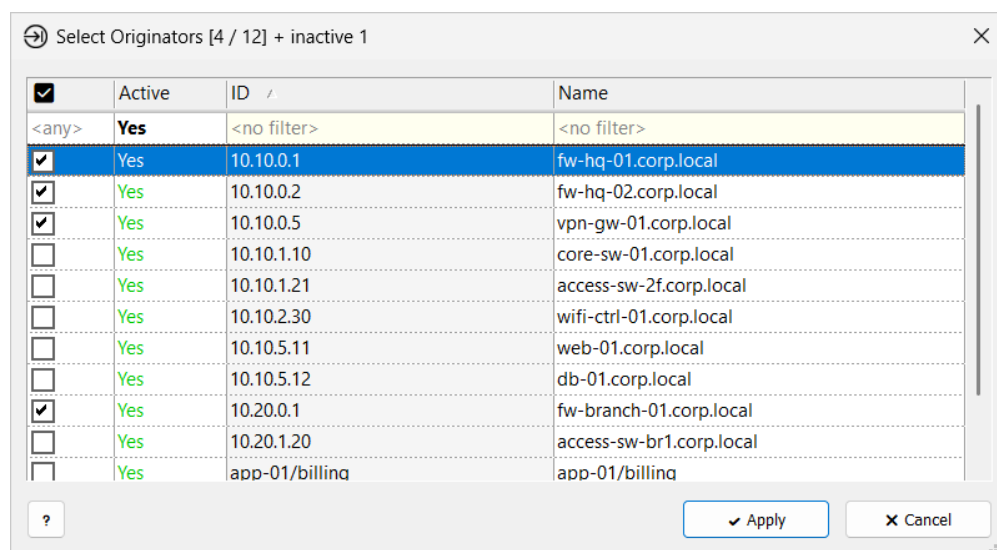
The Edit Syslog Originator window

Active	Whether the originator is in use. If No , it is inactive : the collector discards its new messages, and view tabs, reports, and features skip its stored messages. Inactive originators do not count toward the license limit . New originators are active.
ID	Unique originator ID; in simple cases, the originator's IP address. Required; it cannot be changed after the originator is created.
Name	Required display name, used in the Manager lists, filters, and reports.

Description	Optional comment, shown under Name .
Parser	The parser for this originator's messages. New originators get the default parser. Parsers whose names start with Installation: ship with the product. If you choose one, Manager offers to copy it to syslog storage when you click Apply or Create , and assigns the copy.
Groups	Check the groups this originator belongs to. Shows <no groups> if no groups exist.

Select Originators Window

The **Select Originators** window opens when you choose **<select originators>** in a [message filter](#) or click **Select Originators...** in the [group properties](#).



The Select Originators window

Check the originators to include, then click **Apply**.

- Click a check box to check or clear one originator.
- To change several, select the rows, then press **Space** or double-click to invert their checks, or right-click and choose **Set Checkmarks**, **Clear Checkmarks**, or **Invert Checkmarks**.

The window opens with **Active** set to **Yes** in the filter row, so only active originators are listed. Choose **<any>** to show inactive ones too. In the other columns of the filter row, type text to show only the rows that contain it; case is ignored. In the check box column, choose **Yes** or **No** to show only checked or unchecked originators.

The title shows the number of checked originators and the number of active originators, for example **Select Originators [3 / 12]**. It adds + **inactive N** if checked originators are inactive, and + **deleted N** if the filter lists deleted originators. A deleted originator is an ID that a message filter still lists but that is no longer in storage. It is shown grayed out, cannot be checked or cleared, and is removed from the filter when you click **Apply**.

A message filter with no originators selected includes all originators. If no originators are left when you click **Apply**, for example because you cleared them all or all of them were deleted, Manager

warns you first.

Read-Only Access

You cannot change originators when the storage folder is open read-only, or when your [role](#) on a remote server is **Observer**. In that case:

- The **Syslog Originators** window title shows **(Read Only)**. **Add...** and **Delete** are unavailable, and **Edit...** becomes **View...**
- The originator properties window is titled **Originator (Read Only)**, or **Properties of Multiple Originators (Read Only)** for several originators, and **Apply** is unavailable.

Related Topics

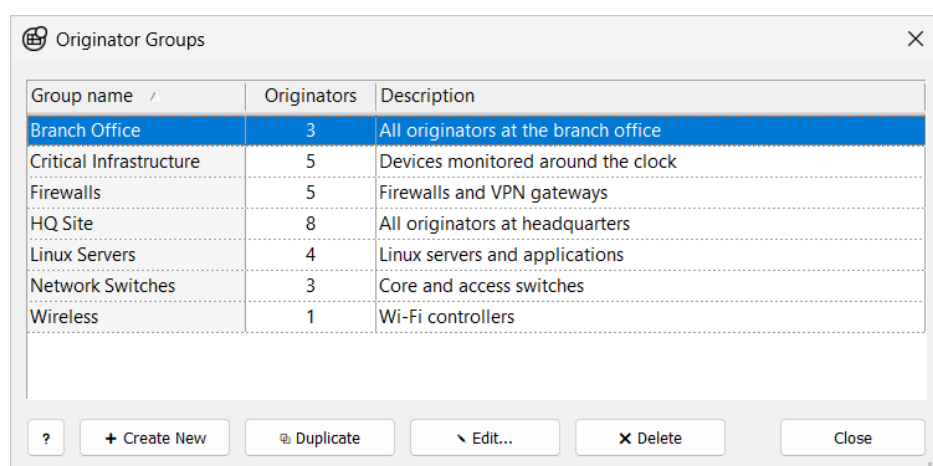
- [Syslog Originators](#) — what originators are and how the collector registers them
- [Originator Groups](#)
- [Syslog Parsers](#)
- [Filtering](#)

Originator Groups

An **originator group** is a named set of [originators](#). A [message filter](#) in a feature, view tab, or report can select a group (**Group: <name>**) instead of listing originators one by one. When you add an originator to a group, every filter that uses the group includes it.

An originator can belong to more than one group.

To open the **Originator Groups** window, in the **Storage** section of the main toolbar, click  **Groups**.



The Originator Groups window



Filters refer to a group by its name. If you rename or delete a group, filters that use the old name match no originators until you select a group again.

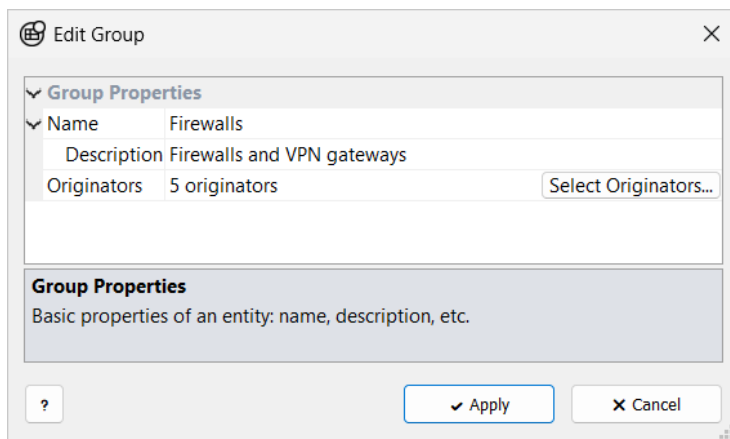
Create a Group

1. Click **Create New** or press `Insert`. To start from an existing group, select it and click **Duplicate** instead.
2. In the **New Group** window, change the **Name** and add a description if needed.
3. Next to **Originators**, click **Select Originators...**, check the members in the [Select Originators](#) window, and click **Apply**.
4. Click **Create**.

You can also add an originator to groups from its [Groups](#) property.

Edit a Group

Select a group and click **Edit...**, double-click it, or press `Enter`. Change the [properties](#) and click **Apply**.



The Edit Group window

Name	Required; must be unique.
Description	Optional comment, shown under Name .
Originators	The members, shown as a count (for example 3 originators). Click Select Originators... or double-click the value to change them.

Delete a Group

Select a group, click **Delete** or press `Delete`, and confirm with **OK**. The originators in the group are not deleted.

Read-Only Access

You cannot change groups when the storage folder is open read-only, or when your [role](#) on a remote server is **Observer**. In that case:

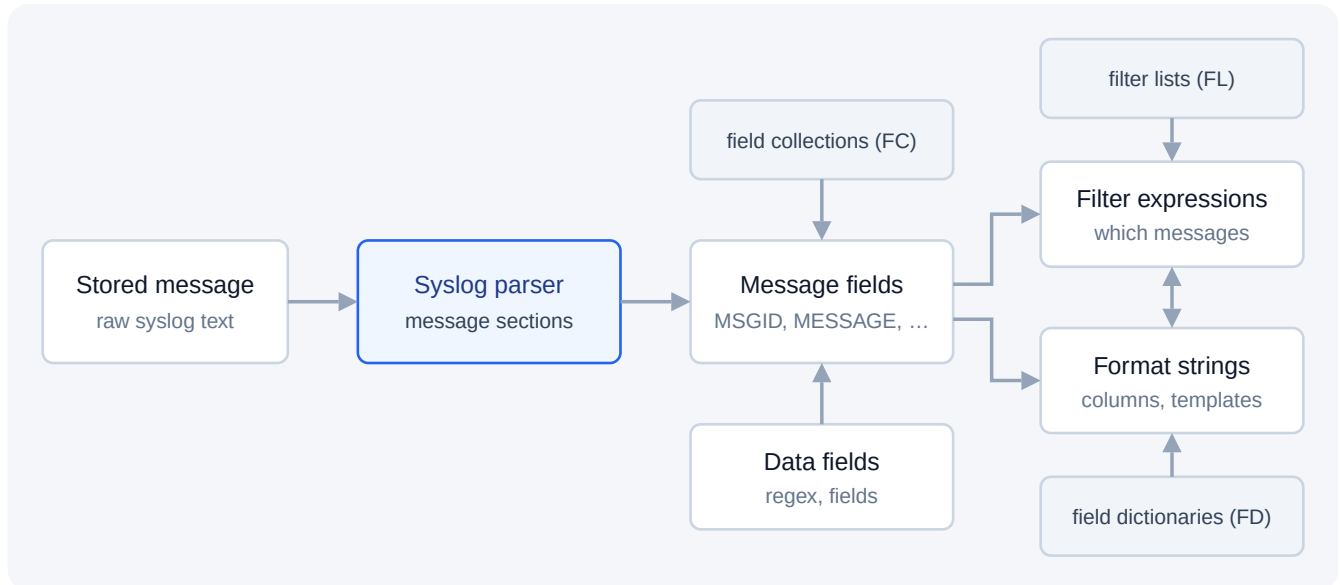
- The **Originator Groups** window title shows **(Read Only)**. **Create New**, **Duplicate**, and **Delete** are unavailable, and **Edit...** becomes **View...**
- The group properties window is titled **Group (Read Only)**, and **Apply** is unavailable.

Related Topics

- [Syslog Originators](#)
- [Managing Originators](#)
- [Filtering](#)

Syslog Messages

Syslog Watcher keeps each message in syslog storage as it was received. When a view tab, feature, or report reads a message, the originator's syslog parser splits it into **message fields**. Filter expressions use those fields to select messages; format strings print them into view columns, files, emails, and requests.



How message fields are produced and used (simplified schematic)

Parsers and Fields

- [Syslog Parsers](#) split a message into fields such as **TIMESTAMP**, **HOSTNAME**, and **MSGID**.
- [Message Fields](#) lists the built-in fields, such as **RECEIVED**, **SEVERITY**, and **MESSAGE**.
- [Severity and Facility Names](#) changes the names printed for severities and facilities.

Field Extraction

- [Field Extraction](#) adds fields from the message body, in the **Data Fields (Optional)** section of features, view layouts, parsers, and report templates.
- [Field Collections](#) give names to the values in vendor messages, with a rule for each message type.

Filtering

- [Filtering](#) selects messages by severity, originators, and a filter expression.
- [Filter Expressions](#) combine fields, operators, and **and** / **or** / **not**.
- [Filter Lists](#) are named value lists for **IN** / **NOT_IN**.

Formatting

A **format string** is text with fields, for example `{RECEIVED|%F} {ORIGINATOR_NAME}: {MESSAGE}`.

- **Field Modifiers** cut, change case, extract, or look up a value.
- **Date/Time Modifiers** format `RECEIVED` timestamps.
- **Escape Modifiers** make a value safe for SQL, CSV, HTML, JSON, URLs, command lines, and file names.
- **Field Dictionaries** are lookup tables that replace a field value with text, for example an explanation of a message ID.

Related Topics

- **Syslog Originators** — choose the parser for each originator in its **Parser** property
- **Viewing Messages**

Formatting

A **format string** is text with fields in braces. For each message, Syslog Watcher replaces every field with its value. Format strings are used in view columns, feature templates, email subjects and bodies, file and folder names, HTTP requests, and report templates. The fields of a **filter expression** are format strings too.

Example:

```
{RECEIVED_S|%F %T} {ORIGINATOR_NAME}: {MESSAGE}
```

For the **example message** this prints:

```
2026-10-13 09:42:17 Edge firewall: Failed password for root from 203.0.113.45 port 51514 ssh2
```



An unknown field prints as empty text, with no error, so a misspelled field name goes unnoticed.

Text with Fields Editor

Click ✧ **Editor...** next to a format string setting to open it in a larger window.

The screenshot shows a window titled "Editor: Body" with a close button in the top right. Below the title bar, there's a label "Text with fields:" and a button "Insert Standard Field" with a dropdown arrow. The main area is a text editor containing the following text:

```
{RECEIVED|%F %T} {ORIGINATOR_NAME|UPPER} ({ORIGINATOR_ID})
{SEVERITY}: {MSGID} {MSGID|FD:asa_messages}
Source: {MESSAGE|r/from outside:([0-9.]+)/}
Rule: {MESSAGE|r/access-group "([^"]+)/}
Interface: {APPNAME|?n/a}
{MESSAGE|}
```

Below the text editor is a larger empty text area with the placeholder text: "Use data fields extracted from a message. For more information, refer to the user manual." At the bottom of the window, there are three buttons: a help button with a question mark, an "Apply" button with a checkmark, and a "Cancel" button with an 'X'.

Text with fields editor

- **Text with fields:** — the format string.
- **Insert Standard Field** — inserts a field at the cursor.

Related Topics

- [Message Fields](#)
- [Field Modifiers](#)
- [Filter Expressions](#)

Message Fields

This page lists the built-in fields for [format strings](#) and filter expressions. Parser fields (such as [TIMESTAMP](#) and [HOSTNAME](#)) come from the originator's [syslog parser](#). [Data Fields](#) in a feature, view layout, parser, or report template add more fields from the message body.

Example

The originator [192.0.2.10](#), named **Edge firewall**, sends this RFC 5424 message:

```
<165>1 2026-10-13T16:42:17.123Z fw01.example.com sshd 2817 AUTH - Failed password for
root from 203.0.113.45 port 51514 ssh2
```

Syslog storage receives it at 09:42:17.250311 server time (UTC-7). With the **Standard IETF/BSD format** parser, the fields are:

Field	Value
RECEIVED	2026-10-13T09:42:17.250311-07:00
RECEIVED_UTC_S	2026-10-13T16:42:17Z
ORIGINATOR_ID	192.0.2.10
ORIGINATOR_NAME	Edge firewall
SEVERITY / SEVERITY_NUM	Notice / 5
FACILITY / FACILITY_NUM	local4 / 20
PRIORITY	165 (20 × 8 + 5)
TIMESTAMP	2026-10-13T16:42:17.123Z, from the sender's clock
HOSTNAME	fw01.example.com, from the message, not the network address
APPNAME / PROCID / MSGID	sshd / 2817 / AUTH
RAW_MESSAGE	1 2026-10-13T16:42:17.123Z fw01.example.com sshd 2817 AUTH - Failed password for root from 203.0.113.45 port 51514 ssh2
MESSAGE	Failed password for root from 203.0.113.45 port 51514 ssh2
PARSER	Standard IETF/BSD format

RECEIVED

The time syslog storage received the message, in the [server time zone](#). It does not depend on the originator's clock. For UTC, use [RECEIVED_UTC](#).

Without a [date/time modifier](#), the value is an RFC 3339 timestamp, as in the examples below. It is also a valid RFC 5424 syslog [TIMESTAMP](#), so it can be used as is when building a syslog message.



Syslog Watcher 6 printed the server time zone offset without a colon ([-0700](#)); version 7 prints [-07:00](#). If a database, script, or other receiver parses [{RECEIVED}](#), [{RECEIVED_S}](#), or [{RECEIVED_MS}](#) without a date/time modifier, check that it accepts the new form. For the old form, use [{RECEIVED|%FT%T%Z}](#).

Field	Description	Example
RECEIVED	Microseconds, server time zone.	2026-10-13T09:42:17.250311-07:00
RECEIVED_UTC	Microseconds, UTC.	2026-10-13T16:42:17.250311Z
RECEIVED_S	Rounded to seconds, server time zone.	2026-10-13T09:42:17-07:00
RECEIVED_MS	Rounded to milliseconds, server time zone.	2026-10-13T09:42:17.250-07:00
RECEIVED_UTC_S	Rounded to seconds, UTC.	2026-10-13T16:42:17Z
RECEIVED_UTC_MS	Rounded to milliseconds, UTC.	2026-10-13T16:42:17.250Z

ORIGINATOR

Field	Description
ORIGINATOR_ID	Originator ID ; in simple cases, the IP address of the sender.
ORIGINATOR_NAME	Originator name.

SEVERITY

Field	Description
SEVERITY	Severity name (for example Emergency). Names can be customized .
SEVERITY_NUM	Severity as a number (0–7).

FACILITY

Field	Description
FACILITY	Facility name (for example kernel). Names can be customized .
FACILITY_NUM	Facility as a number (0–23).

PRIORITY

The syslog priority number: $FACILITY_NUM * 8 + SEVERITY_NUM$. Use it to build the **<PRI>** prefix when forwarding.

RAW_MESSAGE

The message as received, without the **<PRI>** priority prefix.



To forward a syslog message in the same form as it arrived, use **<{PRIORITY}>{RAW_MESSAGE}**.

MESSAGE

The message body: the text that remains after the parser sections.

PARSER

Name of the syslog parser used for the message.

Parser Fields

The originator's syslog parser fills these fields from the message header. A field is empty when the message has no such part or the parser does not read it.

Field	Description
TIMESTAMP	Timestamp from the syslog header (not RECEIVED).
HOSTNAME	Hostname from the syslog header.
APPNAME	Application name (RFC 5424) or tag (RFC 3164), when present.
PROCID	Process ID from the header, when present.
MSGID	Message ID from the header, when present.

Parser sections can add more fields, for example CEF keys, **name=value** pairs, CSV values **001**, **002**, ..., or RFC 5424 structured data as **SDID:param**. See [Message Sections](#).

All Extracted Fields

`{*|...}` repeats a template once per extracted field (sorted by name). Inside that template, `FIELD_NAME` and `FIELD_VALUE` refer to the current field.

Example:

```
{*|{FIELD_NAME}={FIELD_VALUE}; }
```

A prefix before `*` limits the list to fields whose names start with it, for example the fields of one [field collection](#):

```
{pa.*|{FIELD_NAME}={FIELD_VALUE}; }
```

JSON

To print the fields as a JSON object, begin with a fixed member, then put the comma before each repeated member. This avoids a trailing comma. `{{` and `}}` print the object's braces, and `EscJSON` makes names and values safe inside JSON strings:

```
{{"RECEIVED":"{RECEIVED_UTC}"{*|,"{FIELD_NAME|EscJSON}":"{FIELD_VALUE|EscJSON}"}, "MESSAGE":"{MESSAGE|EscJSON}"}}
```

For the [example message](#) this prints:

```
{"RECEIVED":"2026-10-13T16:42:17.250311Z","APPNAME":"sshd","HOSTNAME":"fw01.example.com","MSGID":"AUTH","PROCID":"2817","TIMESTAMP":"2026-10-13T16:42:17.123Z","MESSAGE":"Failed password for root from 203.0.113.45 port 51514 ssh2"}
```

All values are JSON strings.

Related Topics

- [Field Extraction](#) — extra fields from the message body
- [Field Modifiers](#)
- [Date/Time Modifiers](#)
- [Escape Modifiers](#)

Field Modifiers

Modifiers transform a field value in a format string: `{FIELD|modifier}`. The fields of a [filter expression](#) are format strings too, so modifiers work there as well. Separate several modifiers with `|`, in the order they should run. An unknown modifier is ignored.

Put **escape modifiers** **last**, after all other modifiers: `{MESSAGE|70|EscCMD}`.

RECEIVED fields take only a date/time format (`%Y`, `%F`, ...), not the modifiers on this page; see [Date/Time Modifiers](#).

Modifiers at a Glance

Modifier	Goal
N	First N bytes
#N	Last N bytes
N#	From byte offset N to the end
N#M	M bytes from offset N
UPPER or lower	Letter case
?text	Replacement when the field is empty
r/pattern/	Extract with a regular expression
FD:name	Look up text in a Field Dictionary
FDX:name	Look up a format string in a Field Dictionary
Esc...	Safe embedding in SQL, CSV, JSON, a URL, etc.

Length Limit

To shorten a value, add a number: `{MESSAGE|80}` keeps the first 80 bytes. The limit counts bytes, not characters.

If `{MESSAGE}` is **Abcdef**, `{MESSAGE|3}` is **Abc**.



With non-ASCII text, a limit can cut a character in the middle.

Use a limit to fit a value into a fixed-size place, such as an email subject or a database column. In a filter expression, it also speeds up a search when the text you look for is near the start of the message.

`{MESSAGE} CONTAINS "keyword"`

`{MESSAGE|50} CONTAINS "keyword"` (scans only the first 50 bytes)

Substring

A modifier with **#** takes part of the value. Offsets count **bytes** and start at 0.

Form	Result
#N	Last N bytes.
N#	From offset N to the end.
N#M	M bytes starting at offset N.

Form	Result
#0 or N#0	Empty.

If {MESSAGE} is **Abcdef**:

{MESSAGE| #3} is **def**.

{MESSAGE| 2#} is **cdef**.

{MESSAGE| 1#2} is **bc**.

Without #, a number is a length limit, not a substring: {MESSAGE| 3} is **Abc**.



A substring has the same uses as a [length limit](#): fitting a value into a fixed-size place, or searching only part of the message in a filter. It also counts bytes, so with non-ASCII text it can cut a character in the middle.

UPPER / lower

UPPER and lower change letter case.

If {MESSAGE} is **Abc**, {MESSAGE| UPPER} is **ABC**.

If {MESSAGE} is **Abc**, {MESSAGE| lower} is **abc**.

Use either modifier for a case-insensitive filter comparison: {MESSAGE| lower} CONTAINS "login" matches **login**, **Login**, and **LOGIN**.

Blank Field Filler

A modifier that starts with ? supplies replacement text when the field is empty. ? with no text after it is ignored.

If {MESSAGE} is **Abc**, {MESSAGE| ?Blank} is **Abc**.

If {MESSAGE} is empty, {MESSAGE| ?Blank} is **Blank**.

RFC 5424 uses - for an empty header field, so {PROCID| ?-} is a typical use.

Regular Expression

The modifier r/ *pattern* / transforms the value with a regular expression. The result is the text of all capturing groups joined together; it is empty when the pattern does not match or has no groups. An invalid pattern is ignored; it does not affect the rest of the format string.

If {FIELD} is **AB-123-CD**, {FIELD| r/-([0-9]+)-/} is **123**.

For better performance, search only part of the message by putting a length limit or substring first: {MESSAGE| 32| r/%ASA-\d+-(\d+)/}.

Field Dictionary

FD: *name* and **FDX:** *name* look up the value in a field dictionary; see [Use a Dictionary](#).



KB: and **KBX:** (from Syslog Watcher 6) work the same as **FD:** and **FDX:**.

Related Topics

- [Message Fields](#)
- [Date/Time Modifiers](#)
- [Escape Modifiers](#)
- [Filter Expressions](#)

Date/Time Modifiers

These specifiers format **RECEIVED** (server time zone) and **RECEIVED_UTC** (UTC), including the **_S** and **_MS** variants.

Everything after the **|** is the format, so it can mix text and specifiers: **{RECEIVED|%F at %T}**. **RECEIVED** fields take only this format; other **modifiers** do not apply to them.

In the examples below, **{RECEIVED}** is **2023-04-01T09:20:01.000000-07:00**.

Date Format

Spec	Description
%y	Last two digits of the year, 00–99.
%Y	Year, for example 2023.
%b	Abbreviated month name.
%B	Full month name.
%m	Month, 01–12.
%d	Day of the month, 01–31.
%e	Day of the month, 1–31, padded with a space.
%D	Equivalent to %m/%d/%y .
%F	Equivalent to %Y-%m-%d .

{RECEIVED|%B %e, %Y} prints **April 1, 2023**

{RECEIVED|%F} prints **2023-04-01**

Weekday Format

Spec	Description
%a	Abbreviated weekday name.
%A	Full weekday name.
%u	Weekday, 1–7; Monday is 1.
%w	Weekday, 0–6; Sunday is 0.

`{RECEIVED|%A}` prints `Saturday`

Time Format

Spec	Description
<code>%H</code>	Hour, 00–23.
<code>%I</code>	Hour, 01–12.
<code>%p</code>	Locale equivalent of AM/PM for a 12-hour clock.
<code>%M</code>	Minute, 00–59.
<code>%S</code>	Second, 00–59, followed by the fraction when the timestamp has one.
<code>%T</code>	Equivalent to <code>%H:%M:%S</code> .

`{RECEIVED|%I:%M:%S %p}` prints `09:20:01.000000 AM`

`{RECEIVED_S|%I:%M:%S %p}` prints `09:20:01 AM`

Time Zone Format

Spec	Description
<code>%Z</code>	Time zone abbreviation.
<code>%z</code>	Offset from UTC, for example <code>-0430</code> (4 hours 30 minutes behind UTC). <code>+0000</code> if the offset is zero.
<code>%Ez</code>	Same as <code>%z</code> with a colon between hours and minutes (for example <code>-04:30</code>).

Miscellaneous

Spec	Description
<code>%Q</code>	The time as a number of microseconds, for comparing times in SQL. With <code>RECEIVED_UTC</code> , it is the UNIX time: microseconds since 1 January 1970 00:00:00 UTC. With <code>RECEIVED</code> , it is the server time counted the same way, in whole seconds; it matches <code>{FROM %Q}</code> and <code>{TO %Q}</code> in report templates . Use <code>%Q</code> on its own, with no other text.
<code>%j</code>	Day of the year, 001–366.
<code>%U</code>	Week of the year, 00–53. Weeks start on Sunday; days before the first Sunday are week 00.
<code>%W</code>	Week of the year, 00–53. Weeks start on Monday; days before the first Monday are week 00.
<code>%x</code>	Locale date representation.
<code>%c</code>	Locale date and time (rounded to seconds).

`{RECEIVED_UTC|%Q}` prints `1680366001000000`

`{RECEIVED|%Q}` prints `1680340801000000`

`{RECEIVED|%j}` prints `091`

Related Topics

- [RECEIVED fields](#)
- [Export to Files](#) — daily file names

Escape Modifiers

Escape modifiers prepare a field value for a specific output format. Apply them to untrusted syslog text before embedding it in SQL, CSV, HTML, JSON, a URL, a command line, or a file name.

When several modifiers are chained, put the escape **last**: `{MESSAGE|70|EscCMD}`.

Modifiers at a Glance

Modifier	Destination
EscSQL	SQL string literal (MySQL style: backslash is special)
EscSQLANSI	SQL string literal (ANSI: SQL Server, SQLite)
EscCSV	CSV field, with the quotes in the template
EscCSV2	Whole CSV field, safe to open in Excel
EscHTML	HTML text
EscJSON	JSON string
EscDBLQ	C-style <code>"..."</code> string
EscURL	URL path or query
EscCMD	Windows command-line argument (<code>CreateProcess</code>)
EscFNAME	File or folder name

EscSQL

Prepares a value to be enclosed in single quotes: doubles each `'`, writes `\\` for `\`, and writes `\0` for a NUL byte. The modifier does not add the surrounding quotes.

If `{MESSAGE}` is `C:\logs 'x'`, `{MESSAGE|EscSQL}` is `C:\\logs ''x''`.

See [Export to DB \(ODBC\)](#) and [Report Templates](#).

EscSQLANSI

Prepares a value to be enclosed in single quotes for databases that follow ANSI SQL, such as SQL Server and SQLite: doubles each `'` and removes NUL bytes. Backslashes are left as they are. The modifier does not add the surrounding quotes.

If `{MESSAGE}` is `C:\logs 'x'`, `{MESSAGE|EscSQLANSI}` is `C:\logs ''x''`.

EscCSV

Doubles each `"`. The modifier does not add the quotes; put them in the template.

If {MESSAGE} is **abc "xyz"**, {MESSAGE|EscCSV} is **abc ""xyz""**.

Typical CSV line: "{ORIGINATOR_ID|EscCSV}", "{MESSAGE|EscCSV}".

See [Export to Files](#).

EscCSV2

Turns a value into a complete CSV field that is safe even when it contains commas, quotes, or line breaks, or starts like a spreadsheet formula.

- If the value starts with **=**, **+**, **-**, or **@**, a tab is prepended so Excel and similar tools treat the cell as text.
- If the value contains **"**, **,**, **CR**, or **LF**, the result is wrapped in **"** and each **"** inside is doubled.

Do not put quotes around {MESSAGE|EscCSV2} in the template; the modifier adds them when needed.

If {MESSAGE} is **a,b**, {MESSAGE|EscCSV2} is **"a,b"**.

If {MESSAGE} is **abc "xyz"**, {MESSAGE|EscCSV2} is **"abc ""xyz"""**.

If {MESSAGE} is **=1+1**, {MESSAGE|EscCSV2} is a tab followed by **=1+1**.

EscHTML

Prepares a value for HTML text or an HTML attribute value. Use it when a template builds HTML, for example an HTML file written by [Export to Files](#) or the body of an [HTTP request](#) to a service that expects HTML.

Character	Replaced with
&	&amp;
<	&lt;
>	&gt;
"	&quot;
'	&#39;

If {MESSAGE} is **"Tom" & 'Jerry'**, {MESSAGE|EscHTML} is **"Tom" 'Jerry'**.



In [report templates](#), do not use **EscHTML**: report output escapes values itself.

EscJSON

Prepares a value for a JSON string. The modifier does not add the quotes; put {FIELD|EscJSON} inside **"..."** in the template.

Character	Replaced with
\	\\
"	\"
LF (\n)	\n

Character	Replaced with
CR (\r)	\r
TAB (\t)	\t
BACKSPACE (\b)	\b
FORM FEED (\f)	\f
Other control bytes (below 0x20)	\u00XX

If {MESSAGE} is `\abc "xyz"`, {MESSAGE|EscJSON} is `\\abc \"xyz\"`.

See [Send HTTP Requests](#) and [Export to Files](#).

EscDBLQ

Inserts `\` before each `"` and `\`, for a C-style quoted string. Newlines and other control bytes are **not** escaped. For JSON, use `EscJSON`.

If {MESSAGE} is `abc "x\y"`, {MESSAGE|EscDBLQ} is `abc \"x\\y\"`.

EscURL

Percent-encodes the value for a URL path or query (RFC 3986). Letters, digits, and `- _ . ~` stay as is; every other byte becomes `%HH`.

See [Send HTTP Requests](#).

EscCMD

Prepares a value as one argument of a Windows command line passed to `CreateProcess`. A value without spaces, tabs, line feeds, vertical tabs, or `"` is left as it is. Otherwise the value is wrapped in `"`, each `"` inside becomes `\`, and backslashes right before a `"` or at the end are doubled.

Do not wrap {FIELD|EscCMD} in extra quotes in the template.

If {MESSAGE} is `hello`, {MESSAGE|EscCMD} is `hello`.

If {MESSAGE} is `hello world`, {MESSAGE|EscCMD} is `"hello world"`.

If {MESSAGE} is `say "hi"`, {MESSAGE|EscCMD} is `"say \"hi\""`.

See [Execute Program/Script](#).

EscFNAME

Replaces characters that Windows does not allow in a file or folder name with `_`: `" < > ? * | \ / :`, bytes below 0x20, and DEL (0x7F).

See [Export to Files](#).

Related Topics

- [Message Fields](#)
- [Field Modifiers](#)

- [Export to Files](#)
- [Export to DB \(ODBC\)](#)
- [Send HTTP Requests](#)
- [Execute Program/Script](#)

Field Dictionaries

A **field dictionary** is a lookup table of keywords and their replacement text. The **FD:** and **FDX:** **modifiers** replace a field value with the text for that keyword.

Typical uses:

- ▶ Add the vendor's explanation and recommended action to a message ID, in an email or in the view details panel.
- ▶ Translate codes to readable names, for example protocol 6 → TCP or port 443 → HTTPS.
- ▶ Explain Windows event IDs, for example 4625 → An account failed to log on.
- ▶ Show where an originator is and who owns it: {ORIGINATOR_ID|FD:sites} → Building 2, rack B3 (Network team).
- ▶ Group message IDs into categories and filter by category: {MSGID|FD:asa_categories} = "VPN".
- ▶ Convert a severity to the priority of a ticketing or monitoring system: {SEVERITY_NUM|FD:ticket_priority} → P1.
- ▶ Sort exported files into a folder per site: {ORIGINATOR_ID|FD:site_codes} in the **Subfolders template** of [Export to Files](#).
- ▶ With **FDX:**, use a different text layout for each message type: {MSGID|FDX:asa_layouts}.

Field Dictionaries Window

In the **Storage** section of the main toolbar, click  **More** → **Field Dictionaries...**

The list is grouped by **From: Installation** (read-only, shipped with the product) and **Syslog Storage**.

The installation includes **CiscoASA**, with HTML explanations and recommended actions for Cisco ASA message IDs (ASA-1-101001, ...).

Field Dictionary

New Field Dictionary

×

Name:

CiscoASA

Description:

Compiled from Cisco's public Secure Firewall ASA syslog message documentation. It is a compact, unofficial extract of explanations and recommended actions for reference only. Always check Cisco's official documentation for the current wording, severity, and guidance.

List of #keywords, each followed by replacement text:

#ASA-1-101001

<p>Explanation The failover cable is present and

#ASA-1-101002

<p>Explanation The failover cable is present, but

<p>Recommended Action Replace the failover cable.

#ASA-1-101003

<p>Explanation Failover mode is enabled, but the

<p>Recommended Action Connect the failover cable

#ASA-1-101004

<p>Explanation Failover mode is enabled, but the

<p>Recommended Action Connect the failover cable

#ASA-1-101005

Index [2330]:

ASA-1-101001

ASA-1-101002

ASA-1-101003

ASA-1-101004

ASA-1-101005

ASA-1-103001

ASA-1-103002

ASA-1-103003

ASA-1-103004

ASA-1-103005

ASA-1-103006

ASA-1-103007

ASA-1-103008

ASA-1-104001

ASA-1-104002

ASA-1-104003

↓ Sort Alphabetically

?

Import / Export ▼

✓ Create

✕ Cancel

Field dictionary window

Setting	Description
Name:	Required, unique. This is the name after FD: or FDX: .
Description:	Optional.
List of #keywords, each followed by replacement text:	Each keyword on its own line starting with # , followed by its replacement text (one or more lines). Empty lines can be added for readability. A # with no keyword sets the default text, used when the keyword is not found.

Example:

```
#6
TCP

#17
UDP

#
other
```

The **Index** list shows the keywords and the default as **[DEFAULT]**. Click a keyword to jump to its entry. **Sort Alphabetically** puts the entries in keyword order.

Import / Export reads or writes a field dictionary file (**.fd**).

Use a Dictionary

{FIELD|FD:name} looks up the value of **FIELD** and prints the replacement text. If the keyword is missing, the default text is printed (empty when there is no default).

{FIELD|FDX:name} does the same, but treats the replacement text as a format string, so it can contain other fields.

Examples:

```
{MSGID|FD:CiscoASA}
{proto|FD:ip_protocols}
```

Other modifiers can come before the lookup, for example **{MSGID|UPPER|FD:codes}**.

Related Topics

- [Field Modifiers — Field Dictionary](#)
- [Field Collections](#)
- [View Layouts](#)

Filtering

The **Filter** section selects the stored messages that a feature, report, or view tab uses, by severity, originators, and a filter expression. It works on messages already in syslog storage; to drop messages before they are stored, use the [Incoming Filter](#).

Filter/Search		
> Severity level	all severity levels	
Originators	Group: Firewalls	
Filter expression	{MESSAGE lower} CONTAINS "deny"	

Filter/Search section of a view/search preset

Severity level	Severities from Minimum to Maximum , both included ((0) Emergency ... (7) Debug). The full range is shown as all severity levels .
Originators	ALL ORIGINATORS , <select originators> (a selected set), or Group: followed by an originator group name.
Filter expression	Optional filter expression . When it is blank, the setting shows ALL MESSAGES and passes every message that matches severity and originators.



Narrow by severity and originators first. They use storage indexes, so they are much faster than an expression.

Related Topics

- [Filter Expressions](#)
- [Filter Lists](#)
- [Incoming Filter](#)

Filter Expressions

A filter expression selects messages using [message fields](#), comparison operators, **and** / **or** / **not**, and parentheses.

An empty expression matches every message that already passed severity and originators.



Narrow by **severity** and **originators** on the [message filter](#) first. They use storage indexes, so they are much faster than an expression.

Syntax

A comparison is a field in braces, an operator, and a value (quoted text or an unquoted number).

```
{APPNAME} = "sshd"
```

Field names can include [modifiers](#):

```
{MESSAGE|lower} CONTAINS "blocked"
```

Put text values in double quotes. To include a " in the value, double it:

```
{MESSAGE} CONTAINS "begin ""quoted part"" end"
```

Write operators in uppercase: **CONTAINS**, not **contains**. Text comparisons are case-sensitive. **{MESSAGE|lower}** (or **UPPER**) makes a case-insensitive comparison; write the value in the same case:

```
{MESSAGE} CONTAINS "error"      matches "error" only
{MESSAGE|lower} CONTAINS "error" matches "error", "Error", and "ERROR"
```

and / **or** / **not**

Logic keywords are **lowercase**: **and**, **or**, **not**. **AND**, **OR**, and **NOT** are invalid.

Use parentheses to group conditions, especially when an expression mixes **and** and **or**.

```
{APPNAME} = "sshd" and {MESSAGE} CONTAINS "Failed password"
{APPNAME} = "sshd" or {APPNAME} = "sudo"
not {MESSAGE} CONTAINS "test"
({APPNAME} = "sshd" or {APPNAME} = "sudo") and {MESSAGE} CONTAINS "root"
```

Operators

Operator	Meaning
<code>= !=</code>	Equal / not equal (text).
<code>< <= > >=</code>	Quoted values compare as text, character by character, so "10" is less than "9". An unquoted number compares as an integer.
<code>CONTAINS DOES_NOT_CONTAIN</code>	Substring (case-sensitive).
<code>STARTS_WITH ENDS_WITH</code>	Prefix / suffix (case-sensitive).
<code>IN NOT_IN</code>	The value is / is not an item of a filter list .
<code>RE_MATCHES RE_MATCHES_I</code>	The whole field matches a regular expression (case-sensitive / ignore case).
<code>RE_CONTAINS RE_CONTAINS_I</code>	Part of the field matches a regular expression (case-sensitive / ignore case).

Integer Comparison

With an unquoted number (digits, optionally a leading minus), `< <= > >=` compare as integers. A field value that does not start with a number counts as 0.

```
{MSGID} > 404
```

Quoted digits compare as text, so `{MSGID} > "404"` is a text comparison.

Filter Lists

`IN` is true when the value equals an item of the named list exactly; `NOT_IN` is the opposite.

```
{APPNAME} IN "allowed_apps"
{MSGID|lower} NOT_IN "known_errors"
```

See [Filter Lists](#).

Regular Expressions

Patterns use Perl syntax. `RE_MATCHES` requires the entire field to match. `RE_CONTAINS` succeeds when the pattern occurs anywhere in the field. The `_I` forms ignore case.

Messages that contain an email address:

```
{MESSAGE} RE_CONTAINS ".+\\@.+.\\.\\.+"
```

Instead of the **_I** operators, you can start the pattern with **(?i)**. **(?i:...)** makes only that part case-insensitive:

```
{MESSAGE} RE_CONTAINS "user (?i:admin|root)"
```

Limits

An expression can be up to 64 KB long and nested up to 256 levels deep (**and** / **or** / **not** / parentheses). A longer or deeper expression is rejected.

Filter Expression Editor

Click ▼ **Editor...** next to a filter expression setting to open it in a larger window.

The screenshot shows a dialog box titled "Editor: Filter expression" with a close button (X) in the top right corner. Inside the dialog, there is a section labeled "Filter expression:" with three dropdown menus: "Standard Fields", "Operators", and "Logic". Below these is a large text area containing the filter expression: `{MSGID} = "ASA-4-106023" or {MSGID} = "ASA-2-106001" and {MESSAGE|lower} CONTAINS "outside"`. Below the text area is a section titled "SYNTAX OK" which contains a list of examples for filter expressions: `{FIELD1}="foo" and {FIELD2}!="bar"`, `{FIELD}<=50 or {FIELD}=100`, `{FIELD} CONTAINS "foobar"`, `{FIELD} STARTS_WITH "foo"`, and `{FIELD} IN "List"`. It also includes the text "See the reference manual for more examples." At the bottom of the dialog, there is a question mark icon on the left, and "Apply" and "Cancel" buttons on the right.

Filter expression editor

- **Filter expression:** — where you type the expression.
- **Standard Fields, Operators, Logic** — drop-downs that insert a field, an operator, or **and** / **or** / **not** at the cursor.
- Result line — **SYNTAX OK**, or **INVALID SYNTAX** with the reason, updated as you type.
- Bottom pane — syntax examples.

Related Topics

- [Filtering](#)
- [Filter Lists](#)
- [Message Fields](#)
- [Field Modifiers](#)

Filter Lists

A filter list is a named set of values, one per line. With **IN** / **NOT_IN**, a [filter expression](#) checks a field against all items of a list at once, instead of a long chain of **or**.

Filters can only use lists in syslog storage. To use a list shipped with the product (**Installation**), duplicate it first.

Create a List

1. In the **Storage** section of the main toolbar, click **☰ More** → **Filter Lists...**
2. Click **Create New**, or select a list and click **Duplicate**.
3. Enter a **Name**: and the items (see [Filter List](#)).
4. Click **Create**.

Filter List

Setting	Description
Name:	Required, unique. Filter expressions refer to the list by this name: <code>{APPNAME} IN "allowed_apps"</code> .
Description:	Optional.
Filter list items, one per line:	One value per line. Empty lines are skipped. Lines are not trimmed: spaces are part of the value.

Example items:

```
LINK-3-UPDOWN
LINK-3-LINK_FAULT
LINK-3-TOOSMALL
```

IN / NOT_IN

IN is true when the field value, after its modifiers, exactly equals an item of the named list.

```
{APPNAME} IN "allowed_apps"
{ORIGINATOR_ID} IN "block_list"
{MSGID|lower} IN "known_errors"
```

NOT_IN is the inverse: `{MSGID} NOT_IN "known_errors"` is the same as `not {MSGID} IN "known_errors"`.

If no list has that name, **IN** is always false and **NOT_IN** is always true.

See [Filter Expressions](#) for operators.

Field Extraction

The **Data Fields** section takes extra fields out of the message text (`{MESSAGE}`). Use them like any other field, in [filter expressions](#) and [format strings](#).

▼ Data Fields (Optional) ▼	
Regex for extracting fields	Deny (?<PROTO>\w+) src (?<SRC_IF>[^:]+):(?<SRC_IP>[\c
▼ Fields (3) Add Field ▼	
> {ASA_ID}	{MSGID r/ASA-\d-(\d+)/}
> {ASA_HELP}	{MSGID FD:CiscoASA}
▼ {CONNECTION}	{PROTO} {SRC_IP}:{SRC_PORT} → {DST_IP}:{DST_PORT}
Field name	CONNECTION
Field format	{PROTO} {SRC_IP}:{SRC_PORT} → {DST_IP}:{DST_PORT}
▼ Field Collections (1) Add Collection ▼	
▼ {pa._}	{MESSAGE} → PaloAlto[{MSGID}]
Collection access name	pa
Field collection	PaloAlto
Keyword selector	{004}

Data Fields section of a view layout

- | | |
|------------------------------------|---|
| Regex for extracting fields | One regular expression with named groups. |
| Fields | Named format strings. |
| Field Collections | Stored rule sets that pick a rule per message type. |

Example

Network equipment can log each command run in the configuration console:

```
%ASA-7-111009: User 'enable_15' executed cmd: show logging mess 106100
```

The goal is two extra fields: `{USER}` for the username and `{CMD}` for the command. Below are two ways to get them, followed by a comparison.

Regex for extracting fields

One regular expression can capture several fields. Each named group (`?<FIELD_NAME>...`) becomes a field `{FIELD_NAME}`.

For the example line:

```
User '(<USER>[^\']+) ' executed cmd: (<CMD>.+)
```

That gives `{USER} = enable_15` and `{CMD} = show logging mess 106100`.

To test the expression on a sample message, use the [Regular Expression Editor](#).

Fields

Click **Add Field** for each field, then set:

Setting	Description
Field name	The name of the new field, used as <code>{NAME}</code> .
Field format	A format string . It can use any field, including those from the regex and collections.

For the example, each field takes its value from `{MESSAGE}` with a [regular-expression modifier](#):

Field name	Field format
USER	<code>{MESSAGE r/User '([^\']+)'/}</code>
CMD	<code>{MESSAGE r/executed cmd: (.+)/}</code>



For better performance, put a [length limit](#) before the regex: `{MESSAGE|40|r/User '([^\']+)'/}` looks for the username only in the first 40 bytes.

Results and Comparison

Both methods give the same fields for the example message:

Field	Value
<code>{USER}</code>	<code>enable_15</code>
<code>{CMD}</code>	<code>show logging mess 106100</code>

They differ in how they work:

	Regex for extracting fields	Fields
When it runs	For every message, even when none of its fields is used.	Only when a filter or format string uses the field. An unused field costs nothing.
Setup	One regular expression for all fields.	One format string per field.
Value	The captured text as it is.	Any format string: modifiers, field dictionary lookups, or several fields combined.

Use **Regex for extracting fields** for messages with a fixed layout, when most of its values are used.

Use **Fields** for values that are used only sometimes, or to build a value from other fields. Fields can use the regex fields, so the two methods work together.

Field Collections

A [field collection](#) applies a stored set of rules and picks one per message type. See [Use a Collection](#).

Regular Expression Editor

Click * **Regex Editor...** next to **Regex for extracting fields** to open the expression in a larger window and test it on a sample message.

*** Editor: Regular Expression**

Regular expression with named capture groups (?<FIELD_NAME>...):

```
Deny (?<PROTO>\w+) src (?<SRC_IF>[^:]+) : (?<SRC_IP>[\d.]+)/ (?<SRC_PORT>\d+) dst (?<DST_IF>[^:]+) : (?<DST_IP>[\d.]+)/ (?<DST_PORT>\d+) by access-group "(?<ACL>[^\"]+)"
```

(Optional) Part of a syslog message for testing:

```
Deny tcp src outside:203.0.113.45/51514 dst inside:10.1.20.15/443 by access-group "outside_access_in" [0x0, 0x0]
```

```
{ACL}=outside_access_in  
{DST_IF}=inside  
{DST_IP}=10.1.20.15  
{DST_PORT}=443  
{PROTO}=tcp  
{SRC_IF}=outside  
{SRC_IP}=203.0.113.45  
{SRC_PORT}=51514
```

? Apply Cancel

Regular expression editor

- **Regular expression with named capture groups (?<FIELD_NAME>...):** — for example `ip=(?<IP>\S+)`.
- **(Optional) Part of a syslog message for testing:** — paste a message body.
- **Result area** — the extracted fields as `{FIELD_NAME}=value`, or the message **No fields were extracted** or **The regular expression is invalid**.

Related Topics

- [Message Fields](#)
- [Field Modifiers](#)
- [Field Collections](#)
- [Syslog Parsers](#)

Field Collections

Many vendors send only values, without field names, and what each value means depends on the message type. A **field collection** turns those values into named fields.

A collection is a list of **keywords**, each with an extraction rule. For each message, a **keyword selector**, such as `{MSGID}` or the log type in the message, picks the rule.

There are two types:

Type	Each keyword has
RegExp Extractors	A regular expression with named groups (<code>?<NAME>...</code>), applied to <code>{MESSAGE}</code> .
CSV Field Names	A comma-separated list of names for the values <code>001</code> , <code>002</code> , ... produced by the CSV body parser section. An empty name skips that value.

The fields are named `{ACCESS_NAME.FIELD_NAME}`. You set the access name when you add the collection to a **Data Fields** section.

Field Collections Window

In the **Storage** section of the main toolbar, click  **More** → **Field Collections...**

The list is grouped by **From: Installation** (read-only, shipped with the product) and **Syslog Storage**.

The installation includes **PaloAlto**: CSV field names for Palo Alto log types (`AUDIT`, `AUTHENTICATION`, `CONFIG`, `SYSTEM`, `THREAT`, `TRAFFIC`, and more).

Field Collection

New Field Collection

×

Name:

Type:

CSV Field Names

▼

Description:

Maps Palo Alto syslog fields to named fields by log type (THREAT, SYSTEM, etc).

▲

▼

List of #keywords, each followed by comma-separated field names:

#AUDIT

serial_number,generate_time,subtype,,event_id,object,cli

#AUTHENTICATION

,receive_time,serial,type,subtype,,time_generated,vsys,i

#CONFIG

,receive_time,serial,type,subtype,,time_generated,host,v

#CORRELATION

,receive_time,serial,type,subtype,,time_generated,src,src

#DECRYPTION

,receive_time,serial,type,subtype,config_ver,time_genera

app,is_saas_of_app,sanctioned_state_of_app,cluster_name

Index [16]:

AUDIT

AUTHENTICATION

CONFIG

CORRELATION

DECRYPTION

END

GLOBALPROTECT

GTP

HIP-MATCH

IPTAG

SCTP

START

SYSTEM

THREAT

TRAFFIC

USERID

↓ Sort Alphabetically

?

Import / Export ▼

✓ Create

✕ Cancel

Field collection window

Setting	Description
Name:	Required, unique. You choose the collection by this name in the Field collection setting.
Description:	Optional.
Type:	RegExp Extractors or CSV Field Names .
List of #keywords, each followed by ...:	The label ends with a field extractor expression or comma-separated field names , depending on Type :. Each keyword on its own line starting with # , followed by its rule. Empty lines can be added for readability. A # with no keyword sets the default rule, used when no keyword matches.

The **Index** list shows the keywords and the default as **[DEFAULT]**. Click a keyword to jump to its entry. **Sort Alphabetically** puts the entries in keyword order.

Example: RegExp Extractors

```
#EXAMPLE-MSG1
ip=(?<IP>\S+)

#EXAMPLE-MSG2
```

© 2026 EZ5 Systems Ltd.

81

```
IP:(?<IP>\S+)
```

With **Keyword selector** {MSGID}, an EXAMPLE-MSG1 message gets IP from ip=..., and an EXAMPLE-MSG2 message gets it from IP:...

Example: CSV Field Names

A parser with the **Header: IETF/BSD-syslog** and **Body: Comma-Separated Values** sections splits a Palo Alto message into values 001, 002, ... The fourth value, 004, is the log type, such as SYSTEM or TRAFFIC.

```
#SYSTEM
,receive_time,serial,type,subtype,,time_generated,vsys,eventid,object,...
```

With **Keyword selector** {004} and access name pa, a SYSTEM message gets {pa.receive_time}, {pa.serial}, {pa.eventid}, and so on. The built-in **Palo Alto Networks Devices** parser uses the collection this way.

Use a Collection

1. Open the **Data Fields (Optional)** section of a feature, view layout, parser, or report template.
2. Under **Field Collections**, click **Add Collection**.
3. Set:

Setting	Description
Collection access name	Prefix of the field names: {ACCESS_NAME.FIELD_NAME}.
Field collection	The collection to apply.
Keyword selector	Format string that gives the keyword for each message, for example {MSGID} or {004}. When no keyword matches, the collection's default rule is used, if it has one.

To list all fields of one collection, for example in a view layout's details panel, put the access name and a dot before the *:

```
{pa.*|<tr><td>{FIELD_NAME}</td><td>{FIELD_VALUE|EscHTML}</td></tr>}
```

Related Topics

- [Field Extraction](#)
- [Syslog Parsers](#)
- [Field Dictionaries](#)

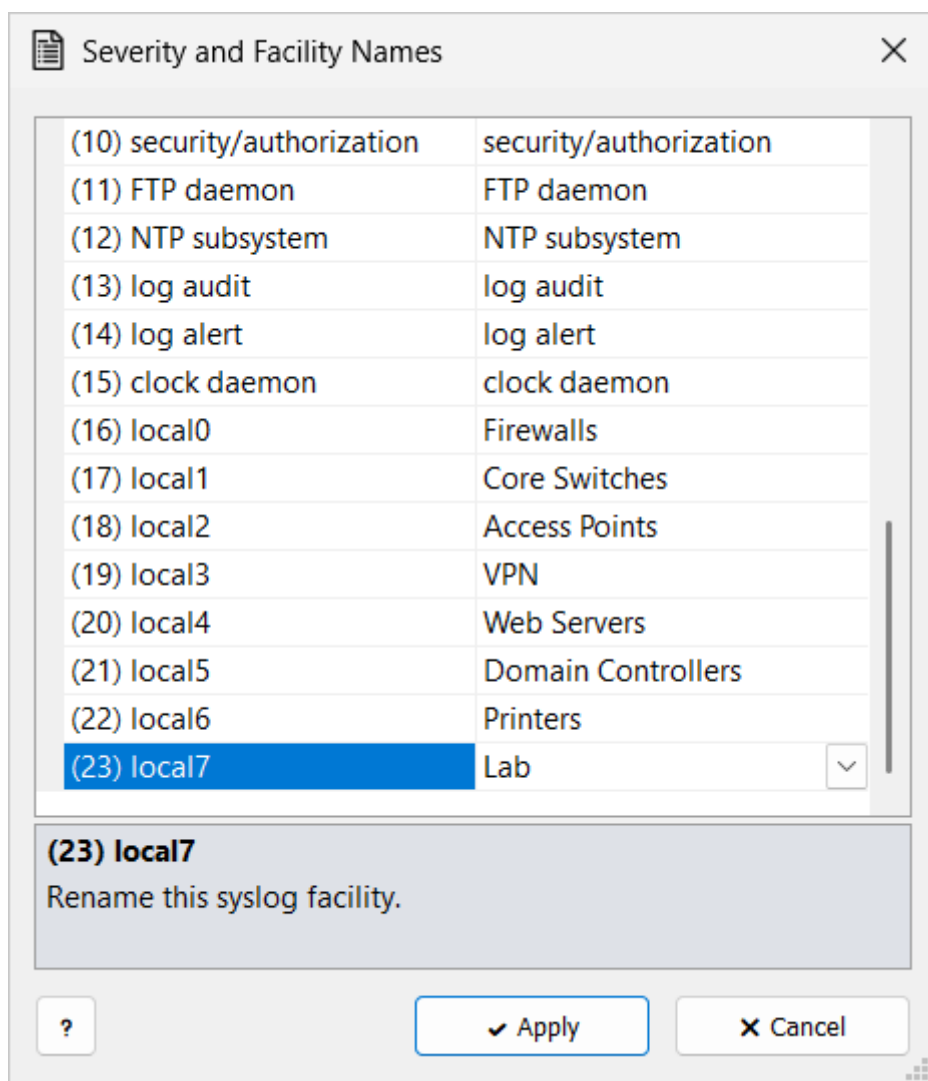
Severity and Facility Names

Syslog severities (0–7) and facilities (0–23) are numbers. Syslog Watcher shows them with names from RFC 5424, such as **Warning** or **local0**. You can rename them to match vendor documentation or your own terms.

Renaming does not change the numbers, so severity ranges in message filters, and filter expressions that use `{SEVERITY_NUM}` or `{FACILITY_NUM}`, keep working.

Change the Names

1. In the **Storage** section of the main toolbar, click **More** → **Severity and Facility Names...**
2. Edit a name under **Severity Level Names** or **Facility Names**. Names cannot be blank.
3. Click **Apply**.



Severity and Facility Names, with local facilities renamed

The names are kept in syslog storage.

Where the Names Appear

- `{SEVERITY}` and `{FACILITY}` in view columns, feature templates, emails, and reports

- Severity lists in filters and on the Server and Storage tabs



A filter expression that compares `{SEVERITY}` or `{FACILITY}` with text stops matching after a rename. Compare `{SEVERITY_NUM}` or `{FACILITY_NUM}` instead.

Default Names

Severity	Name	Facility	Name
0	Emergency	0	kernel
1	Alert	1	user-level
2	Critical	2	mail system
3	Error	3	system daemons
4	Warning	4	security/authorization
5	Notice	5	syslogd
6	Informational	6	line printer subsystem
7	Debug	7	network news subsystem
		8	UUCP subsystem
		9	clock daemon
		10	security/authorization
		11	FTP daemon
		12	NTP subsystem
		13	log audit
		14	log alert
		15	clock daemon
		16–23	local0 ... local7

Related Topics

- [Message Fields](#)
- [Filtering](#)

Syslog Parsers

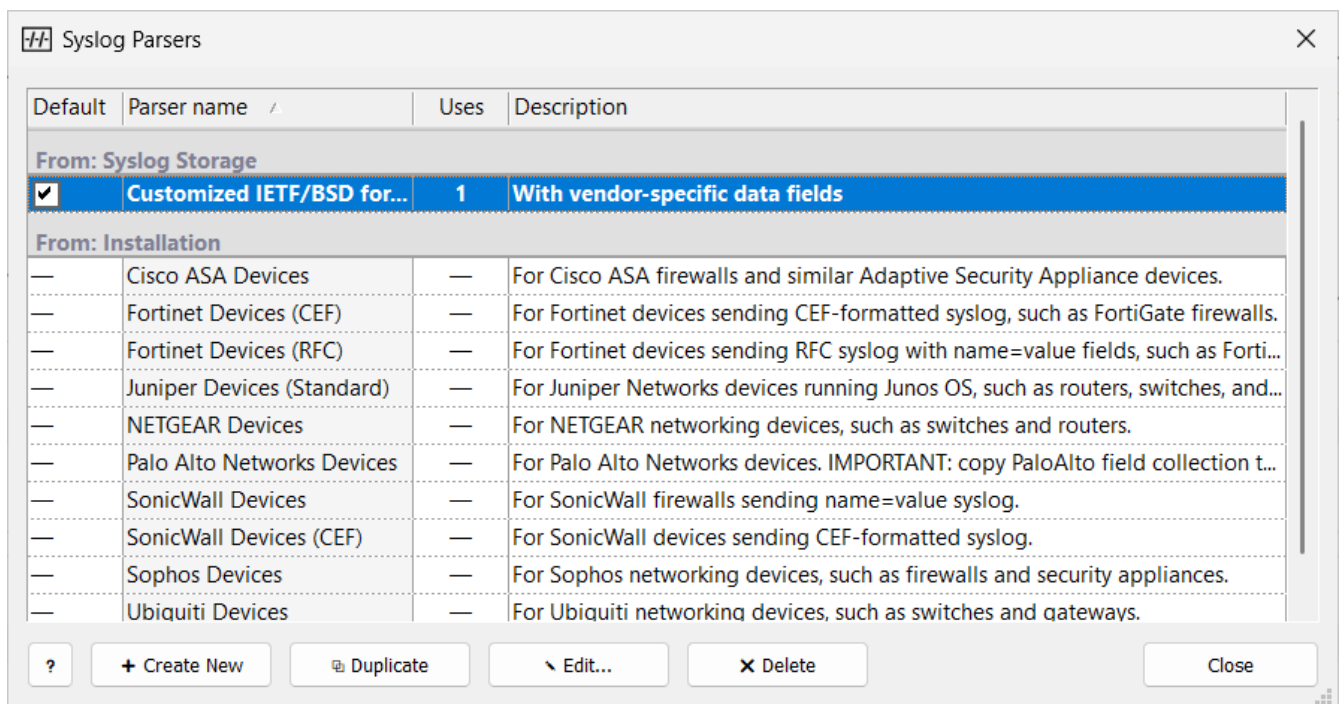
A **syslog parser** breaks a syslog message (one line of text) into fields such as **TIMESTAMP**, **HOSTNAME**, **APPNAME**, and **MSGID**. You can use these fields in **filters**, view columns, and feature templates.

Each **originator** has one parser; new originators get the **default** parser. Messages are parsed when they are read from syslog storage, so a new parser also applies to messages that are already stored.

- [Create or Edit a Parser](#) — the parser window and its message sections
- [Report Incorrect Parsing](#) — send a wrongly parsed message to EZ5

Syslog Parsers Window

In the **Storage** section of the main toolbar, click  **Parsers**.



Syslog Parsers window

The list is grouped by **From: Syslog Storage** and **Installation** (read-only, shipped with the product). Installation parsers cover common vendors, and product updates add more.

To make a syslog storage parser the default for new originators, select its **Default** check box, or right-click it and choose **Set Default Parser**. An installation parser cannot be the default; duplicate it and make the copy the default.

Assign a Parser to an Originator

Select the parser in the **Parser** property of the **originator**. If you select an installation parser, Manager offers to copy it into syslog storage and assigns the copy.

If no parser fits, duplicate the closest one and adjust it (see [Create or Edit a Parser](#)), or [report the message](#) to EZ5.

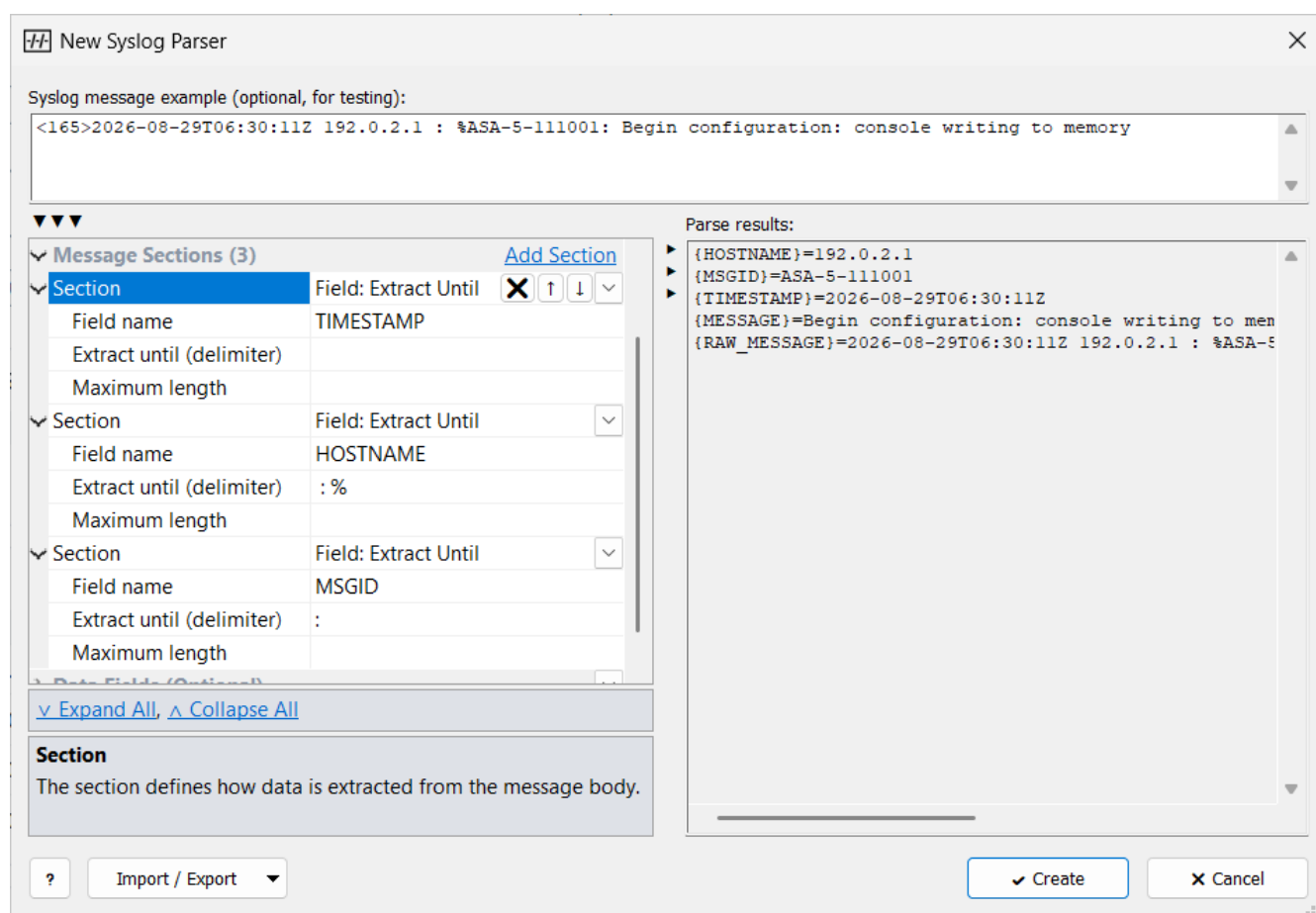
Related Topics

- [Originator Properties](#) — the **Parser** setting
- [Message Fields](#)
- [Field Collections](#)
- [Field Extraction](#)

Create or Edit a Parser

Create or Edit a Parser

1. In the **Storage** section of the main toolbar, click  **Parsers**.
2. Click **Create New**, or select a parser and click **Duplicate** or **Edit...**
3. Enter the **Parser name** and click **Add Section** for each parsing step (see [Message Sections](#)).
4. Paste a message into **Syslog message example (optional, for testing)**; **Parse results:** shows the fields the parser finds.
5. Click **Create** (new parser) or **Apply** (existing parser).
6. Select the parser in the **Parser** property of the [originators](#) that send this format.



New Syslog Parser

Syslog message example (optional, for testing):

```
<165>2026-08-29T06:30:11Z 192.0.2.1 : %ASA-5-111001: Begin configuration: console writing to memory
```

Message Sections (3) [Add Section](#)

Section	Field: Extract Until	Field name
Section	X	TIMESTAMP
Section	HOSTNAME	HOSTNAME
Section	MSGID	MSGID

[Expand All](#) [Collapse All](#)

Section
The section defines how data is extracted from the message body.

Parse results:

```
{HOSTNAME}=192.0.2.1  
{MSGID}=ASA-5-111001  
{TIMESTAMP}=2026-08-29T06:30:11Z  
{MESSAGE}=Begin configuration: console writing to men  
{RAW_MESSAGE}=2026-08-29T06:30:11Z 192.0.2.1 : %ASA-5
```

[?](#) [Import / Export](#) [Create](#) [Cancel](#)

Syslog parser window

General Properties

Parser name (required, unique) and **Description**.

Data Fields (Optional)	Extra fields taken from the message body after the message sections run. See Field Extraction .
Message Sections	The parsing steps, in order.

Message Sections

Click **Add Section** for each step. Sections run from top to bottom; each one takes its part from the start of the remaining text. The text that remains is **{MESSAGE}**.

Most sections take the part they recognize and leave the rest to the next section. **Field: Extract Until** and **Skip: Until Delimiter** stop parsing when the delimiter is not found; the fields found so far are kept.

Section	Effect
Header: IETF/BSD-syslog (RFC5424/RFC3164)	Parses a standard syslog header: TIMESTAMP , HOSTNAME , APPNAME , PROCID , and, for RFC 5424, MSGID and structured data. For RFC 3164, the tag gives APPNAME and the [pid] gives PROCID .
Header: RFC5424:STRUCTURED-DATA	Parses RFC 5424 structured data at the current position. Each parameter becomes a field named SDID:param , for example {origin:ip} . Use it only when the header is parsed by other sections; the IETF/BSD header section already parses structured data.
Field: Legacy Timestamp (RFC3164)	Parses an RFC 3164 timestamp, such as Aug 29 06:30:11 , into TIMESTAMP . A year and milliseconds are included when present, for example Aug 29 06:30:11.123 2026 .
Field: Extract Until	Saves the text up to Extract until (delimiter) in the field named in Field name (for example HOSTNAME or MSGID). Maximum length limits how far to search for the delimiter (0 = no limit); a delimiter beyond it counts as not found, so parsing stops.
Skip: Spaces	Skips spaces at the start of the remaining text.
Skip: Symbols	With one character in Symbols to skip , skips every repetition of that character. With several characters, skips that exact text once, if the remaining text starts with it.
Skip: Until Delimiter	Skips text up to and including Skip until (delimiter) .
Body: Common Event Format (CEF)	Parses a CEF:0 or CEF:1 body: deviceVendor , deviceProduct , deviceVersion , deviceEventClassId , name , agentSeverity , and every extension key (for example src , dst).
Body: Name=value pairs	Parses name=value and name="quoted value" pairs; each name becomes a field.

Section	Effect
Body: Comma-Separated Values (CSV)	Splits the body into values named 001 , 002 , 003 , ... Use a field collection of the CSV Field Names type to give them names.

Related Topics

- [Syslog Parsers](#)
- [Message Fields](#)
- [Field Collections](#)
- [Field Extraction](#)

Report Incorrect Parsing

When a message is parsed wrongly, right-click it in a view tab and choose **Report Incorrect Parsing...**

Setting	Description
Originator description	Required. Vendor, model, and version of the software or hardware that sent the message.
(Optional) What is wrong	What is wrong and what you expected.
(Optional) Contact email	Address for a reply.

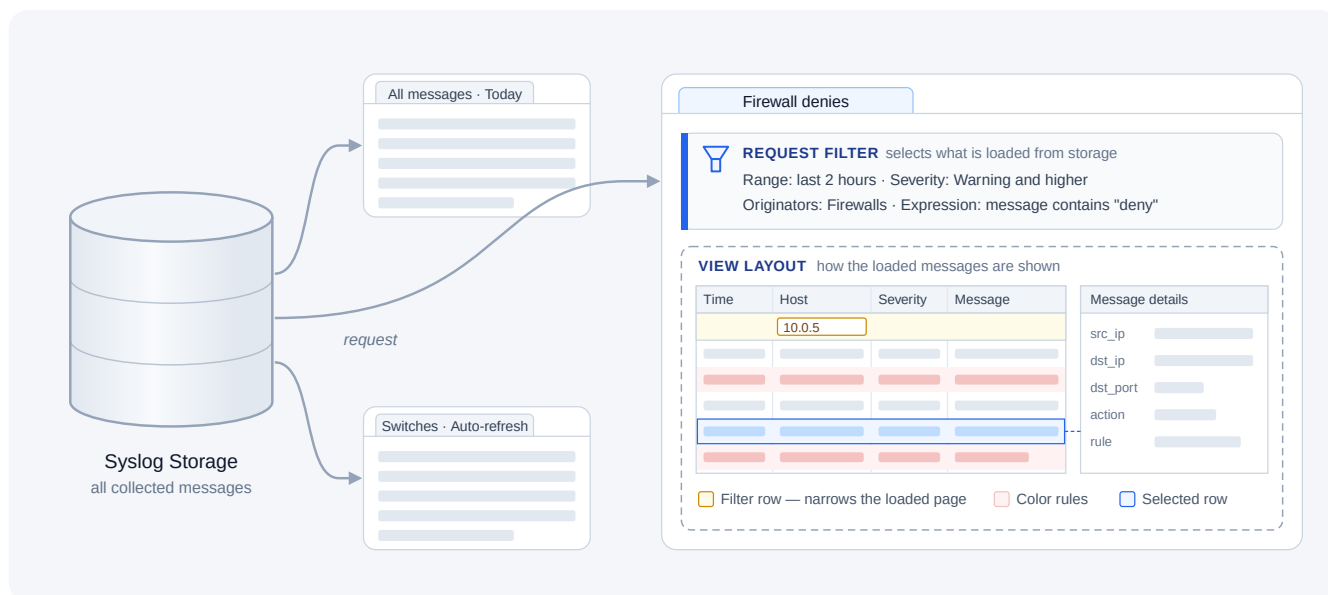
The report contains the selected message, its parsed fields, the columns as shown, the view layout, and the parser configuration. **Send Request** sends it to EZ5. If the computer has no Internet access, click **Save Request to File...** and attach the file to a [support ticket](#).

Related Topics

- [Syslog Parsers](#)
- [View and Search Messages](#)

Viewing Messages

Syslog messages the [collector](#) receives end up in [syslog storage](#). You work with those messages in **view tabs** in Manager. A view tab is a read-only window into the storage: you can open, filter, and close tabs freely, and the stored messages stay as they are.



Storage and view tabs (simplified schematic, not the actual Manager window)

Each tab sends its own request to the storage. The **request filter** — time range, severity, originators, and a filter expression — searches the whole storage and decides which messages are loaded. The **view layout** decides how they look: columns, row colors, and the details panel for the selected message. The **filter row** and **Find** then narrow down or search the loaded page, without going back to the storage.

View Tabs

To open a tab, click **View/Search** in the **Messages** section of the main toolbar, pick a time range and a filter, and click **Request**. The tab loads the matching messages from storage and shows them as a grid, one message per row.

Alternatively, open a view tab from the [Storage tab](#): click a message count there, and a new tab opens with exactly those messages — for example, the errors received in a given hour.

Keep as many tabs open as you need: one per firewall, one for errors only, one following live traffic with auto-refresh. Tab settings are saved on the server for your user account, so the tabs come back after Manager restarts or when you connect from another computer; click **Refresh** to load their messages again.

See [View/Search Messages](#).

View Layouts

A **view layout** controls how a tab presents messages: which fields appear as columns, which rows

get highlighted, and what the details panel shows for the selected message. A layout that fits your message format makes the grid easy to scan.

Syslog Watcher ships with a number of view layouts, including standard RFC syslog and key-value logs. For other devices, duplicate one of these layouts and adjust the copy to the fields your devices send. Each tab keeps its own copy of the layout, so you can tweak a single tab without affecting the others.

See [View Layouts](#).

View/Search Presets

If you run the same search often — say, firewall denies over the last two hours — save it as a **View/Search preset**. Presets are listed under the **View/Search** button on the main toolbar, so you can start a new tab with the stored range, filter, and layout instead of filling them in each time.

See [View/Search Presets](#).



For counts and trends over longer periods, a [report](#) is usually a better fit than scrolling through a view tab.

View/Search Messages

A **view tab** shows messages from syslog storage that match a time range and a [filter](#). A [view layout](#) defines the columns, colors, and the message details panel.



A view tab only reads the storage: closing it or changing its request does not change the stored messages.

View tabs are saved on the server for each user. They come back after Manager restarts, and in a [remote session](#) from another computer.



Only the tab settings are saved — name, time range, filter, and layout — not the loaded messages. When Manager starts again, the restored tabs are empty: click **Refresh** on a tab to run its search again.

Open a View Tab

Open a view tab in one of these ways:

- ▶ In the **Messages** section of the main toolbar, click **View/Search** → **View/Search Messages...**
- ▶ In the same **View/Search** drop-down, choose one of up to 20 [presets](#) (**Preset:** <name>).
- ▶ Click a message count on the [Storage tab](#).
- ▶ On the [Server tab](#) diagram, click 🔍 on **Syslog Storage**.

The New View Tab window with a CUSTOM time range

In the **New View Tab** window:

1. Enter a **Name** for the tab — a short descriptive name, such as **Firewall denies**, helps you recognize it among other open tabs.
2. In **Layout based on**, choose a **view layout**. Its configuration is copied to the tab, so you can later edit the tab's own copy without changing the stored layout (**Layout of a Tab**).
3. Choose the time **Range** — see [below](#).
4. Set **Messages per page** — the page size (100 ... 200000). When more messages match, the results are split into pages; **Prev. Page** and **Next Page** on the **tab toolbar** move between them.
5. Set **Filter/Search**: **severity**, **originators**, and **filter expression**. Only matching messages are loaded from the syslog storage.
6. Click **Request**.

To change the request of an open tab later, click **Request...** on the **tab toolbar**: it opens the same settings in the **Modify View Request** window.

Time Range

Days follow the time zone of the Syslog Watcher Server — for a remote connection, the server's time zone, not that of the Manager computer. The tab's status bar shows the time zone in use (**Time zone**).

Range	Messages
TODAY	The current calendar day.
YESTERDAY	The previous calendar day.

Range	Messages
RECENT	The last N minutes, hours, or days, up to the current time — for example, the last 2 hours.
ENTIRE STORAGE	Everything in storage.
CUSTOM	Between the From and Until date and time you set.

Set and Adjust the Range

RECENT

In **Last**, type a number from 1 to 999 or use the – and + buttons, then choose minutes, hours, or days from the drop-down.

CUSTOM

Set **From** and **Until**: type a date and time, or use the buttons next to each value:

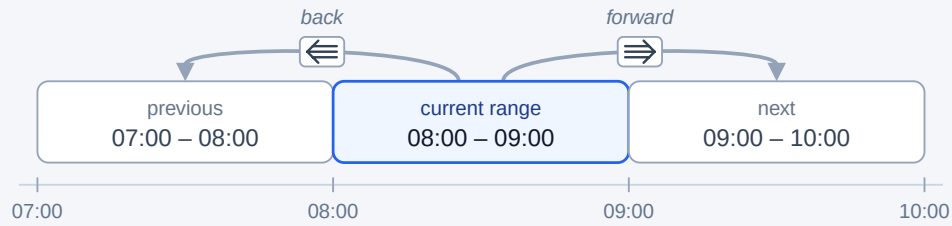
- « / » — one day back or forward
-  — pick a date in a calendar
- < / > — one hour back or forward
-  — set the time to **Midnight** or **Midday**

From cannot be later than **Until**: if you move one past the other, the other one follows to the same time.

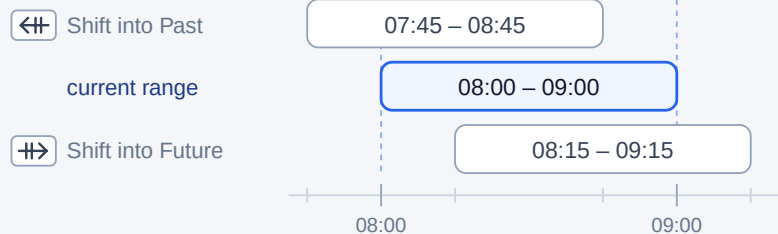
With **CUSTOM**, the **Range** row also moves the whole range without changing its length:

- the two arrow buttons move it back or forward by its own length — for example, from one hour to the previous hour
- the drop-down next to them shifts it by a fixed step: **Shift Range into Past** / **Shift Range into Future** by 15 minutes ... 30 days

Arrow buttons: move by the range length (like pages)



Shift Range menu: move by a fixed step (here 15 minutes)



Moving a one-hour CUSTOM range

Search Progress

A search over a wide range with a filter expression can take a while. A progress window then shows how many messages have been checked so far and which point in the time range the search has reached.



To speed up a search, narrow the time range or filter by severity and originators — these use the storage index. A filter expression has to check every message.

Tab Toolbar

▢ Tab ▾	Tab settings — see Tab Menu below.
☰ Layout...	Edit the tab's view layout.
🔍 Request...	Change the time range and the message filter of the tab.
⏮ Prev. Page	Load the previous page of messages.
⏭ Next Page	Load the next page of messages.
🔄 Refresh	Load new messages now.
Auto:	Refresh automatically every N seconds or minutes, or Auto: OFF .
Filter Rows ▾	Show or hide the filter row .
Find ▾	Show or hide the find bar .

Tab Menu

Command	Description
Rename Tab...	Change the name shown on the tab.
Sort: ↑ Newest at top	Show the newest messages first.
Sort: ↓ Newest at bottom	Show the newest messages last.
Auto-Scroll to New Messages	After each refresh, scroll to and select the newest message — useful with Auto: refresh.

Result Line and Status Bar

The result line of the tab shows what was **Requested** (range and filters) and what was **Loaded**: the number of messages, the page number when there is more than one page, and the time of the first and last loaded message.

The status bar shows:

- **Total** — messages loaded
- **Visible** — messages left after the filter row
- **Selected** — selected rows
- **Time zone** — the server time zone used for the range
- **Tab updated** — how long ago the tab was refreshed, and how long the request took

Message Grid

Each row is one message; the columns come from the view layout. Row colors come from the layout's color rules.

Filter Row

The filter row under the column headers has a text cell for each column. Type text in a cell to keep only the rows whose value in that column contains it (case-sensitive). When several cells have text, a row must match all of them. While the filter row is hidden (**Filter Rows** on the tab toolbar), its filters are not applied and all loaded rows are shown.



The filter row works only on the loaded page. To search the whole storage, change the tab's **Filter/Search** with **Request....**

Find

Find searches in **ANY column** or in one selected column. Matching ignores letter case. ↕ **Next** and ↕ **Prev.** move to the next match below or above the current row, wrapping around at the end.



Find searches only the rows shown in the grid: the loaded page, after the **filter row**. Rows hidden by the filter row are skipped.

Message Details

The message details panel shows the selected message as HTML, formatted by the layout's **HTML Sections**. Its position (left, right, or bottom) and size are layout settings.

Copy Messages

Select the rows to copy:

- click a row to select it
- **Ctrl** + click to add or remove a row
- **Shift** + click to select all rows between the current row and the clicked one
- **Ctrl** + **A** to select all rows shown in the grid

Then right-click the selection and choose a command:

Command	Copies
Copy as Shown (CSV)	The visible columns, comma-separated.
Copy as Shown (TAB)	The visible columns, tab-separated — pastes into a spreadsheet.
Copy as Parsed (JSON)	The parsed fields of each message as JSON.
Copy as Received (TEXT)	The raw messages as received.

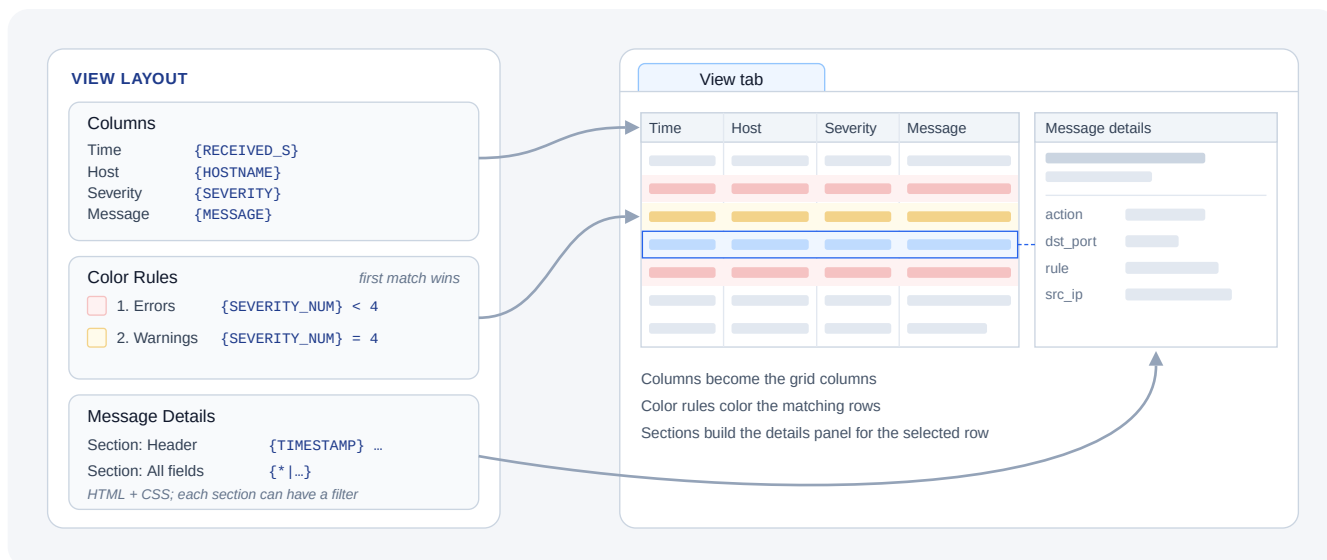
Report Incorrect Parsing... sends the selected message to EZ5 when a [parser](#) splits it wrongly.

Related Topics

- [Viewing Messages](#)
- [View Layouts](#)
- [View/Search Presets](#)
- [Filtering](#)
- [Storage Overview](#)

View Layouts

A **view layout** defines how a [view tab](#) displays messages: the grid columns, row colors, and the message details panel. Different message formats call for different layouts — for example RFC syslog headers, key-value logs, or a vendor format with a field collection.



How a view layout shapes a view tab (simplified schematic)

Create a Layout

The easiest way is to start from a layout that is close to your message format:

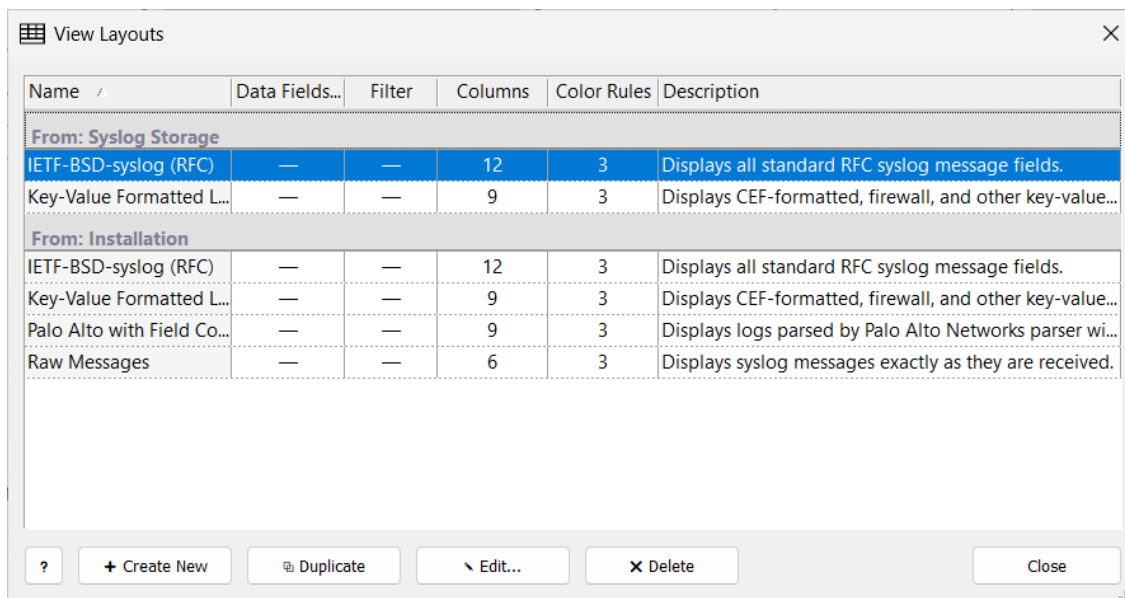
1. In the **Messages** section of the main toolbar, click **Layouts**.
2. Select an **Installation** layout and click **Duplicate**. A **New View Layout** window opens with a copy named **<name> copy 1**. Installation layouts are read-only; the copy can be edited.
3. In **General Properties**, change the **Name**.
4. Adjust the **columns** — the fields shown in the grid.
5. Add **color rules** to highlight important rows.
6. Design the **message details** panel.
7. Click **Create**. The layout is saved in syslog storage.

To use the layout, choose it in **Layout based on** when you **open a view tab**.

View Layouts Window

In the **Messages** section of the main toolbar, click **Layouts**.

The list groups layouts by where they come from. **Installation** layouts ship with the product and are read-only; editing one offers to create an editable copy instead. Your own layouts appear under **Syslog Storage** and are saved in the syslog storage index.



The View Layouts window

The installation includes these layouts:

- **IETF-BSD-syslog (RFC)** — all standard RFC syslog fields
- **Key-Value Formatted Logs** — details panel that lists every extracted field
- **Raw Messages** — the message as received
- more layouts are added in product updates

View Layout

Import / Export saves the layout to a JSON file (**Export to File...**) or loads one (**Import from File...**).

Edit View Layout

General Properties

NameIETF-BSD-syslog (RFC)

DescriptionDisplays all standard RFC syslog message fields.

Data Fields (Optional)

Layout Filter [OFF]

Columns (12)Add Column

Received{RECEIVED_S|%Y/%m/%d %H:%M:%S}

Originator ID{ORIGINATOR_ID}

Originator Name{ORIGINATOR_NAME}

Severity{SEVERITY}

Facility{FACILITY}

Timestamp{TIMESTAMP}

Hostname{HOSTNAME}

AppName{APPNAME}

ProcID{PROCID}

MsgID{MSGID}

SeqNum{SEQNUM}

Message{MESSAGE}

Expand AllCollapse All

A view layout defines how messages stored in syslog storage are displayed. It customizes the table appearance and the message details panel.

?

Import / Export

Apply

Cancel

Editing a view layout

The layout editor has these sections:

General Properties	Name (required, unique) and Description .
Data Fields (Optional)	Extra fields from the message body, for use in columns, color rules, and details; see Field Extraction .
Columns	The grid columns.
Color Rules	Row colors.
Message Details	The HTML details panel.



Columns, color rules, and HTML sections are ordered lists, and the order matters.

Columns appear in the grid from left to right, the first matching color rule wins, and sections are added to the details panel from top to bottom. Use the ↑ and ↓ buttons on an item to rearrange the list.

Columns

Click **Add Column** to add a new column. A layout needs at least one column.

Setting	Description
Column title	Header text.

Setting	Description
Column format	Fields and text, for example {SEVERITY_NUM} / {SEVERITY} or {RECEIVED_S %Y/%m/%d %H:%M:%S}. Modifiers are allowed.
Column width	Width in pixels.

Color Rules

Click **Add Color Rule** to add a new rule.

Setting	Description
Rule name	Name of the rule, for example Errors in Red.
Rule filter	Messages the rule applies to, for example {SEVERITY_NUM} < 4. See Filter Expressions.
Text color / Background color	Type an RGB value, for example 0; 128; 0, or pick a color.

Rules are checked from top to bottom, and the first rule that matches sets the colors of the row.



Put specific rules above general ones. For example, a rule for one firewall's denies must come before a rule for all errors, or the error color always wins.

Message Details

- Panel position** Left, Bottom, or Right.
- Panel size** Width of a left or right panel, or height of a bottom panel.
- Style (CSS)** CSS for the panel, for example body { font-family: sans-serif; }.
- HTML Sections** One or more HTML templates.

Click **Add Section** to add a new section.

Setting	Description
Section name	Name of the section.
Section filter	Messages the section is shown for. Leave it blank to show the section for every message.
Section (HTML)	HTML with message fields.

Use section filters to show extra details only for some messages, for example a firewall section only for firewall messages.

Example section that lists every extracted field in a table:

```
<p>{TIMESTAMP|EscHTML}<br><strong>{SEVERITY}</strong> / {FACILITY}</p>
<table>
```

```
{*|<tr><td>{FIELD_NAME|EscHTML}</td><td><strong>{FIELD_VALUE|EscHTML}</strong></td></tr>}</table>
```

`{*|...}` repeats the template inside it once for every extracted field; `{FIELD_NAME}` and `{FIELD_VALUE}` are the name and value of the current field. See [Message Fields](#).



Apply **EscHTML** to message text in HTML sections so `<`, `>`, and `&` in syslog messages display correctly.

Layout of a Tab

A view tab keeps its own copy of the layout it was created from. **Layout...** on the tab toolbar edits that copy, so the change affects only that tab.



Editing a stored layout does not change tabs already opened with it. To apply the new version to an open tab, use **Load from Existing Layout...** in the tab's layout editor.

In the layout editor of a tab:

- **Save Layout to Storage...** — save the tab's layout to a stored layout (new or existing)
- **Load from Existing Layout...** — replace the tab's layout with a stored or installation layout

Related Topics

- [View/Search Messages](#)
- [View/Search Presets](#)
- [Message Fields](#)
- [Field Collections](#)
- [Escape Modifiers](#)
- [Filter Expressions](#)

View/Search Presets

A **View/Search preset** is a saved set of settings for a new view tab: time range, filter, layout, page size, and sorting. Use presets for searches you run often, instead of filling in the request each time.

Presets are saved in syslog storage, so they are shared: every user who connects to the server sees and uses the same presets.

Create a Preset

1. In the **Messages** section (the main toolbar), click **View/Search** → **Manage View/Search Presets...**

2. Click **Create New**, or select a preset and click **Duplicate** to start from a copy.
3. Give the preset a **Name**; it is shown in the **View/Search** drop-down.
4. Set the time range, filter, layout, page size, and sorting; see [View/Search Preset](#).
5. Click **Create**.

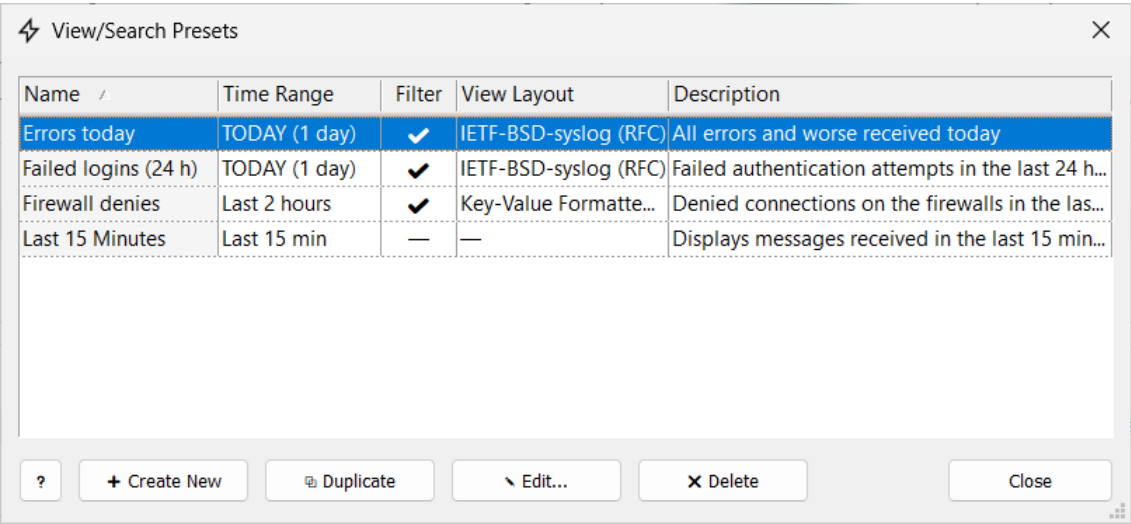
Use a Preset

In the **Messages** section (the main toolbar), click  **View/Search**. The drop-down lists presets as **Preset: <name>** (up to 20).

Clicking one opens the **New View Tab** window filled in with the preset settings. You can still change any setting, for example narrow the time range, before you click **Request** to open the tab.

View/Search Presets Window

In the **Messages** section (the main toolbar), click  **View/Search** →  **Manage View/Search Presets...** The window lists all presets saved in syslog storage; here you can create, edit, duplicate, and delete them.



Name /	Time Range	Filter	View Layout	Description
Errors today	TODAY (1 day)	✓	IETF-BSD-syslog (RFC)	All errors and worse received today
Failed logins (24 h)	TODAY (1 day)	✓	IETF-BSD-syslog (RFC)	Failed authentication attempts in the last 24 h...
Firewall denies	Last 2 hours	✓	Key-Value Formatte...	Denied connections on the firewalls in the las...
Last 15 Minutes	Last 15 min	—	—	Displays messages received in the last 15 min...

The View/Search Presets window

View/Search Preset

Import / Export saves the preset to a JSON file (**Export to File...**) or loads one (**Import from File...**).

Editing a View/Search preset

Preset Properties

Name	Required, unique. Shown in the View/Search drop-down.
Description	Optional.

Request

Range	Time range of the new tab; see Time Range .
Messages per page	Page size of the new tab; see Open a View Tab .



TODAY, **YESTERDAY**, and **RECENT** (for example the last 2 hours) are the most useful ranges for a preset: they are counted from the moment the tab is opened, so the preset always shows current messages. A **CUSTOM** range is saved as fixed dates, so the preset always shows the same period.

Filter/Search

Severity level	Severities to load.
Originators	Originators or an originator group to load.
Filter expression	An expression that messages must match.

See [Filtering](#).

View Tab Defaults

Layout based on	View layout of the new tab.
Message sorting	Sort: ↓ Newest at bottom or Sort: ↑ Newest at top ; see Tab Menu .

Related Topics

- [View/Search Messages](#)
- [View Layouts](#)
- [Filtering](#)

Syslog Server

Syslog Watcher Server is the Windows service (**Syslog Watcher 7 Server**, **SW7Server**) that runs:

- **features**: export, forwarding, email, HTTP requests, and programs
- scheduled **reports**
- **storage retention and the storage archive**
- **remote Manager access**
- **diagnostic emails**

The Server is separate from the **Syslog Collector**, which receives and stores messages.

The Server service is designed to run all the time. If the Server is stopped, start it from Manager on the server computer: in the **Server** section of the main toolbar, click  **Server** → **Start Syslog Server**.

Server Tab

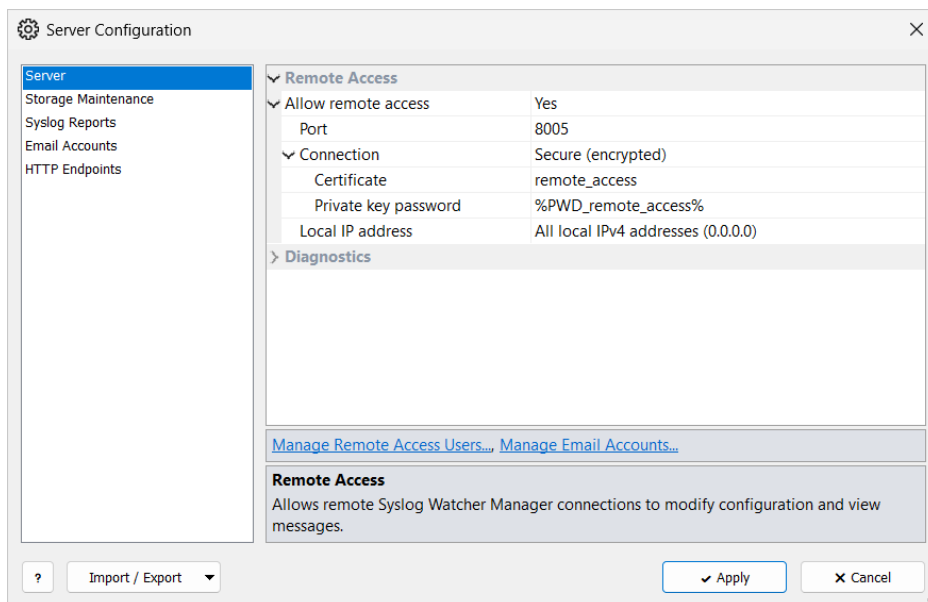
The **Server** tab shows a diagram of how messages move through the syslog server: **Originators** → **Syslog Collector** → **Syslog Storage** → **Server Features**. Click a part to open it or to show its details below the diagram.

Part	Click	Buttons
Originators	Opens the Syslog Originators window.	—
Syslog Collector	Shows collector status, network interfaces, and discarded messages; see Monitoring .	⚙ opens Syslog Collector Configuration . Start Collector is shown while the collector is stopped.
Syslog Storage	Shows stored messages by severity and the storage archive status .	🔍 opens a new view tab . ⚙ opens Server Configuration .
Server Features	Shows the features table; see Monitoring Features .	⚙ opens Server Features .

To change the scale of the tab, hold **Ctrl** and turn the mouse wheel, or set **Server tab scale** in **Manager Settings**.

Server Configuration

In the **Server** section of the main toolbar, click  **Server** → ⚙ **Server Configuration...**



The Server Configuration window

Server	Remote Access and Diagnostics (email warnings and errors).
Storage Maintenance	Storage retention and the storage archive .
Syslog Reports	Scheduled report generation .
Email Accounts	SMTP accounts for features and diagnostic emails.
HTTP Endpoints	Web servers for the Send HTTP Requests feature.

To copy the settings to another server, use **Import / Export: Export to File...** saves them to a `.config.json` file, and **Import from File...** loads one into the window. Review the imported settings and click **Apply**.

Related Topics

- [Secret Strings](#)
- [TLS Certificates](#)

Remote Access

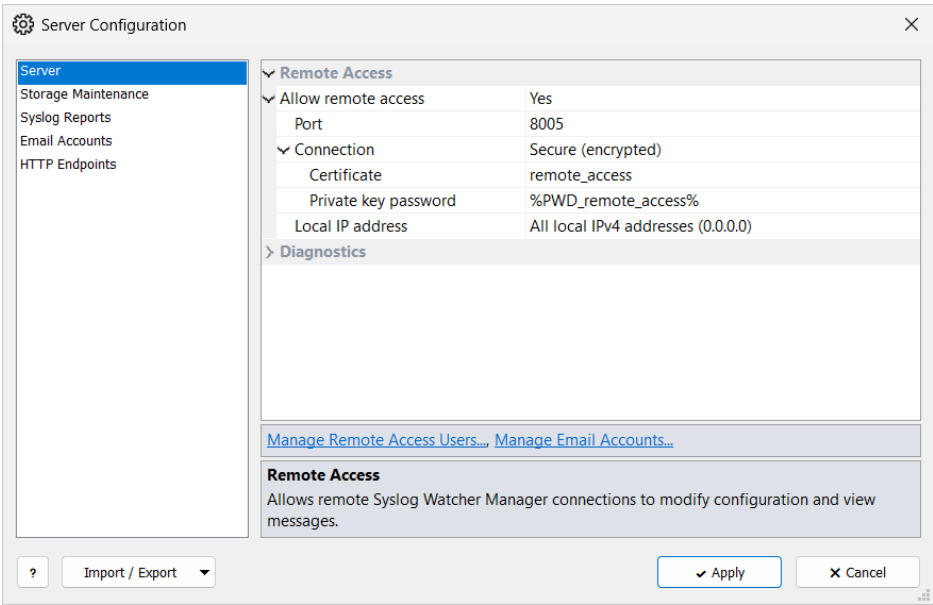
With remote access, you can manage a [Syslog Watcher Server](#) from Syslog Watcher Manager on another computer. Remote users sign in with a username and password; each user's [role](#) defines what they can view and change. To set up remote access, [enable it](#) on the server computer and [add users](#). Then [connect from Manager](#) on the other computer.

Enable Remote Access

On the server computer, connect Manager to the local server, and then:

1. In the **Server** section of the main toolbar, click **Server** → **Server Configuration...**
2. Select the **Server** page.

- 3. Set **Allow remote access** to **Yes**.
- 4. Check **Port** and **Connection**.
- 5. Click **Apply**.



Remote access settings on the Server page of Server Configuration

If no users exist yet, Manager warns and opens [Remote Access Users](#). Add at least one user; without users, no one can sign in.

Allow remote access	Yes lets Manager connect from other computers.
Port	TCP port for Manager connections (1–65535).
Connection	Plain (unencrypted) or Secure (encrypted) . The Protocol in Manager’s connection settings must match.
Certificate	Certificate for Secure (encrypted) , selected by name from TLS Certificates . The button next to the field opens the TLS Certificates window.
Private key password	Password for an encrypted private key. When you select a certificate whose key password is stored as a secret string , the field is filled with that secret (<code>%PWD_<certificate name>%</code>).
Local IP address	Local address to listen on. <code>0.0.0.0</code> listens on all IPv4 addresses of the computer; <code>:::0</code> on all IPv6 addresses.

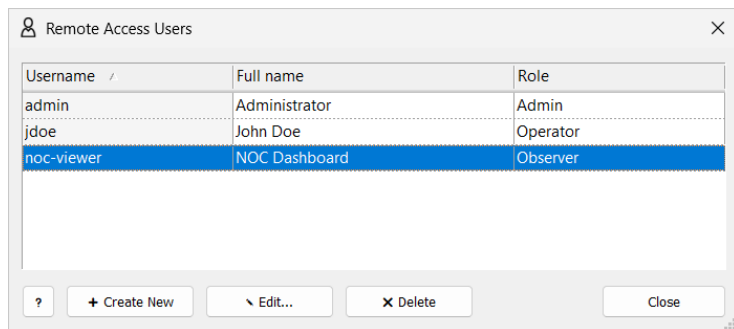
Secure Connection

When you set **Connection** to **Secure (encrypted)** and no certificate is selected, Manager generates a self-signed certificate named `remote_access` and selects it. The certificate has this computer’s name as Common Name (CN), a 2048-bit key, and is valid for 3650 days (10 years). Its key password is stored as the secret `PWD_remote_access`.

To use your own certificate instead, [import](#) it in **TLS Certificates** and select it in **Certificate**.

Remote Access Users

In the **Server** section of the main toolbar, click  **Server** → **Remote Access Users...** On the **Server** page of **Server Configuration**, **Manage Remote Access Users...** opens the same window.



The Remote Access Users window

Users who cannot manage other users see **Remote Access Users: Self Only** with only their own account, which they can edit.

Add a User

1. Click **Create New**.
2. Fill in the [user properties](#).
3. Click **Create**.

The first user is prefilled as **admin** with full name **Administrator** and role **Admin**. Further users start with the role **Observer**.

Edit a User

Select the user and click **Edit...**, change the properties, and click **Apply**.

The **Username** cannot be changed. You cannot change your own **Role**.

Delete a User

Select the user, click **Delete**, and confirm. You cannot delete your own account.

User Properties

User Properties	
Username	admin
Password	*****
Full name	Administrator
Role	Admin

User Properties
User property set

? Apply Cancel

The Edit User window

- Username** Sign-in name used to [connect](#). Required and unique; cannot be changed after the user is created.
- Password** Password for the connection. Required.
- Full name** Name shown in the users list. Required.
- Role** **Admin**, **Operator**, or **Observer** (see [Roles](#)).

Roles

Roles apply to remote sessions only. Manager on the server computer is not limited by roles: what it can do depends on the permissions of the Windows account that runs Manager. To connect to the local server, Manager asks for administrator rights.

Role: Admin

Everything: users, licenses, collector configuration and start/stop, storage location and limits, server configuration, secrets, certificates, and all storage objects.

Role: Operator

Day-to-day work: features (including suspend and resume), originators, groups, parsers, view layouts and presets, filter lists, field dictionaries and collections, report templates, scheduled reports, severity and facility names, server configuration, and test emails and HTTP requests.

Can add secrets and certificates, but not delete them. Can view, but not change, the collector configuration, storage location and limits, and licenses. Cannot manage other users or start and stop the collector.

Role: Observer

Read-only: status, configuration, diagnostic records, and stored messages. Can change only their own account and their own view tabs. Cannot schedule reports or send tests.

Related Topics

- [Syslog Server](#)

- Syslog Watcher Manager
- TLS Certificates

Email Accounts

An **email account** holds the SMTP server settings that the Syslog Watcher Server uses to send email. You set them up once and select the account by name in the [Send Emails](#) feature and in [diagnostic emails](#).

Server Configuration

Server
Storage Maintenance
Syslog Reports
Email Accounts
HTTP Endpoints

✓ Email Account: IT Alerts [Test Account](#) [Delete](#)

Name	IT Alerts
Server	smtp.example.com
Port	587
Connection type	STARTTLS
Username	syslog-alerts@example.com
Password	%SMTP_IT_ALERTS%
'From' email address	syslog-alerts@example.com

> Email Account: Internal Relay [Test Account](#) [Delete](#)

> Email Account: SOC Mailbox [Test Account](#) [Delete](#)

[Add Email Account](#)

Email Account: IT Alerts
Email accounts used to send email messages.

? Import / Export ▼ [✓ Apply](#) [✕ Cancel](#)

The Email Accounts page of Server Configuration

Add an Account

1. In the **Server** section of the main toolbar, click **Server** → **Server Configuration...**
2. Select the **Email Accounts** page.
3. Click **Add Email Account**.
4. Fill in the [account settings](#).
5. Click **Apply**.

Use the SMTP settings that your mail provider gives for email clients.



Many providers require an app password or an SMTP relay for automated senders.

Email Account

✓ Email Account: IT Alerts Test Account Delete	
Name	IT Alerts
Server	smtp.example.com
Port	587
Connection type	STARTTLS
Username	syslog-alerts@example.com
Password	%SMTP_IT_ALERTS%
'From' email address	syslog-alerts@example.com

An email account

Name	Name shown in features and in the Diagnostics settings. Required.
Server	SMTP server IP address or host name, for example <code>smtp.example.com</code> . Required.
Port	SMTP port; the list offers 25, 465, and 587. Usually 587 for STARTTLS and 465 for SMTPS.
Connection type	SMTP (non-secure) , SMTPS (TLS from the start), or STARTTLS (plain connection upgraded to TLS).
Username	SMTP login, usually an email address or account name.
Password	SMTP password. Use a secret string (<code>%EXAMPLE%</code>) instead of the actual password.
'From' email address	Sender address of the emails. Required. The SMTP server must accept it as a sender for this login.

Test the Account

1. Click **Test Account** on the account.
2. In **Send a test email to:**, enter a recipient.
3. Click **Send Email**.

The window shows **SUCCESS** or **FAILED**, followed by the SMTP server's response. The test uses the settings currently in the window, so you can test before you click **Apply**.

The email is sent from the **Syslog Watcher Server** computer, so the test also checks DNS, firewall, and TLS settings on that computer.

Delete an Account

Click **Delete** on the account, confirm, and click **Apply**.



Features that use the account stop sending until another account is selected.

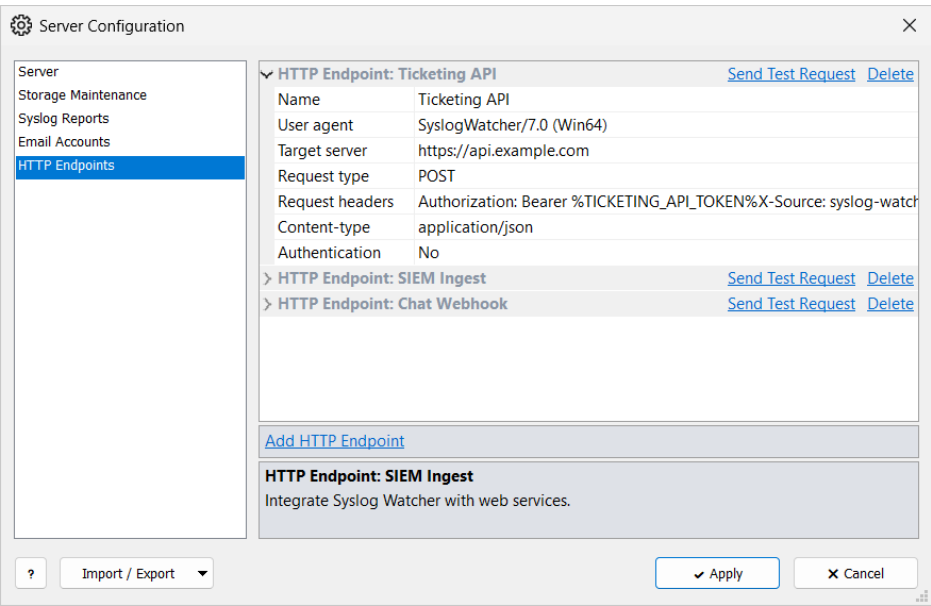
Related Topics

- [Send Emails](#)
- [Server Diagnostics](#)
- [Secret Strings](#)

HTTP Endpoints

An **HTTP endpoint** holds the web server settings that the Syslog Watcher Server uses to send HTTP requests: address, request type, headers, and authentication. You set them up once and select the endpoint by name in the [Send HTTP Requests](#) feature, which adds the resource path and body for

each message.



The HTTP Endpoints page of Server Configuration

Add an Endpoint

1. In the **Server** section of the main toolbar, click **Server** → **Server Configuration...**
2. Select the **HTTP Endpoints** page.
3. Click **Add HTTP Endpoint**.
4. Fill in the [endpoint settings](#).
5. Click **Apply**.

HTTP Endpoint

HTTP Endpoint: Ticketing API		Send Test Request	Delete
Name	Ticketing API		
User agent	SyslogWatcher/7.0 (Win64)		
Target server	https://api.example.com		
Request type	POST		
Request headers	Authorization: Bearer %TICKETING_API_TOKEN%X-Source: syslog-watch		
Content-type	application/json		
Authentication	No		

An HTTP endpoint

Name	Name shown in the feature. Required.
User agent	User-Agent header sent with each request.
Target server	Address with protocol and optional port, for example https://api.example.com or http://10.0.0.5:8080 . Required. Use https:// for TLS.
Request type	POST or PUT .
Request headers	Optional headers, one per line, for example an API key: Authorization: Bearer %API_TOKEN% . Use secret strings (%EXAMPLE%) for private values.

Content-type	Content-Type of the body: choose <code>text/plain</code> , <code>application/json</code> , <code>multipart/form-data</code> , or <code>application/x-www-form-urlencoded</code> , or type another type. Required.
Authentication	None or Basic . With Basic , Username and Password are required; use a secret string for the password.

Send a Test Request

1. Click **Send Test Request** on the endpoint.
2. Enter a **Resource path** (for example `/api/send-message`) and a **Request body**.
3. Click **Send Request**.

The window shows the **Status code** and the body of the web server's response, or the error.

The request is sent from the **Syslog Watcher Server** computer.



Use a body in the same format as the feature template, for example a small JSON object.

Delete an Endpoint

Click **Delete** on the endpoint, confirm, and click **Apply**.



Features that use the endpoint stop sending until another endpoint is selected.

Related Topics

- [Send HTTP Requests](#)
- [Secret Strings](#)
- [Escape Modifiers](#): `EscJSON` and `EscURL`

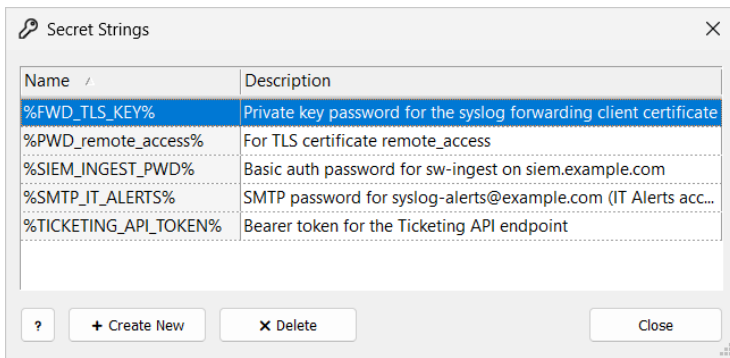
Secret Strings

A **secret string** is a named, encrypted value stored on the Syslog Watcher Server. Settings refer to it as `%Name%` instead of holding the actual password or key.

- Configuration files do not contain the real value.
- One secret can be used in several places; when the password changes, you update only the secret.

Secret Strings Window

In the **Server** section of the main toolbar, click **More** → **Secret Strings...** The  button next to a setting that accepts secrets opens the same window.



The Secret Strings window

In a remote session, **Operator** can add secrets and **Admin** can also delete them. For other users, the window is **Read Only**.

Create a Secret

1. In the **Secret Strings** window, click **Create New**.
2. Fill in the [secret settings](#).
3. Click **Create**.

Secret String

 A screenshot of the 'Secret String' window. It shows a form with the following fields: 'Name' (containing 'SMTP_IT_ALERTS'), 'Description' (containing 'SMTP password for syslog-alerts@example.com (IT Alerts acco...)', 'Secret string' (containing '*****'), and 'Secret confirmation' (containing '*****'). Below the form is a section titled 'Name' with a description: 'Name of the secret string. A secret name enclosed in percent signs (%EXAMPLE%) can be used in place of a password.' At the bottom are buttons for '?', '✓ Create', and 'X Cancel'.

The Secret String window

Setting	Description
Name	Used as %Name% . Required; no % signs; at most 128 UTF-8 bytes.
Description	Optional; at most 1024 UTF-8 bytes.
Secret string	The value. Required. You enter it once; it cannot be viewed or changed later.
Secret confirmation	The same value again.

To change a value, delete the secret and create it again with the same name.

Use a Secret

In a setting that accepts secrets, choose the secret from the setting's list, or type **%Name%**. These settings include:

- email account and HTTP endpoint passwords, and HTTP request headers
- private key passwords (TLS network interfaces, remote access, forwarding over TLS)
- the **Password** of **Execute Program/Script** and of the archive command
- the archive zip password

The server replaces **%Name%** with the value when it uses the setting. If no secret has that name, the text stays as typed.

When you generate or import a TLS certificate with an encrypted private key, Manager saves the key password as the secret **PWD_<certificate name>** (description **For TLS certificate <certificate name>**). Deleting the certificate also deletes the secrets with that description.

How Secrets Are Protected

Secrets are encrypted with Windows DPAPI for the server computer. They cannot be decrypted on another computer.

When you move a configuration to another installation, create the same secret names there.

Related Topics

- [Email Accounts](#)
- [HTTP Endpoints](#)
- [TLS Certificates](#)

TLS Certificates

TLS Certificates is the certificate store of the Syslog Watcher Server. Settings that need a certificate select it by name from this store instead of pointing to files:

- ▶ **TLS network interfaces**: server certificate and client CA
- ▶ **Remote access**: certificate for encrypted Manager connections
- ▶ **Forward to Syslog Server** over TLS: CA and client certificate

TLS Certificates Window

In the **Server** section of the main toolbar, click **More** → **TLS Certificates...**

The list shows **Name**, **Type**, **Issuer**, and **Subject**. Self-signed certificates show **Self-signed** as the issuer.

Type	Meaning
Certificate + Key	Certificate with an unencrypted private key.

Type	Meaning
Certificate + Encrypted Key	Certificate with a password-protected private key. The password is stored as the secret string <code>PWD_<certificate name></code> . When you select the certificate in a setting, its Private key password is filled with that secret.
CA	CA certificate without a private key, used to validate peers.

In a remote session, **Operator** can add certificates and **Admin** can also delete them. For other users, the window is **Read Only**.

Generate a Self-signed Certificate

1. Click **Generate**.
2. Check the prefilled **Common Name (CN)** and **SAN** entries, and fill in the other settings.
3. Click **Generate**.

If you entered a key password, Manager shows the name of the secret that stores it.

Setting	Initial	Description
Name	Certificate1	Name in the store.
Expiration (days)	3650	Validity period (1–36500 days).
Common Name (CN)	This computer's full DNS name	Usually the fully qualified host name of the server.
SAN: Subject Alternative Names	This computer's DNS names and IP addresses (except loopback)	DNS names and IP addresses the certificate is valid for (up to 32). Click Add , choose DNS or IP as Type , and pick a local host name or address, or type one. Clients check the name they connect with against this list.
Optional Subject Fields	—	Country code (C) , State or province name (ST) , Locality name (L) , Organization name (O) , Organizational unit (OU) .
Key size	2048	RSA key size: 2048 or 4096 bits.
Encrypt key with password, Password confirmation	—	Optional password for the private key. Generate Random fills both fields with a random password. Leave both empty for an unencrypted key.



Add to **SAN** every name and address that clients use to reach the server. Modern TLS clients check SAN, not CN.



Manager generates the certificate and prefills **CN** and **SAN** from the computer it runs on. In a remote session, replace them with the server computer's names and addresses.

Import a Certificate

1. Click **Import**, then **From PEM File...** or **From Clipboard...**
2. In the **Import Certificate** window, check the **Name** suggested from the certificate.
3. For an encrypted private key, enter its **Password**.
4. Click **Import**.

What is imported depends on the PEM content:

- A certificate and a private key: **Certificate + Key** or **Certificate + Encrypted Key**.
- Only a certificate or only a key: Manager asks for the other part (a second file, or the clipboard).
- Only a CA certificate: **CA**.

The PEM data is read on the Manager computer and stored on the server.

Export a Certificate

Select an entry and click **Export** → **Certificate Only (No Private Key)** → **To PEM File...** or **To Clipboard...** The private key is never exported.

Export a self-signed or CA certificate to install it as trusted on the clients.

Delete a Certificate

Select an entry, click **Delete**, and confirm. The secret with its key password is deleted too. Settings that refer to the certificate by name stop working until another certificate is selected.

Related Topics

- [Syslog over TLS](#)
- [Remote Access](#)
- [Secret Strings](#)

Server Diagnostics

The Syslog Watcher Server writes its own diagnostic records: startup, license, features, reports, storage maintenance, and remote access. They are separate from the [collector's diagnostic records](#).

Diagnostic Records (Server)

In the **Server** section of the main toolbar, click  **Server** → **Diagnostic Records (Server)**. A **Diagnostics (Server)** tab opens.

Server Storage Last 15 Minutes Firewall denies Diagnostics (Server)			
? Prev. Records 2026-10-09 Next Records Refresh Show DEBUG records Save to File...			
Level	Timestamp (ISO Format)	Component	Diagnostic record
Info	2026-10-09 17:25:10-07:00	Main	> > > Syslog Watcher Server version 7.0.5, Windows OS 602931718
Info	2026-10-09 17:25:10-07:00	Main	Timezone: America/Los_Angeles
Info	2026-10-09 17:25:10-07:00	Main	Syslog storage: C:\ProgramData\SyslogStorage7
Info	2026-10-09 17:25:10-07:00	Main	Creating syslog storage in: C:\ProgramData\SyslogStorage7
Info	2026-10-09 17:25:10-07:00	Main	Configuration file is missing, creating default configuration.
Info	2026-10-09 17:25:10-07:00	Main	Server started successfully.

Diagnostics (Server)

Records are kept in one file per day. The tab opens on the latest day.

◀ Prev. Records	Show the records of the previous (older) day.
Date drop-down	Jump to a day.
▶ Next Records	Show the records of the next (newer) day.
↻ Refresh	Reload the records of the selected day.
Show DEBUG records	Show all records, including Debug ones, or only the important ones.
💾 Save to File...	Save the records of the selected day to a .log file.

Typical records: feature failures and recoveries, report generation results, storage files deleted by [retention](#), archive syncs, and the result of the command run after a sync.

Email Diagnostic Records

The server can email new critical, error, and warning records from both the server and the collector.

1. In the **Server** section of the main toolbar, click **Server** → **Server Configuration...**
2. Select the **Server** page and find **Diagnostics**.
3. Set **Email error diagnostic records** to **Yes**.
4. Fill in **Send emails to** and **Use email account**.
5. Click **Apply**.

Setting	Description
Email error diagnostic records	Yes sends warning, error, and critical records by email.
Send emails to	Comma-separated recipient addresses. Required when sending is on.
Use email account	One of the email accounts . Required when sending is on. Manage Email Accounts... on the same page opens the Email Accounts page.

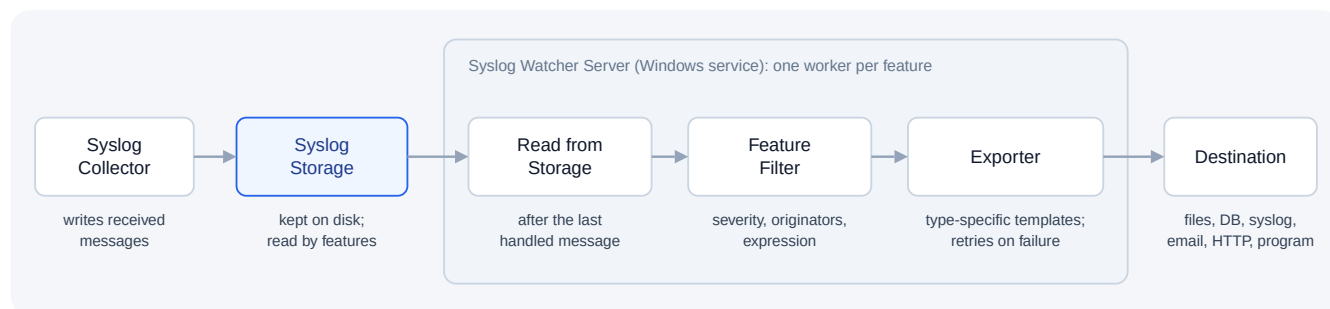
Related Topics

- [Diagnostic Records \(Collector\)](#)
- [Server Tab](#)
- [Technical Support](#)

Features

A **feature** is a background task of the **Syslog Watcher Server** service. It reads syslog messages that are already in syslog storage and sends the matching ones somewhere else: files, a database, another syslog server, email, an HTTP endpoint, or a program.

Use features when Syslog Watcher must do more than store logs, for example to forward a filtered stream to a SIEM, keep a text copy for another product, or email alerts for high-severity events.



How a feature processes messages (simplified schematic)

How a Feature Processes Messages

Features are not part of the [syslog collector](#). The collector writes messages to storage; features read them from storage later. Collection therefore continues while a feature is slow, suspended, or failing; the feature catches up later.

Each active feature that is not suspended works like this:

1. It reads messages from storage, starting after the last message it handled.
2. It applies the feature [filter](#): severity, originators, and an optional expression.
3. It passes the matching messages to its exporter, which formats them and sends them to the destination.

If the destination fails, the feature retries the same message until it succeeds; it does not skip it. See [Monitoring Features](#).



Messages that do not match the filter are skipped permanently. The feature reads them again only if you [resume](#) it from an earlier date and time.

New features start suspended. [Resume](#) a feature to start processing.

Feature Types

Type	What it does
Export to Files	Writes messages to text files, for example one file per day or one folder per originator.
Export to DB (ODBC)	Runs SQL commands (usually INSERT) on an ODBC data source.

Type	What it does
Forward to Syslog Server	Forwards messages to another syslog server over UDP, TCP, or TLS.
Send Emails	Sends email alerts for messages that match email rules.
Send HTTP Requests	Sends one HTTP request (POST or PUT) per message to an HTTP endpoint, such as a webhook or an API.
Execute Program/Script	Starts a program or script for each matching message.

Related Topics

- [Managing Features](#) — add, configure, suspend, resume, delete, import, and export
- [Monitoring Features](#) — status, counters, and errors on the Server tab
- [Syslog Collector](#) — how messages get into storage

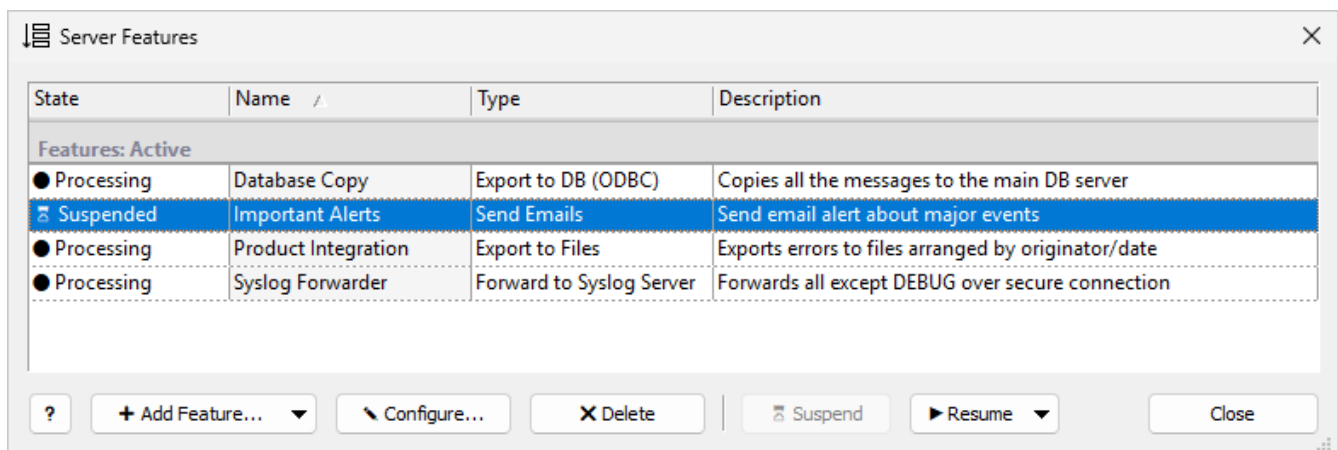
Managing Features

You create and control features in the **Server Features** window. It is available when Manager is connected to a local or remote server, not when only a storage folder is open.

Server Features

Open the window in one of these ways:

- In the **Server** section of the main toolbar, click  **Features**.
- On the [Server tab](#), click the gear symbol next to **Server Features** in the diagram.



Server Features

- + Add Feature...** Create a feature of the chosen type.
- ⚙ Configure...** Open the selected feature (**View...** without permission to change features).
- ⏸ Suspend** Pause the selected feature.

- **Resume** Start the selected suspended feature (drop-down).
- Delete** Delete the selected feature.

Adding a Feature

- Click + **Add Feature...** and choose the type. The **New Feature** window opens with example settings for that type.
- Enter a **Name**, set the **Filter**, and change the type-specific settings.
- Click **Create**.
- Resume** the feature.



A new feature is created suspended. It does not process messages until you resume it.

Configuring a Feature

- Select a feature and click ⚙ **Configure...**, or double-click the feature.
- Change the settings in the **Edit Feature** window.
- Click **Apply**.

Without permission to change features, the button is 👁 **View...** and the window is read-only.

Every feature window has the same **Feature**, **Data Fields**, and **Filter** sections. The type-specific section is described on each type’s page (see **Feature Types**).

Suspending a Feature

Select the feature and click ⏸ **Suspend**.

The feature stops reading storage but keeps its position. Messages collected in the meantime stay in storage, so you can process them when you resume.

Resuming a Feature

Select a suspended feature, click ► **Resume**, and choose where to start:

Command	Processing starts with
From Suspension Time	The first message after the feature’s saved position. Messages collected while the feature was suspended are processed.
From Now (Skip Messages)	Messages collected after you resume. Messages collected while the feature was suspended are skipped.
From Date/Time (Reset)...	Messages from the date and time you choose in the Resume From Date/Time window. Messages already handled after that time are processed again.

A feature that has never run, such as a new one, has no saved position. Its **Resume** drop-down shows only **From Date/Time...** and **From Now**.

Deleting a Feature

Select the feature, click **Delete** (or press Delete), and confirm. The feature's saved position is deleted too.



To keep a feature for later, set **Active** to **No** instead of deleting it. The server then stops and unloads the feature but keeps its settings and saved position; set **Active** back to **Yes** to continue.

This is not the same as suspending a feature: a suspended feature stays loaded and is shown on the Server tab; an inactive one is not.

Importing and Exporting a Feature

The **Import** / **Export** button in a feature window saves the feature's settings to a file or loads them from one. Use it to back up a feature before a risky change, or to copy a feature to another Syslog Watcher 7 installation.

- **Export to File...** saves the settings shown in the window, including changes not yet applied, to a **.feature** or **.json** file.
- **Import from File...** loads a **.feature** or **.json** file into the window. Review the settings, then click **Create** or **Apply**.

You can import only a file of the same feature type as the window; Manager ignores a file of another type. The **Export to Files**, **Export to DB (ODBC)**, **Forward to Syslog Server**, and **Send Emails** windows can also import a file exported from Syslog Watcher 6; Manager asks before converting it.



Exported files can contain connection strings, host names, and passwords. Store them securely, and use **secret strings** instead of plain-text passwords in features.

Data Fields (Optional)

Use this section only when the filter or the templates need extra fields taken from the message text.

- **Regex for extracting fields:** one regular expression whose named groups (**?<FIELD_NAME>...**) become fields such as **{FIELD_NAME}**.
- **Fields:** extra fields whose value is a **format string**.
- **Field Collections:** stored rule sets that pick a rule per message type.

See [Field Extraction](#) for details and examples.

Filter

The feature filter selects the stored messages that the feature processes. It has the same **Severity level**, **Originators**, and **Filter expression** settings as other filters; see [Filtering](#).



Narrow by severity and originators first. They use storage indexes, so the feature reads fewer messages.

Most feature types also have section filters in advanced mode. A message must pass the feature filter **and** a section filter to use that section.

Related Topics

- [Features](#) — feature types and how a feature processes messages
- [Monitoring Features](#) — live status on the Server tab
- [Filtering](#)
- [Message Fields](#) — `{FIELD}` syntax in templates

Monitoring Features

The live status of features is on the [Server tab](#) in Manager. Click **Server Features** in the diagram to show the **Features** table. To change or control features, use the [Server Features](#) window.

The table lists only active features. If the Syslog Watcher Server service is stopped, the table shows **Syslog Server is stopped**.

Features Table

Status	Processing , Suspended , or Failed with the time since the current failure started (Failed ... ago).
Name	Feature name.
Type	Feature type, such as Export to Files or Send Emails .
Last Timestamp	Time of the last syslog message the feature processed successfully.
Messages	Number of messages the feature has processed successfully.
Errors / Recoveries	Number of failures, and number of times the feature recovered from a failure. While the feature is failing, the numbers are red and show when it retries next (retry in ...). For a suspended feature the column shows —.

A second row under a feature shows its last error:

- **Last error [time]: ...** — the feature is running or retrying.
- **Initialization failed [time]: ...** — the feature could not start, for example because of a missing

setting, and the server suspended it.

Reading the Status

Status	Meaning
Processing	The feature is running. Messages grows when matching messages arrive in storage.
Suspended	The feature is loaded but does not read storage. It was suspended, is new, or failed to start (see the error row).
Failed	Reading storage or sending to the destination failed. The feature retries the same message automatically: first after a short delay, then at a longer interval.

Troubleshooting

Symptom	Likely cause
Feature not in the table	Active is No , or the server is stopped. Check the feature in Server Features .
Messages stays at 0 after resume	The filter matches nothing, or the feature was resumed From Now and no new matching messages arrived.
Suspended with Initialization failed	A required setting is missing or invalid, such as the email account or HTTP endpoint. Fix the setting, then resume the feature.
Failed	Read the error row to see what failed.
Errors / Recoveries keeps growing	The destination (mail server, database, syslog server, HTTP endpoint) is unstable. Fix the destination; the feature then catches up from storage.
Collector counters grow, Messages does not	The feature is suspended, its filter excludes the messages, or it is failing (see Failed).

Related Topics

- [Managing Features](#) — suspend, resume, and edit settings
- [Features](#) — how a feature processes messages
- [Collector Monitoring](#) — received and stored messages

Export to Files

Export to Files writes matching syslog messages to text files. Use it to:

- ▶ feed another product that reads only files
- ▶ keep an extra copy of selected logs
- ▶ keep a separate folder for each originator



The feature reads messages from syslog storage, so a slow or failing export never blocks collection (see [How a Feature Processes Messages](#)).

Edit Feature: Export to Files

Feature

Name

Product Integration

Active

Yes

Data Fields (Optional)

Filter

Severity level

< > (0) Emergency - (3) Error

Originators

ALL ORIGINATORS

Filter expression

ALL MESSAGES

File Exporter

Target folder

C:\Integrations\SyslogWatcher

Subfolders template

{ORIGINATOR_ID|EscPATH}

Filename template

{RECEIVED|%Y-%m-%d}.txt

File header

Limit file size

No

Advanced

Line endings

CR+LF (Windows style)

Max open files

100

Close idle files after (s)

10

File Contents

Message to text

<{PRIORITY}>{RAW_MESSAGE}

[Switch to Advanced Mode](#)

[^ Collapse All](#), [v Expand All](#)

Target folder

Path to the folder where the output subdirectories and files will be created.

? Import / Export

✓ Apply

✗ Cancel

Edit Feature: Export to Files

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in Managing Features. This page covers the **File Exporter** section.

File Exporter

Setting	Description
Target folder	Required. Folder where the subfolders and files are created. The Syslog Watcher Server service account must be able to write to it. Click (⋮) to browse (only when managing the local server).
Subfolders template	Optional. Format string for subfolder names. Example: {ORIGINATOR_ID EscFNAME} creates one folder per originator and replaces characters that Windows does not allow in file names.
Filename template	Required. Format string for the file name. Example: {RECEIVED %Y-%m-%d}.txt creates one file per day.

Setting	Description
File header	Optional. Text written once at the start of each new file, for example CSV column names. Files that already have content are not changed.
Limit file size	No (default): files grow without limit; only the filename template starts new files. Yes : start a new file when Maximum size (KB) is reached (default 1000). See Limit File Size and File Names .

The **Advanced** subsection has settings whose defaults suit most cases:

Setting	Description
Line endings	Added after each line: CR+LF (Windows style) (default) or LF (Unix style) . File header uses the same line endings.
Max open files	How many files the server keeps open at once: 1–999, default 100. Set it to 1 so that the server does not keep files locked between writes; this is slower.
Close idle files after (s)	Close a file that has not been written to for this many seconds: 1–3600, default 10.

Templates use [message fields](#) and [date/time modifiers](#), for example `{RECEIVED|%Y-%m-%d}`.



Dates from `{RECEIVED}` use the [server time zone](#), not UTC and not the originator's clock. Use `{RECEIVED_UTC}` for UTC days.

Subfolder and Filename Examples

Paths are under **Target folder** (here `C:\Integrations\SyslogWatcher`). Use `EscFNAME` on any field that can contain characters not allowed in Windows file names. A `/` or `\` in **Subfolders template** creates nested folders.

One file per day for all originators

```
Subfolders: (none)
Filename:   {RECEIVED|%Y-%m-%d}.txt
Result path: C:\Integrations\SyslogWatcher\2026-08-25.txt
```

One folder per originator, one file per day

```
Subfolders: {ORIGINATOR_ID|EscFNAME}
Filename:   {RECEIVED|%Y-%m-%d}.txt
Result path: C:\Integrations\SyslogWatcher\firewall-01\2026-08-25.txt
```

Year and month folders, one file per day

```
Subfolders: {RECEIVED|%Y}/{RECEIVED|%m}
```

```
Filename:      {RECEIVED|%d}.txt
Result path: C:\Integrations\SyslogWatcher\2026\08\25.txt
```

One folder per originator, one file per severity

```
Subfolders:  {ORIGINATOR_NAME|EscFNAME}
Filename:     {SEVERITY}.txt
Result path: C:\Integrations\SyslogWatcher\Core Firewall\Error.txt
```

File Contents

In simple mode, **File Contents** has one **Message to text** template. Example: `<{PRIORITY}>{RAW_MESSAGE}` writes each message as received, including the syslog priority prefix.

Click **Switch to Advanced Mode** to define several **File Content Sections (Add Section)**. Each **File section** has:

- a **Section filter** (blank = **ALL MESSAGES** that passed the feature filter)
- a **Message to text** template

For each message, every section whose filter matches writes one line, in list order. If no section matches, nothing is written for that message.

Use several sections when originators need different output formats: give each section a filter for its originators and the template the reader expects. You can also use sections for optional parts: add a section for each part, with a filter that decides when the part is written.

Formatted Files

Each matching section writes one line, so **Message to text** can produce any line-based format. The examples below are CSV and JSON Lines. Use [escape modifiers](#) so that commas, quotes, and line breaks in the message do not break the format.

Example: CSV

Quote text fields and apply **EscCSV**, which doubles embedded quotes. Put the column names in **File header** so that each new file starts with a header line:

```
Filename:      {RECEIVED|%Y-%m-%d}.csv
File header:   "received","originator","severity","message"
Message to text: "{RECEIVED|%Y-%m-%dT%H:%M:%S%Ez}", "{ORIGINATOR_ID|EscCSV}", "{SEVERITY}", "{MESSAGE|EscCSV}"
```

A line break inside a message still splits the CSV record across several physical lines, even inside quotes. If the reader cannot handle that, use JSON Lines.

Example: JSON Lines

Apply **EscJSON** inside JSON string values so that quotes and line breaks stay on one line:

```
Filename:          {RECEIVED|%Y-%m-%d}.jsonl
Message to text: {{ "received": "{RECEIVED|%Y-%m-%dT%H:%M:%S%Z}", "originator": "{ORIGINATOR_ID|EscJSON}", "severity": "{SEVERITY}", "message": "{MESSAGE|EscJSON}" }}
```



In **Message to text**, a single **{** starts a message field. Write **{{** and **}}** for the literal braces of a JSON object.

Limit File Size and File Names

The output path is **Target folder** + **Subfolders template** + **Filename template**, evaluated for each message.

With **Limit file size** set to **No**, the file name is used as is. The daily template **{RECEIVED|%Y-%m-%d}.txt** produces one file per day:

```
C:\Integrations\SyslogWatcher\2026-08-25.txt
```

With **Limit file size** set to **Yes**, the exporter starts a new file when **Maximum size (KB)** is reached. It adds a three-digit number before the extension: **-000**, then **-001**, **-002**, and so on:

```
C:\Integrations\SyslogWatcher\2026-08-25-000.txt
C:\Integrations\SyslogWatcher\2026-08-25-001.txt
C:\Integrations\SyslogWatcher\2026-08-25-002.txt
```

Each path from the templates has its own numbering (for example, one sequence per originator folder). After a restart, export continues in the highest existing number for that path. Each new part starts with **File header**, if set.

Notes

- If **Target folder** is on a network share, give the Syslog Watcher Server service account (Local System by default) share and NTFS write access, or run the service under an account that has it.

Related Topics

- [Managing Features](#)
- [Message Fields](#)
- [Date/Time Modifiers](#)
- [Escape Modifiers](#)

Export to DB (ODBC)

Export to DB (ODBC) runs SQL commands, usually an **INSERT**, on an ODBC data source for each matching message.



The feature reads messages from syslog storage, so a slow or failing export never blocks collection (see [How a Feature Processes Messages](#)).

Edit Feature: Export to DB (ODBC)

Feature

NameDatabase Copy

ActiveYes

Data Fields (Optional)

Filter [OFF]

ODBC Configuration

ODBC connection stringDSN=MyDatabaseDSN;

Messages per transaction10000

SQL Commands

CommandsINSERT INTO syslog (message) VALUES ('{MESSAGE|EscSQL

Switch to Advanced Mode

^ Collapse All, v Expand All

The 'Export to DB' feature exports incoming syslog messages to an external database via ODBC.

? Import / Export

✓ Apply

✕ Cancel

Edit Feature: Export to DB (ODBC)

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in Managing Features. This page covers the **ODBC Configuration** section.

ODBC Configuration

Setting	Description
ODBC connection string	Required. Used by the Syslog Watcher Server service, not by Manager. Click (⋮) to open the connection string builder (only when managing the local server).

Setting	Description
Messages per transaction	Number of messages combined in one SQL transaction (BEGIN / COMMIT): 0–1,000,000, default 10,000. 0 (shown as OFF) disables transactions; each command commits on its own.

System DSN

The server service runs as **Local System** by default, so it cannot use a User DSN. Create a **System Data Source** (System DSN) instead. If the System DSN option is not available in the builder, restart Manager as Administrator.

The builder lists ODBC drivers and data sources on the computer where Manager runs. When Manager is connected to a remote server, paste a connection string that works on the server, or create the DSN on the server with the 64-bit ODBC Data Source Administrator (%windir%\System32\odbcad32.exe).

SQL Commands

In simple mode, **SQL Commands** has one **Commands** template, usually one **INSERT**. Example:

```
INSERT INTO syslog (message) VALUES ('{MESSAGE|EscSQL}');
```

EscSQL makes the value safe inside an SQL string literal: it doubles single quotes and escapes backslashes, as MySQL expects. For SQL Server, SQLite, and other databases that treat a backslash as a normal character, use **EscSQLANSI** instead; it only doubles single quotes. See [Escape Modifiers](#).

Click **Switch to Advanced Mode** to define several command groups (**Add Commands**). Each **Commands group** has:

- a **Group filter** (blank = **ALL MESSAGES** that passed the feature filter)
- one or more **SQL Commands**

For each message, the commands of every group whose filter matches run, in list order. If no group matches, no SQL runs for that message.

Use several groups when messages need different SQL, for example a different table per originator, or **INSERT** for some messages and **UPDATE** for others. A group can also run extra SQL for some messages only, for example a second **INSERT** into an audit table for severity Error and higher.



The destination table must already exist; see [Destination Table](#).

Destination Table

The feature does not create tables, columns, or indexes. Create them in the database first, then write **Commands** whose column names match.

Do not put **CREATE TABLE** in the feature commands: it would run for every matching message.

There is no required schema. Choose columns for the [fields](#) you need, with types the database can store. Add indexes on the columns you search by, often the received time and the originator.

Example table and a matching insert (SQL Server types; adjust them for your database):

```
CREATE TABLE syslog (  
    received          DATETIME          NOT NULL,  
    originator_id     VARCHAR(64)       NOT NULL,  
    originator_name   NVARCHAR(256)     NULL,  
    severity          SMALLINT          NULL,  
    facility          VARCHAR(32)       NULL,  
    message           NVARCHAR(MAX)     NULL  
);
```

```
INSERT INTO syslog (received, originator_id, originator_name, severity, facility,  
message)  
VALUES (  
    '{RECEIVED|%Y-%m-%d %H:%M:%S}',  
    '{ORIGINATOR_ID|EscSQLANSI}',  
    '{ORIGINATOR_NAME|EscSQLANSI}',  
    {SEVERITY_NUM},  
    '{FACILITY}',  
    '{MESSAGE|EscSQLANSI}'  
);
```

`{RECEIVED|%Y-%m-%d %H:%M:%S}` is the received time in the [server time zone](#), formatted for a datetime column. See [Date/Time Modifiers](#) if the database needs another format. Use a Unicode large-text type for the message text (`NVARCHAR(MAX)` on SQL Server).

Notes

- A large **Messages per transaction** value improves throughput but delays the commit. If the server stops before a commit, those messages are exported again after it restarts.
- The ODBC driver must be 64-bit, like the Syslog Watcher Server service.

Related Topics

- [Managing Features](#)
- [Monitoring Features](#) — database errors show as **Failed**, and the feature retries
- [Message Fields](#)
- [Escape Modifiers](#)

Forward to Syslog Server

Forward to Syslog Server sends matching stored messages to another syslog server or SIEM.



The feature reads messages from syslog storage, so slow or failing forwarding never blocks collection (see [How a Feature Processes Messages](#)).

New Feature: Forward to Syslog Server

Feature

Name Syslog Forwarder

Description Forwards all except DEBUG over secure connection

Active Yes

Data Fields (Optional)

Filter

Severity level (0) Emergency - (6) Informational

Originators ALL ORIGINATORS

Filter expression ALL MESSAGES

Syslog Forwarder

Target server syslog.example.com

Target port 514

Use local interface (optional)

Protocol Syslog over TLS

Messages in stream Use the 'octet counting' algorithm

TLS Options

Send messages As received (no changes)

[^ Collapse All](#), [v Expand All](#)

Name

Short, unique identifier.

? Import / Export Create Cancel

New Feature: Forward to Syslog Server

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in Managing Features. This page covers the **Syslog Forwarder** section.

Destination

Setting	Description
Target server	Required. IPv4 or IPv6 address or host name of the syslog server.
Target port	Destination port: 1–65535, default 514.
Use local interface (optional)	Local IP address to send from. Blank = chosen by Windows.
Protocol	Syslog over UDP (default), Syslog over TCP, or Syslog over TLS.
Messages in stream	TCP and TLS only. How messages are separated in the stream: Use the 'octet counting' algorithm (default, RFC 6587), Separate with \0, Separate with \n, or Separate with \r\n. Use the framing the receiver expects.

TLS Options

Shown for **Syslog over TLS**.

Setting	Description
Protocol version	TLS 1.0, 1.1, 1.2 (default), or 1.3.
Verify server certificate	OFF: Do not verify (default) or ON: Verify certificate . When on, the server certificate must chain to a Windows trusted root or the selected CA, and its name must match Target server . The default lets self-signed test receivers work; turn verification on in production.
Certificate Authority (CA)	Shown when verification is on. Named CA certificate from TLS Certificates . Blank = Windows trusted roots only.
Timeout	Connect, handshake, and I/O timeout in milliseconds: 100–60,000, default 2000.
Certificate	Optional client certificate from TLS Certificates , for receivers that require mutual TLS.
Private key password	Password for a protected private key. Use a secret string .

Send Messages (Format)

Send messages sets how each message is formatted before it is sent:

Option	Result
As received (no changes)	The default. The message as it arrived, with its syslog priority prefix.
Formatted as IETF-syslog (RFC5424)	The message rebuilt with an RFC 5424 header.
Formatted as IETF-syslog + SD:origin (RFC5424 7.2)	The same, plus origin structured data with the original sender's address, so the receiver knows the real originator.
In custom format	Your own template (see below).

With **In custom format**, the **Message Format** section has one **Message template** in simple mode. Example: `<{PRIORITY}>{RAW_MESSAGE}` sends the message as received, including the syslog priority prefix.

Click **Switch to Advanced Mode** to define several **Format Templates (Add Template)**. Each template has:

- a **Template filter** (blank = **ALL MESSAGES** that passed the feature filter)
- a **Message template**

For each message, every template whose filter matches is applied, in list order, and the results are joined into one forwarded message.



If no template matches, an empty message is sent.

Use several templates when originators need different output formats: give each template a filter for its originators. If each template builds a complete message, keep the template filters mutually exclusive so that only one matches. You can also use templates for optional parts: add a template for each part, with a filter that decides when the part is included.

Related Topics

- [Managing Features](#)
- [TLS Certificates](#)
- [Message Fields](#)
- [Date/Time Modifiers](#)

Send Emails

Send Emails sends email alerts for matching syslog messages. Each **Send Emails** feature has its own filter, recipients, and email rules.



The feature reads messages from syslog storage, so a slow mail server never blocks collection (see [How a Feature Processes Messages](#)).


New Feature: Send Emails

Feature

Name

Important Alerts

Active

Yes

Data Fields (Optional)

Filter

Severity level

< > (0) Emergency - (3) Error < >

Originators

ALL ORIGINATORS

Filter expression

ALL MESSAGES

Email Configuration

Email account

Corp Mail Server

Send to

alerts@example.com

Emails (2)

Add Email

Link Down

Send for: {MESSAGE} CONTAINS "Link Down"

Name

Link Down

Filter

{MESSAGE} CONTAINS "Link Down"

Subject

{MESSAGE}[80]

Body

{RAW_MESSAGE}

Email 2

Send for: ALL MESSAGES

Consolidation

ON: Merge multiple alerts into one email

^ Collapse All

v Expand All

Name

Short, unique identifier.

?

Import / Export

✓ Create

✕ Cancel

New Feature: Send Emails

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in [Managing Features](#). This page covers the **Email Configuration** section.

A message must pass the [feature filter](#) before the email rule filters are checked. Put broad conditions (severity, originators) on the feature filter and per-alert conditions on the email rules.

Email Configuration

Setting	Description
Email account	Required. An email account from Server Configuration. If the list shows No email accounts , create an account first.
Send to	Required. Recipients, separated by commas or semicolons. Both <code>user@example.com</code> and <code>Name <user@example.com></code> are accepted.

Email Account

Create SMTP accounts in [Email Accounts \(Server Configuration\)](#).



Click [Test Account](#) on the account before relying on the feature.

Emails (Rules)

Each **Email** in the **Emails** list is a rule: a filter, a subject, and a body. Click **Add Email** to add one (up to 100). The list shows each rule's filter after **Send for**.

Setting	Description
Name	A name that describes the alert, for example Link Down .
Filter	Filter expression for this rule. Blank = ALL MESSAGES that passed the feature filter.
Subject	Format string for the email subject. Example: {ORIGINATOR_ID}: {MESSAGE 80} (the first 80 bytes of the message text).
Body	Format string for the email text. Emails are sent as plain text. Example: {RAW_MESSAGE} .

One syslog message can match several rules. All alerts from that message go into the same email, even if that exceeds **Maximum merged emails**.

Consolidation

Setting	Description
Consolidation	OFF: One email per alert (only with a single email rule) or ON: Merge multiple alerts into one email. With two or more rules, it is always on.
Maximum merged emails	Shown when consolidation is on. Maximum number of alerts in one email: 2–10,000, default 100. Alerts from one syslog message that match several rules can still exceed it.
Email subject	Shown when consolidation is on. Subject of a merged email; {N} is replaced with the number of alerts in it. Default: {N} consolidated emails from Syslog Watcher . Blank = the subject of the first alert.
Delay between emails	Minimum time between emails, in seconds, to reduce the load on the mail server: 0–3600, default 1. 0 = no delay. Alerts are held until the next email is due, not dropped.

Filters and Rules

One Feature or Several

One **Send Emails** feature is enough in most cases. Add another feature for different recipients, or to suspend one set of alerts without stopping the others.

Narrow the Feature Filter

Set severity and originators on the **feature filter**. They use storage indexes. Keep slower tests, such as **{MESSAGE} CONTAINS ...**, in the rule **Filter**, which sees only the messages that passed the feature filter.

Combine Rules That Send the Same Text

If two rules have the same subject and body, use one rule and combine the filters. For example, these two filters:

```
{MSGID} = "LINK-3-UPDOWN"  
{MSGID} = "LINK-3-TOOSMALL"
```

can be one rule:

```
{MSGID} = "LINK-3-UPDOWN" or {MSGID} = "LINK-3-TOOSMALL"
```

Use Filter Lists

When a rule compares a field with many values, a [filter list](#) is easier to maintain and faster than a long **or** chain. Example: `{MSGID} IN "link_events"`

Troubleshooting

If emails do not arrive:

1. Click **Test Account** on the email account to check that Syslog Watcher Server can send email.
2. On the **Server tab**, check the feature status and its error row.
3. Check the feature: **Active** is **Yes**, it is not suspended, **Email account** and **Send to** are set, and there is at least one **Email**.
4. Copy the feature filter (drop-down button on the **Filter** section) and use it in a view tab for a time range that should contain matching messages. Check that the view tab shows them.
5. If these checks pass, contact [technical support](#) with the details and a support data file.

Related Topics

- [Managing Features](#)
- [Monitoring Features](#)
- [Email Accounts](#)
- [Message Fields](#)
- [Filter Expressions](#)
- [Filter Lists](#)

Send HTTP Requests

Send HTTP Requests sends one HTTP/1.1 request for each matching message. Use it for webhooks, ticketing APIs, SMS gateways, and other HTTP integrations.



The feature reads messages from syslog storage, so a slow or failing web service never blocks collection (see [How a Feature Processes Messages](#)).

Edit Feature: Send HTTP Requests

Feature

Name: On-call SMS

Active: Yes

Data Fields (Optional)

Filter

Severity level: (0) Emergency - (3) Error

Originators: ALL ORIGINATORS

Filter expression: ALL MESSAGES

HTTP Request

HTTP endpoint: TextLink

Resource path: /v1/messages

Request Body Sections (1)

HTTP request section

Section filter: {SEVERITY_NUM} = 0

HTTP request section

Section filter: {SEVERITY_NUM} > 0

[Collapse All](#), [Expand All](#)

HTTP endpoint

An HTTP endpoint defines access to a web server. You can create endpoints here: Main Toolbar > Server > Server Configuration...

? Import / Export Apply Cancel

Edit Feature: Send HTTP Requests

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in Managing Features. This page covers the **HTTP Request** section.

HTTP Request

Setting	Description
HTTP endpoint	Required. A named HTTP endpoint from Server Configuration. The endpoint sets the web server address, TLS, authentication, headers, and Request type (POST or PUT). If the list shows No HTTP endpoints , create an endpoint first.
Resource path	Required. Path on the web server; message fields are allowed. Examples: /v1/messages, /api/send-message/{SEVERITY_NUM}. Do not put spaces or line breaks in the path; use {FIELD EscURL} for field values.

Request Body

In simple mode, **Request Body** has one **HTTP request body** template. Example: `{MESSAGE|70}` sends the first 70 bytes of the message text.

Click **Switch to Advanced Mode** to define several **Request Body Sections (Add Request Section)**. Each **HTTP request section** has:

- a **Section filter** (blank = **ALL MESSAGES** that passed the feature filter)
- an **HTTP request body** template

For each message, every section whose filter matches is applied, in list order, and the results are joined into one request body. The feature still sends one request per message, not one per section.



If no section matches, the request is sent with an empty body.

Use several sections when originators need different request formats, or when the body depends on severity, for example a high-priority SMS for Emergency and a standard SMS for Alert to Error. If each section builds a complete JSON object, keep the section filters mutually exclusive so that only one matches. You can also use sections for optional parts: add a section for each part, with a filter that decides when the part is included.

JSON Body

For a JSON body, put message fields inside JSON string values and apply **EscJSON**, so that quotes, backslashes, and line breaks in the message do not break the JSON:

```
{{"from":"{ORIGINATOR_ID|EscJSON}","sev":{SEVERITY_NUM},"msg":"{MESSAGE|EscJSON}"}}
```



In **HTTP request body**, a single `{` starts a message field. Write `{{` and `}}` for the literal braces of a JSON object.



Check the endpoint and the body format first with [Send Test Request](#) on the endpoint.

Notes

- Requests are sent from the Syslog Watcher Server computer, not from Manager. DNS, the firewall, and TLS must work there.
- A response status outside 200–299, or a connection error, marks the feature **Failed** on the [Server tab](#). The feature retries the same message; it does not skip it.

Related Topics

- [Managing Features](#)
- [HTTP Endpoints](#)

- [Message Fields](#)
- [Escape Modifiers](#)

Execute Program/Script

Execute Program/Script starts a program for each matching message and passes message fields as command-line parameters. Use it to run:

- ▶ a PowerShell or batch script
- ▶ a vendor CLI
- ▶ an in-house tool that has no syslog, file, or HTTP interface



The feature reads messages from syslog storage, so a slow or failing program never blocks collection (see [How a Feature Processes Messages](#)).

Edit Feature: Execute Program/Script

Feature

Name

Ops Notification

Description

Run Notify-Ops.ps1 for hight-severity events

Active

Yes

Data Fields (Optional)

Filter

Severity level

< > (0) Emergency - (3) Error

Originators

ALL ORIGINATORS

Filter expression

ALL MESSAGES

Program Configuration

Executable file

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Work folder

C:\Integrations\SyslogWatcher\scripts

Username

Password

Success exit code

Command Line Parameters (1)

Add Parameters

Parameters

-File C:\Integrations\SyslogWatcher

^ Collapse All

v Expand All

Name

Short, unique identifier.

?

Import / Export

Apply

Cancel

Edit Feature: Execute Program/Script

The common [Feature](#), [Data Fields](#), and [Filter](#) sections are described in Managing Features. This page covers the **Program Configuration** section.

Program Configuration

Setting	Description
Executable file	Required. Path of the program on the server computer. Click (⋯) to browse (only when managing the local server).
Work folder	Working folder for the process. Blank = the working folder of the Syslog Watcher Server service.
Username	Windows account that starts the process: DOMAIN\user , user@domain , or a local name. Blank = the Syslog Watcher Server service account (Local System by default).
Password	Password for Username ; ignored when Username is blank. Use a secret string instead of the password itself.
Success exit code	Blank: any exit code means success. A number: only that exit code means success.

The process runs without a window. The feature waits for it to exit, up to 10 seconds, before it processes the next message. If the program does not exit in time, the feature ends it. If the program cannot start, times out, or returns an exit code other than **Success exit code**, the feature is marked **Failed** and retries the same message.

Command Line Parameters

In simple mode, **Command Line Parameters** has one **Parameters** template. The command line is the quoted **Executable file** path followed by the parameters. Example:

```
-File C:\Integrations\SyslogWatcher\scripts\Notify-Ops.ps1 {ORIGINATOR_ID|EscCMD}  
{MESSAGE|70|EscCMD}
```

EscCMD escapes a value for the Windows command line. It adds double quotes only when the value contains spaces or ", so do not put extra quotes around the field: **{MESSAGE|EscCMD}** is enough.



Without **EscCMD**, message text is inserted into the command line as is, and a crafted syslog message can add its own parameters. Use **EscCMD** on every message field that is not fully under your control.

Click **Switch to Advanced Mode** to define several parameter groups (**Add Parameters**). Each group has:

- a **Filter** (blank = **ALL MESSAGES** that passed the feature filter)
- a **Parameters** template

For each message, the parameters of every group whose filter matches are joined, in list order, into one command line. The program still starts once per message.



If no group matches, the program starts without parameters.

Use several groups when originators need different parameters, or when some parameters apply only to some messages, for example an extra flag for severity Error and higher.

Notes

- To run a script (`.ps1`, `.bat`, `.cmd`), set **Executable file** to the interpreter (`powershell.exe`, `cmd.exe`) and put the script path in the parameters.
- Local System cannot see mapped drive letters; use UNC paths or run the process under another account.
- A broad filter can start many processes; keep the feature filter narrow.

Related Topics

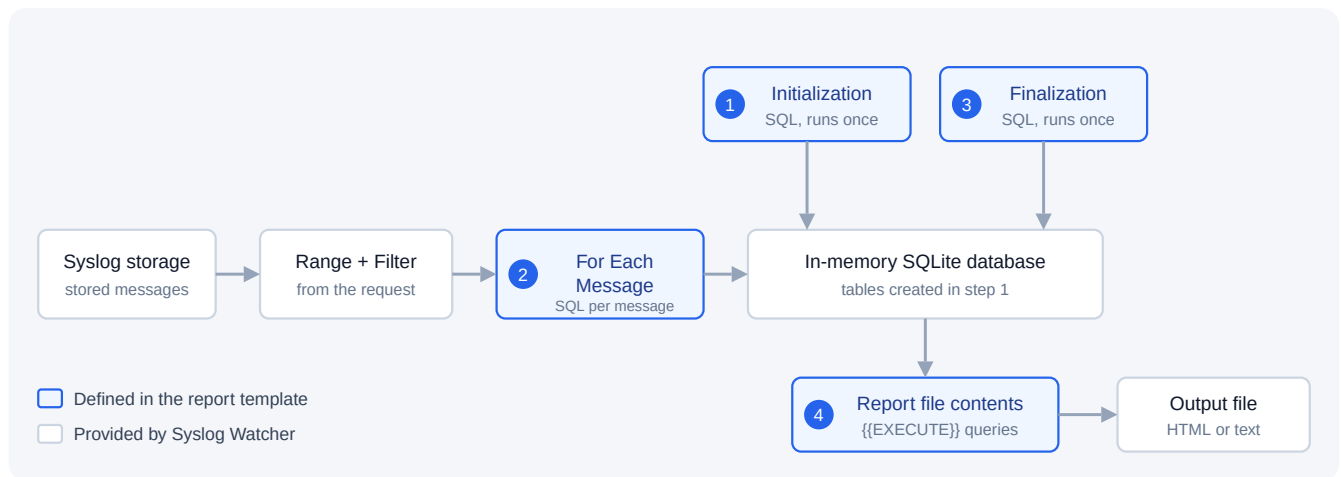
- [Managing Features](#)
- [Message Fields](#)
- [Escape Modifiers](#)

Syslog Reports

A **syslog report** analyzes messages that are already in syslog storage and writes the result to an HTML or text file. Use reports for counts, top lists, and trends over hours, days, or months. A [report template](#) defines what a report collects and how the file looks.

A report only reads syslog storage. The collector keeps writing new messages while a report runs.

How a Report Is Built



How a report is built (simplified schematic)

You start a report with a request: a template, a message time range, and an optional filter. Syslog Watcher then:

1. Creates an empty in-memory SQLite database and runs the template's **Initialization** SQL once.
2. Reads each stored message in the range that passes the request filter and runs every **For Each Message** command whose **Execute for** expression matches.
3. Runs the **Finalization** SQL once.
4. Fills **Report file contents** with the results of its `{{EXECUTE}}` queries and writes the output file.

When the report finishes, the database is discarded and only the output file is kept.

Generate Now or Schedule

	Generate Report Now	Scheduled report
Generated by	Manager, on this computer	The Syslog Watcher Server service
While it runs	Manager is unavailable until the report is done	You can keep working in Manager
Output file	Saved where you choose	Saved in the server's Output folder
Repeats	No	Optional: recurring, weekly, or monthly

Reports Button

In the **Messages** section of the main toolbar, click  **Reports**. The drop-down shows only the items that work in the current connection mode:

Item	Local server	Remote server	No server (storage folder only)
Generate Report Now...	✓	—	✓
Show Scheduled Reports	✓	✓	—
 Manage Report Templates...	✓	✓	✓

Related Topics

- [Scheduled Reports](#)
- [Report Templates](#)
- [Template example: Simple Counters](#)

Generate a Report Now

Generate Report Now... runs a report in Manager on this computer and saves the file where you choose. Use it to test a new template or to run a one-off analysis. For reports that repeat, or when Manager is connected to a remote server, [schedule the report](#) instead.

Generate a Report

1. In the **Messages** section of the main toolbar, click  **Reports** → **Generate Report Now...**
2. In the **Generate Report** window, select a **Report template**.
3. Set the message **Range** and, optionally, a **Filter**; see [Generate Report Window](#).
4. Click **Generate**.
5. When the **Generating Report...** window closes, choose where to save the file. The suggested name comes from the template's [Filename template](#). Manager opens the file after saving it.



Manager is unavailable while the report is generated. To end it early, click **Stop** in the **Generating Report...** window. No file is saved.

Generate Report Window

Setting	Description
Report template	Templates from the installation are listed as Installation: <name> .

Setting	Description
Include folders	Optional folders for <code>{{INCLUDE}}</code> files, one path per line. They are searched after the ReportResources folder in the installation directory. Scheduled reports use the server's Include folders instead.
Messages → Range	Time range of the stored messages to analyze; see Messages Range .
Filter	Optional; see Filter . Blank means all messages in the range.

Messages Range

Range	Description
TODAY	The current calendar day.
YESTERDAY	The previous calendar day.
RECENT	The Last N minute(s), hour(s), or day(s), up to now. For a scheduled report that runs Once , the range ends at the run time.
ENTIRE STORAGE	Every message in syslog storage.
CUSTOM	Fixed From and Until date and time.

Filter

The filter has the same parts as a view tab filter: severity levels, originators or an originator group, and a **Filter expression**. See **Filtering**.



Narrow by severity and originators first. Syslog Watcher skips other messages while reading syslog storage, but tests the **Filter expression** on each message it reads.

Related Topics

- [Syslog Reports](#)
- [Scheduled Reports](#)
- [Report Templates](#)

Scheduled Reports

Scheduled reports are generated by the **Syslog Watcher Server** service, not by Manager. Use them for reports that repeat and when Manager is connected to a remote server. The **Scheduled Reports** tab lists upcoming reports and the history of finished ones.

Schedule a Report

1. In the **Messages** section of the main toolbar, click  **Reports** → **Show Scheduled Reports**.
2. On the **Scheduled Reports** tab, click + **Schedule New Report...**
3. In the **Schedule Report** window, select a **Report template**.

4. Select a **Run** option and fill in its time settings; see [Run](#).
5. Optionally set a **Filter**; see [Filter](#).
6. Click **Schedule**.

The report appears on the tab with the status **Scheduled**. When it is **Completed**, the file is in the server's [Output folder](#); click  **Open Report** to open it.



Reports are generated only while [Generate on a schedule](#) is on. It is on by default.

Schedule Report Window

Setting	Description
Report template	Templates from the installation are listed as Installation: <name> .
Run	When the report runs; see Run . The time settings under it depend on the option you select.
Messages → Range	Time range of the stored messages; see Messages Range . Shown only for As soon as possible and Once ; the other choices set the range themselves. TODAY and YESTERDAY are not offered here.
Filter	Optional; see Filter .

Run

Value	Description
As soon as possible	Runs as soon as the server can start it. Messages sets the range.
Once	Runs once, at the date and time in At . Messages sets the range.
Recurring	Runs at First at , then again after each Repeat every interval. Each run covers the interval that has just ended; the first run covers the interval before First at .
Weekly	Runs at midnight on the weekday in Run on and covers the previous 7 days. If you schedule it on that weekday, the first run is on the same weekday next week.
Monthly	Runs at midnight on the day in Run on (month day) (1–28) and covers the time since the same day of the previous month.



If a **Recurring**, **Weekly**, or **Monthly** report ends with **Error**, it is not scheduled again. Fix the cause and use [Reschedule...](#) to restart it.

Scheduled Reports Tab

In the **Messages** section of the main toolbar, click  **Reports** → **Show Scheduled Reports**.

Toolbar

+ Schedule New Report...	Schedule a new report; see Schedule a Report .
✎ Edit...	Change a report that has not started; see Edit a Report .
🔄 Reschedule...	Schedule a finished, failed, or canceled report again; see Reschedule a Report .
Delete / Cancel	Delete a finished report, or cancel one that has not started; see Cancel or Delete .
Show reports for:	How far back the list goes: Last 3 days to Last 365 days .
📄 Open Report	Open the file of a Completed report; see Open a Report .

Buttons that your [role](#) does not allow are unavailable.

Columns

Column	Description
Date/Time	When the report runs or ran.
Status	Scheduled , ...processing... , Completed (green row), Error (red row), or Canceled .
Report template	Template name; installation templates show as Installation: <name> .
Filter	✓ when the report has a filter, — when it has none.
Range	Message range: start, end, and length, or ENTIRE STORAGE .
Repeat	Every <interval>, Weekly (<weekday>), Monthly (on <day>), or — for a single report.
Messages	Number of messages analyzed; — before the report starts.
Result	For a Completed report, the file path; click it to open the file. For an Error , the error message. While the report runs, its speed in msg/s.

Edit a Report

✎ **Edit...** is available for **Scheduled** reports. It opens the **Edit Scheduled Report** window, where you can change:

- **Report template** and **Filter**
- **Messages** range, for **As soon as possible** and **Once**
- **At**, for **Once**

Run and its schedule settings cannot be changed. To change them, cancel the report and use

Reschedule...

Reschedule a Report

Select a **Completed**, **Error**, or **Canceled** report and click  **Reschedule...** The **Schedule Report** window opens with that report's settings. Change what you need and click **Schedule**. This adds a new report; the old row stays in the history.

Cancel or Delete

- **Cancel** (for **Scheduled** reports) stops the report from running. The row stays with the status **Canceled**.
- **Delete** (for finished reports) removes the row from the history. For a **Completed** report it also deletes the file.

Both ask for confirmation. A report that is **...processing...** cannot be canceled.

Open a Report

Select a **Completed** report and click  **Open Report**, double-click the row, or click the file path in **Result**.

- Local server: Manager opens the file in the server's **Output folder**.
- Remote server: Manager downloads the file, asks where to save the copy, and opens it.

Server Configuration

In the **Server** section of the main toolbar, click  **Server** →  **Server Configuration...**, then select **Syslog Reports**.

Setting	Description
Generate on a schedule	Turns scheduled report generation on or off. On by default. When it is off, the settings below are hidden.
Concurrent tasks	How many reports can be generated at the same time (1–9, default 1). Other due reports stay Scheduled until a task is free.
Include folders	Optional folders for {{INCLUDE}} files, one path per line. They are searched after the ReportResources folder in the installation directory.
Output folder	Folder on the server computer for report files. Required when Generate on a schedule is on.
Keep reports (days)	How long finished reports and their files are kept (1–9999, default 30). Older ones are deleted automatically.

Related Topics

- [Syslog Reports](#)
- [Generate a Report Now](#)

- [Report Templates](#)
- [Remote Access](#)

Report Templates

A **report template** defines what a report collects and what it writes: SQL commands that fill an in-memory database, and the text or HTML of the output file. See [How a Report Is Built](#) for the order in which the parts run.

Templates are saved in syslog storage, so every user of the storage shares them. The installation also includes read-only templates, listed as **Installation**.

Report Templates Window

In the **Messages** section of the main toolbar, click  **Reports** →  **Manage Report Templates...**

Add a Template

1. Click **Create New**, or select a template and click **Duplicate** to start from a copy.
2. Fill in the [template settings](#).
3. Click **Create**.

Name is required and must be unique in syslog storage. To change an **Installation** template, duplicate it and edit the copy.

Edit a Template

Select a **Syslog Storage** template, click **Edit...**, change the settings, and click **Apply**.



Scheduled reports find their template by name when they run. If you rename or delete a template, its scheduled reports end with **Error**.

Delete a Template

Select a **Syslog Storage** template, click **Delete**, and confirm. **Installation** templates cannot be deleted.

Template Settings

Collecting Data

Initialization (SQL commands)

Runs once, before the first message. Create tables, indexes, and triggers here, and insert starting rows.

These fields are replaced before the SQL runs:

- **{FROM}** and **{TO}** — start and end of the message range, in server time. Without a modifier the format is `2026-10-10T08:00:00`; add a [date/time modifier](#) after `|` for another format, for example `{FROM|%Y-%m-%d %H:%M:%S}`.
- **{SAMPLING_INTERVAL}** — a time step that suits the length of the range, as an SQLite date modifier: `+1 day` (more than 5 days), `+01:00:00` (more than 2 hours), `+00:01:00` (more than 2 minutes), or `+00:00:01`.

To compare times in SQL, use them as numbers: **{FROM|%Q}** and **{TO|%Q}** here, and **{RECEIVED|%Q}** in [For Each Message](#). All three are server time in microseconds, rounded down to whole seconds, so you can compare them directly (see **%Q**).

Example:

```
CREATE TABLE Counters (Name TEXT PRIMARY KEY, Value INTEGER);
INSERT INTO Counters (Name, Value) VALUES ('Keyword1', 0);
```

For Each Message

Click **Add Commands** to add a command. Commands run in list order; use the buttons next to a command to delete it or move it up or down.

Setting	Description
SQL Commands	SQL to run for each message that passes Execute for . Can include message fields . Apply EscSQL to values taken from syslog text.
Execute for	Optional filter expression . Blank means all messages that passed the request filter.

{SAMPLED_TIMESTAMP} in the SQL becomes the message’s **{RECEIVED}** time rounded down to the sampling step (see **{SAMPLING_INTERVAL}** above), for example `2026-10-10T08:00:00` with a 1-hour step. Use it to count messages per hour or per day.

Finalization (SQL commands)

Runs once, after the last message. Combine and sort the collected rows for output.

These fields are replaced before the SQL runs: **{FROM}**, **{TO}**, **{SAMPLING_INTERVAL}**, **{N}** (number of messages that passed the request filter), and **{BYTES}** (total size of those messages).

Output File

Filename template

Name of the report file, for example:

```
Counters-{GENERATED|%Y-%m-%dT%H-%M-%S}.html
```

{GENERATED} is the time the report is generated; add a date/time modifier after `|` as above. Characters

that are not allowed in Windows file names are replaced with `_`.

- **Generate Report Now...** suggests this name in the save dialog.
- Scheduled reports save the file under this name in the server's [Output folder](#); any folder part of the name is ignored.

Report file contents

The text or HTML of the output file. It is filled in after finalization, in this order:

1. `{{INCLUDE file}}` is replaced with the contents of that file.
2. The fields `{FROM}`, `{TO}`, `{GENERATED}`, `{N}`, `{BYTES}`, and `{SAMPLING_INTERVAL}` are replaced.
3. Each `{{EXECUTE ...}}` block is replaced with query results.

Because includes come first, an included file can contain fields and `{{EXECUTE}}` blocks too.

To query the in-memory database:

```
{{EXECUTE SELECT Name, Value FROM Counters ORDER BY Value DESC;}}  
  <tr><td>{0}</td><td>{1}</td></tr>  
{{END}}
```

The text between the query and `{{END}}` is repeated for each result row. `{0}`, `{1}`, ... are the columns of the row, counted from 0. The values are escaped automatically; see [Escaping in the Report File](#). If a query fails, that block and all blocks after it are left in the file unprocessed.

To include a file, give its name or a path relative to an include folder:

```
{{INCLUDE header.html}}
```

Syslog Watcher looks for the file in the [ReportResources](#) folder in the installation directory, then in the [Include folders](#) of the Generate Report window or, for scheduled reports, in the [server's Include folders](#). If the file is not found, the `{{INCLUDE}}` is removed.

Escaping in the Report File

When an `{{EXECUTE}}` block prints the values `{0}`, `{1}`, ..., it escapes them automatically:

- `&`, `<`, `>`, `"`, and `'` become HTML codes, as with the [EscHTML](#) modifier;
- each `\` is doubled, so a value is also safe inside a JavaScript string, for example `'{0}'` in a chart script.

In the SQL commands, escape values for SQL only, as the **Installation** templates do:

```
INSERT INTO Originators (OrigID, OrigName) VALUES ('{ORIGINATOR_ID|EscSQL}',  
'{ORIGINATOR_NAME|EscSQL}');
```

Do not add `EscHTML` there. The value would be escaped twice, and readers would see the codes instead of the characters: `<b>` is stored as `<b>`, printed as `&lt;b&gt;`, and shown in the browser as `<b>`.



The same escaping applies to text reports, so a text file shows `&` as `&` and `\` as `\\`.

Related Topics

- [Syslog Reports](#)
- [Template example: Simple Counters](#)
- [Template example: Advanced Counter](#)
- [Date/Time Modifiers](#)
- [Escape Modifiers](#)

Template Examples

Simple Counters

Count how many stored messages contain each keyword.

Initialization (SQL commands)

```
CREATE TABLE Counters (Name TEXT PRIMARY KEY, Value INTEGER);
INSERT INTO Counters (Name, Value) VALUES
('Keyword1', 0),
('Keyword2', 0);
```

For Each Message

Add two commands, one per keyword.

SQL Commands:

```
UPDATE Counters SET Value = Value + 1 WHERE Name = 'Keyword1';
```

Execute for:

```
{MESSAGE} CONTAINS "Keyword1"
```

Repeat for `Keyword2`.

Finalization is not required.

Filename template

```
Counters-{GENERATED|%Y-%m-%dT%H-%M-%S}.html
```

Report file contents

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Syslog report: Counters</title>
  </head>
  <body>
    <h1>Syslog report: Counters</h1>
    <p>{FROM|%F %T} - {TO|%F %T}</p>
    <ul>
      <li>Keyword1:
        {{EXECUTE SELECT Value FROM Counters WHERE Name='Keyword1';}}
        {0}
        {{END}}
      </li>
      <li>Keyword2:
        {{EXECUTE SELECT Value FROM Counters WHERE Name='Keyword2';}}
        {0}
        {{END}}
      </li>
    </ul>
  </body>
</html>
```

Advanced Counter

Count how often each value appears when messages contain text such as **IP=192.168.1.1**.

Initialization (SQL commands)

```
CREATE TABLE Vals (Val TEXT PRIMARY KEY, Counter INTEGER DEFAULT 0);
```

Data Fields

Under **Fields**, click **Add Field** and set:

- **Field name:** **IP**
- **Field format:** **{MESSAGE| r/IP=(\S+)/}**

See [Regular Expression](#) modifiers.

For Each Message

Add two commands and leave **Execute for** blank, so they run for all messages that passed the request filter.

First command:

```
INSERT OR IGNORE INTO Vals (Val) VALUES ('{IP|EscSQL}');
```

Second command:

```
UPDATE Vals SET Counter = Counter + 1 WHERE Val = '{IP|EscSQL}';
```

Always apply [EscSQL](#) to values taken from syslog text.

Finalization is not required.

Filename template

```
AdvCounter-{GENERATED|%Y-%m-%dT%H-%M-%S}.html
```

Report file contents

```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8">
    <title>Syslog report: Advanced Counter</title>
    <style>td { border: 1px solid black; }</style>
  </head>
  <body>
    <h1>Syslog report: Advanced Counter</h1>
    <p>{FROM|%F %T} - {TO|%F %T}</p>
    <table>
      <thead><tr><th>IP</th><th>Counter</th></tr></thead>
      <tbody>
        <tr>
          <td>TOTAL</td>
          <td style="text-align: end;">{{EXECUTE SELECT SUM(Counter) FROM
Vals;}}{{0}}{{END}}</td>
        </tr>
        {{EXECUTE SELECT * FROM Vals ORDER BY Counter DESC;}}
        <tr>
          <td>{0}</td>
          <td style="text-align: end;">{1}</td>
        </tr>
        {{END}}
      </tbody>
    </table>
  </body>
</html>
```

```
</tbody>
</table>
</body>
</html>
```



In the request [Filter](#), narrow severity and originators to those that log **IP=** values, so fewer messages are read.

Licenses, Updates, Support

This section explains Syslog Watcher licenses, how to update or migrate Syslog Watcher, and how to contact EZ5 technical support.

Licenses

A license sets how many originators the collector accepts and how many messages per hour it stores. Several licenses can be installed on a Syslog Watcher Server, but only the **selected** license applies. Without a valid selected license, the Free License applies: up to 3 originators and 5000 messages per hour.

- [License Management](#): install, select, and uninstall licenses, online or offline.
- [Evaluation License](#): try a paid license for a limited time.

Updates and Migration

- [Product Updates](#): check for newer versions and update the server and remote Managers.
- [Migrate from Version 6](#): move the Syslog Watcher 6 configuration and license to Syslog Watcher 7.

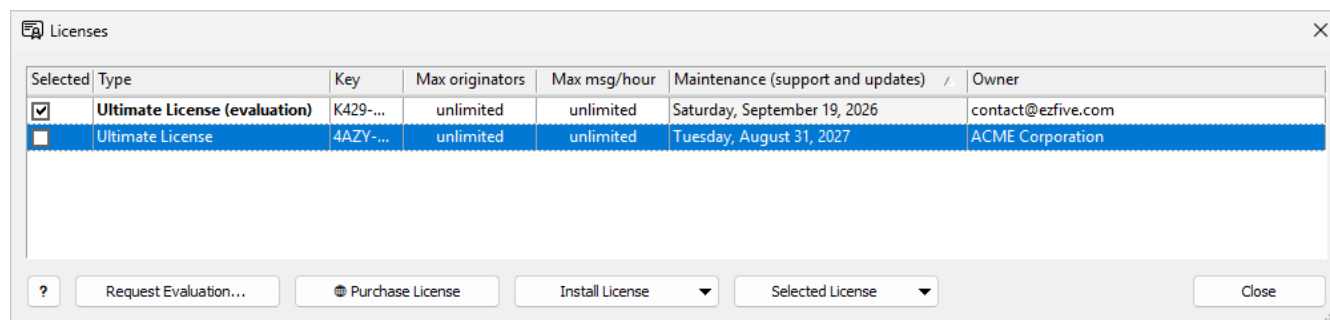
Support

- [Technical Support](#): the support code and the support data file to send with a ticket, and the online and offline User Guide.

License Management

Use the **Licenses** window to install, select, and uninstall licenses on the Syslog Watcher Server. Several licenses can be installed at once, but only the selected one applies. If no license is selected, the Free License applies: up to 3 originators and 5000 messages per hour.

In the **Server** section of the main toolbar, click  **Licenses**.

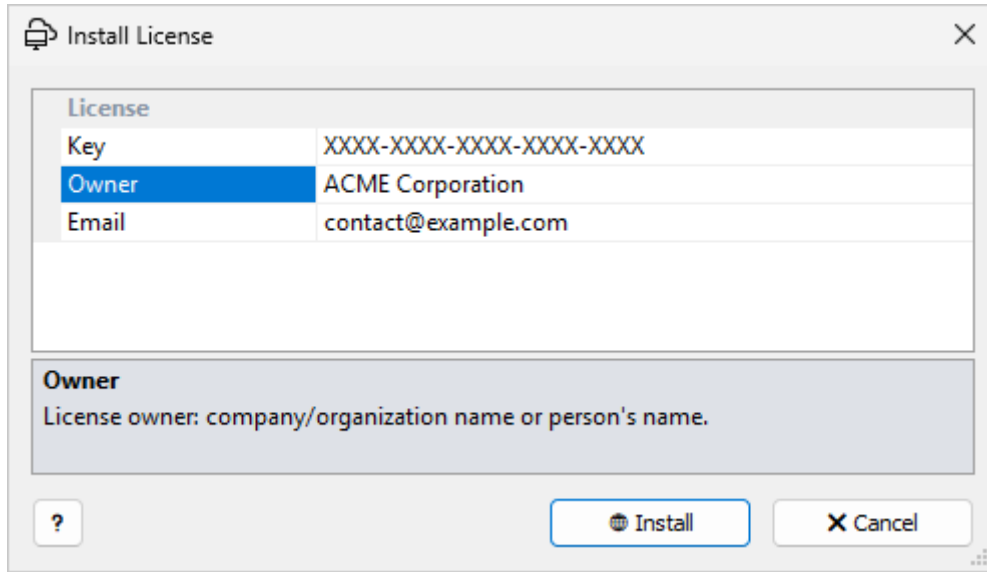


Licenses window

To try a paid license first, see [Evaluation License](#).

Install a License

1. Click **Install License** → **License Key...**
2. Fill in the **Install License** window:



Install License window

- Key** The purchased license key, in the form **XXXX-XXXX-XXXX-XXXX-XXXX**.
- Owner** Company, organization, or person.
- Email** Used for technical support and notifications.

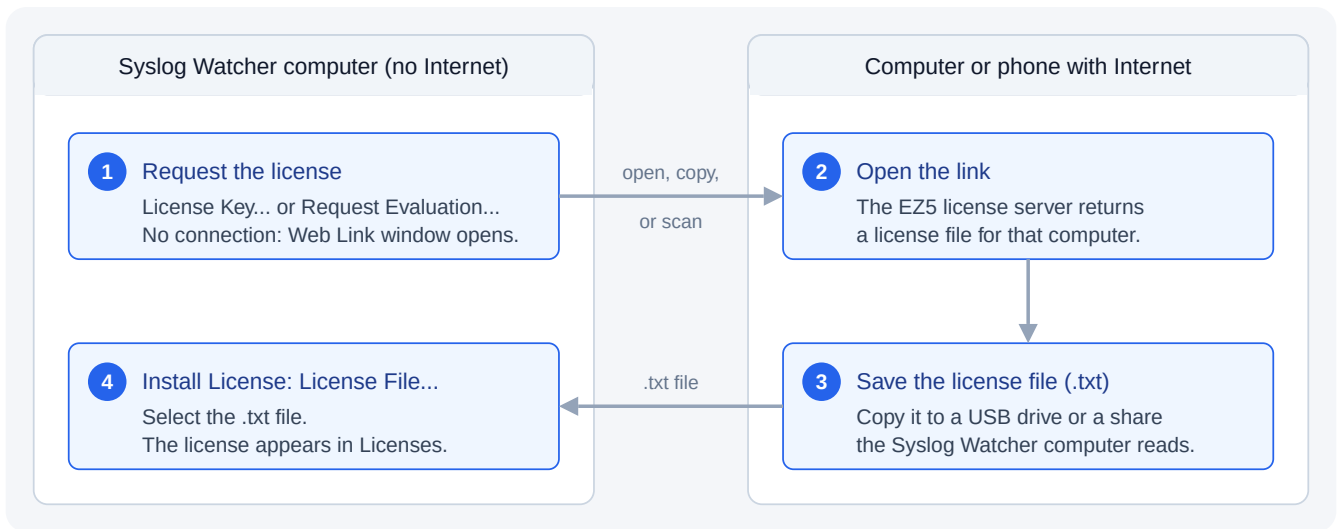
3. Click  **Install**.

Manager sends the request to the EZ5 license server and installs the license it returns. If no other license is selected, the new license is selected automatically; otherwise, [select it](#).

If the license server cannot be reached, see [Offline Installation](#).

Offline Installation

When the license server cannot be reached, Manager opens a **Web Link** window with a request link. This happens with **License Key...**, **Reinstall License...**, and [Request Evaluation....](#)



Offline installation (simplified schematic)

1. Get the request link to a computer or phone with Internet access, using one of the **Web Link** window buttons:
 - **Open Link** opens the link in the default browser on this computer.
 - **Copy Link** copies the link.
 - **Save Link** saves the link to a **.url** file.
 - **Link in QR code** shows the same link for a phone camera.
2. Open the link. The license server returns a license file (**.txt**).
3. Copy the file to the Syslog Watcher computer, for example with a USB drive or a network share.
4. Click **Install License** → **License File...**, select the **.txt** file, and click **Open**. Manager installs the file without contacting the license server.



A license file works only on the Syslog Watcher Server computer where the request link was created.

Select a License

Check **Selected** in the license row, or double-click the row. Only one license can be selected; its **Type** is shown in bold.



A selected license that is **(expired)** or **(inactive)** gives only the Free License limits. A license is inactive when its maintenance ended before this Syslog Watcher version was released; **renew maintenance** to use it.

Reinstall a License

Reinstall License... installs a paid license again using only its key. Use it to get the updated license from the license server, for example after the maintenance period is extended or the license type is changed.

1. Highlight the license row.

2. Click **Selected License** → **Reinstall License...**
3. Enter the license **Key**.
4. Click  **Reinstall**.

If the license server cannot be reached, see [Offline Installation](#).

Uninstall a License

Highlight the license row, then click **Selected License** → **Uninstall License...**

- Paid license: enter the **Key** used to install it and click  **Uninstall**. If the license server cannot be reached, a **Web Link** window opens.
- Evaluation license: removed immediately, without a key or confirmation.



When the selected license is uninstalled, no other license is selected automatically. The Free License applies until you [select another license](#).

Purchase, Upgrade, or Renew

-  **Purchase License**: the Syslog Watcher order page.
- For a paid license, **Selected License** → **Upgrade License** or **Renew Maintenance**: the upgrade or renewal page for that license.

Each command opens a **Web Link** window with a link to the page. Click **Open Link** to open it in the browser, or use **Copy Link** or the QR code to open it on another device.

After an upgrade or a maintenance renewal, [reinstall the license](#) to apply the changes.

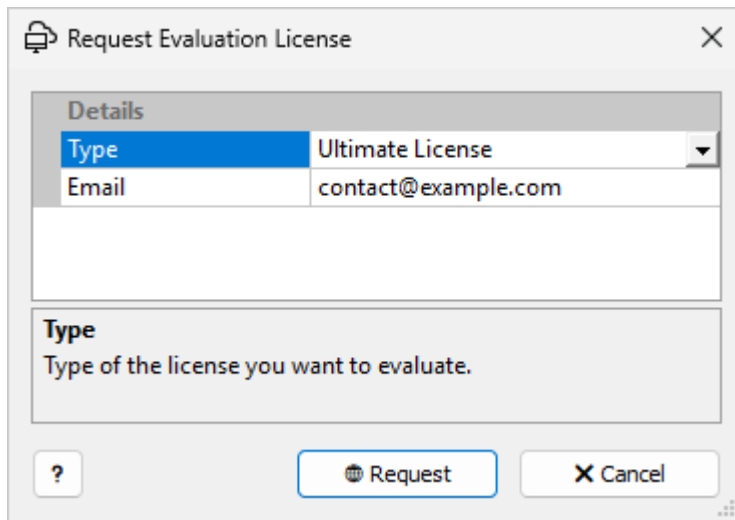
Related Topics

- [Evaluation License](#)
- [Technical Support](#)
- [Syslog Originators](#)

Evaluation License

An evaluation license lets you try a paid Syslog Watcher license for a limited time.

1. In the **Server** section of the main toolbar, click  **Licenses**.
2. Click **Request Evaluation...**
3. Fill in the **Request Evaluation License** window:



The 'Request Evaluation License' window contains a 'Details' section with a 'Type' dropdown menu set to 'Ultimate License' and an 'Email' field containing 'contact@example.com'. Below this is a text area labeled 'Type' with the instruction 'Type of the license you want to evaluate.' At the bottom are three buttons: a help button '?', a 'Request' button with a globe icon, and a 'Cancel' button with an 'X' icon.

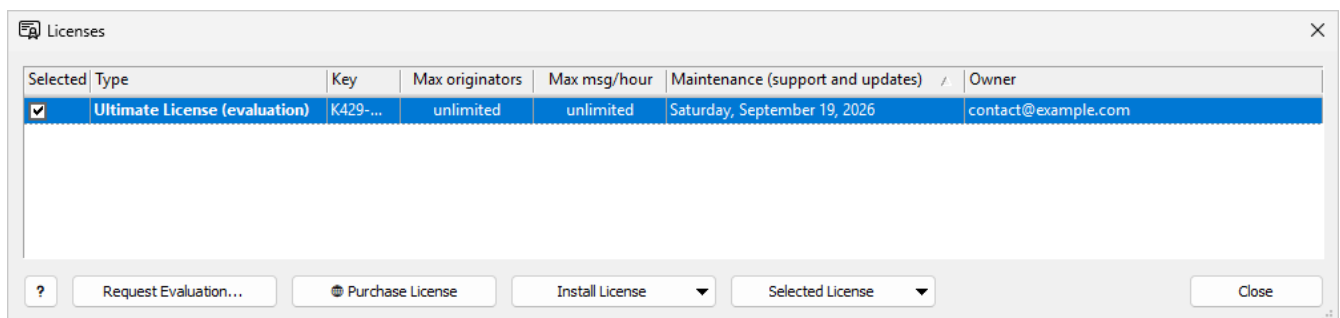
Request Evaluation License window



Email is required: if the license cannot be obtained online, EZ5 sends the evaluation license to this address.

4. Click  **Request**.

When the license server can be reached, the evaluation license is installed. If no other license is selected, it is selected automatically; otherwise, [select it](#). The **Type** column shows the edition with **(evaluation)**, and the **Maintenance (support and updates)** column shows the date the evaluation ends.



Selected	Type	Key	Max originators	Max msg/hour	Maintenance (support and updates)	Owner
☒	Ultimate License (evaluation)	K429-...	unlimited	unlimited	Saturday, September 19, 2026	contact@example.com

Below the table are buttons for '?', 'Request Evaluation...', 'Purchase License' (with a globe icon), 'Install License' (with a dropdown arrow), 'Selected License' (with a dropdown arrow), and 'Close'.

Licenses window

No Connection to the License Server

If the license server cannot be reached, a **Web Link** window opens with a request link; see [Offline Installation](#).

When the Evaluation Ends

The **Type** column shows **(expired)**, and the Free License limits apply: up to 3 originators and 5000 messages per hour. Install and select a purchased license to continue with the full edition.

To remove an evaluation license, highlight it and click **Selected License** → **Uninstall License...** It is removed immediately, without a key or confirmation.

Related Topics

- [License Management](#)
- [Technical Support](#)

Product Updates

The **Syslog Watcher Updates** window lists newer Syslog Watcher versions. Manager also checks for updates when it starts, unless **Check for updates** is off in [Manager Settings](#).

Check for Updates

1. In the **General** section of the main toolbar, click  **Updates**.
2. In the list, select a version to see its changes below the list.
3. To get a version, click **Download Page** to open the download website.

If Manager cannot reach the update server, it shows a warning. On a computer without Internet access, check ezfive.com/syslog-watcher/downloads/ from another computer and copy the installer over.

Install an Update

1. Run the new installer on the server computer.
2. Run it on every other computer that has Manager installed.

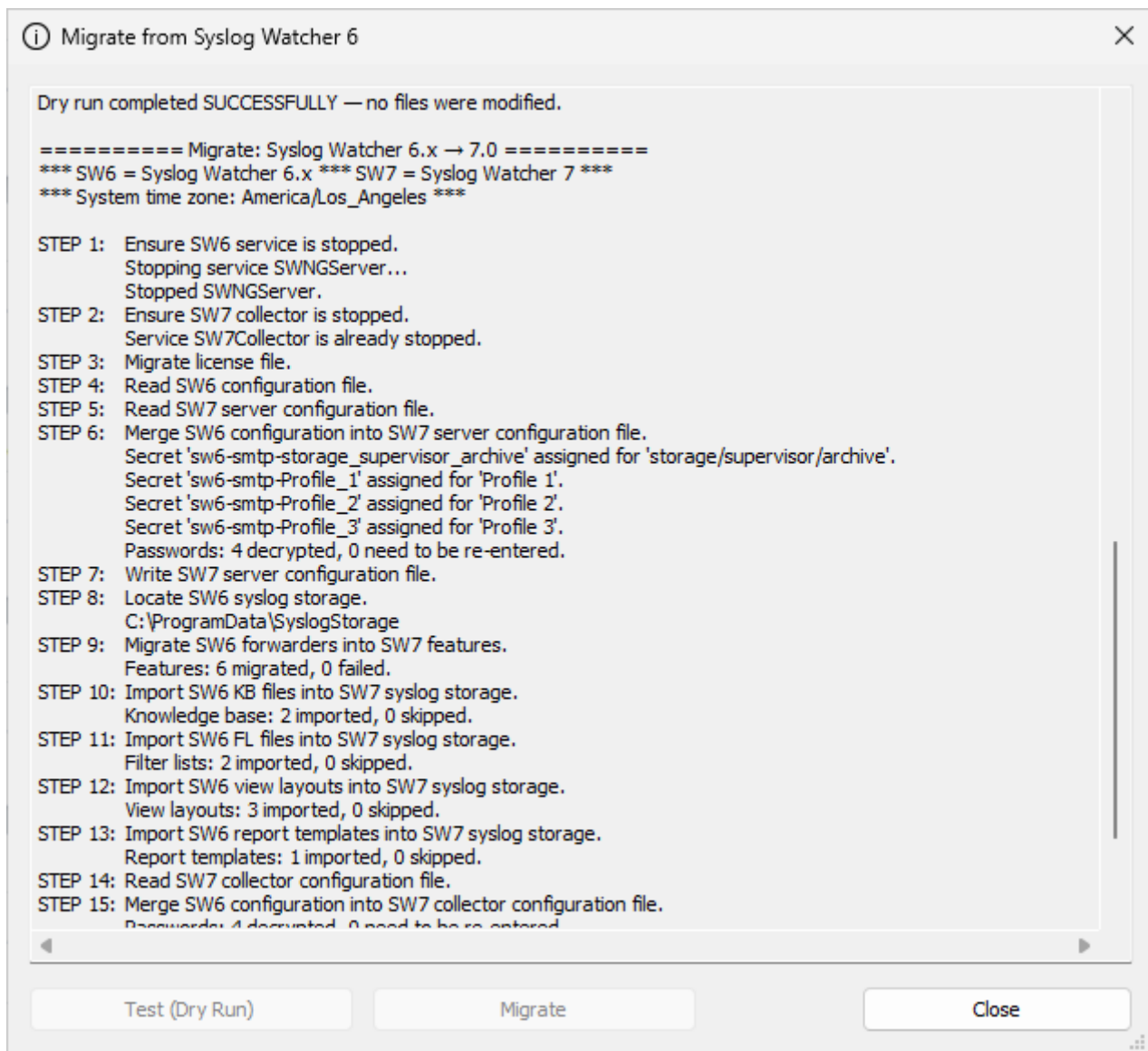
The Collector keeps running during the update unless the new version includes a newer Collector.

Migrate from Version 6

If Syslog Watcher 6 is installed on the same computer, Syslog Watcher 7 can migrate its configuration and license and keep using its syslog storage.

Messages are not copied or converted. The version 6 message files stay in place, and Syslog Watcher 7 writes new messages to the same folder in its own format. It reads both formats, so view tabs, searches, and reports include old and new messages.

If Manager finds Syslog Watcher 6 when it connects to the local server, it opens the **Migrate from Syslog Watcher 6** window.



Migrate from Syslog Watcher 6

Migrate

1. Click **Test (Dry Run)**. The log lists what can be converted and any warnings. Nothing is changed: no services are stopped, no files are written, and no license is installed.
2. Click **Migrate**, then click **Yes** to confirm.
3. Wait until the log shows **Migration completed SUCCESSFULLY**. A message reminds you that retention is turned off; click **OK**.
4. Check the storage limits and turn retention back on (see [Turn Retention On](#)).
5. Start the collector: in the **Server** section of the main toolbar, click **Collector** → **Start Syslog Collector**.

The migration log is saved to **C:\ProgramData\SyslogWatcher7\sw6_migration.log**. After a successful migration, the window is not shown again. If the migration finishes with errors, review the log; the window opens again the next time Manager starts.

Turn Retention On



Migration turns off storage and archive retention, so nothing is deleted until you review the limits.

1. In the **Storage** section of the main toolbar, click  **Storage** → **Storage Settings...** and check the migrated limits.
2. In the **Server** section, click  **Server** →  **Server Configuration...**, open **Storage Maintenance**, and turn on **Enforce storage limits**.
3. If the **storage archive** is used, check its settings on the same **Storage Maintenance** page. If the version 6 archiver was active, migration sets **Synchronize archive** to **Daily** and keeps the version 6 **Archive location** and **Keep archive files for (days)**. To delete old archive files again, set **Limit archive retention** to **Yes, delete older archive files**.

What Migrate Does

- Stops the version 6 server service (**SWNGServer**) and sets its startup type to **Manual**, so it does not start with Windows.
- Moves the Syslog Watcher 6 license, if any, to Syslog Watcher 7.
- Converts the Syslog Watcher 6 configuration to Syslog Watcher 7: collector settings, email accounts, and storage and archive settings.
- Saves passwords from the version 6 configuration as **secret strings**.
- Imports the version 6 TLS and CA certificates for syslog over TLS and TLS forwarding into **TLS Certificates**.
- Converts version 6 forwarders to **features**.
- Imports knowledge-base files, filter lists, view layouts, and report templates.
- Points Syslog Watcher 7 at the version 6 storage folder.



If a migrated password does not work, enter it again as a secret string in the **Server** section of the main toolbar:  **More** →  **Secret Strings...** Then select that secret in the password setting, or type **%Name%**.



Do not start the Syslog Watcher 6 server after a successful migration: Syslog Watcher 7 now uses its storage folder.

Skip

Skip closes the window without migrating. Confirm with **Yes**; the window is not shown again.

Related Topics

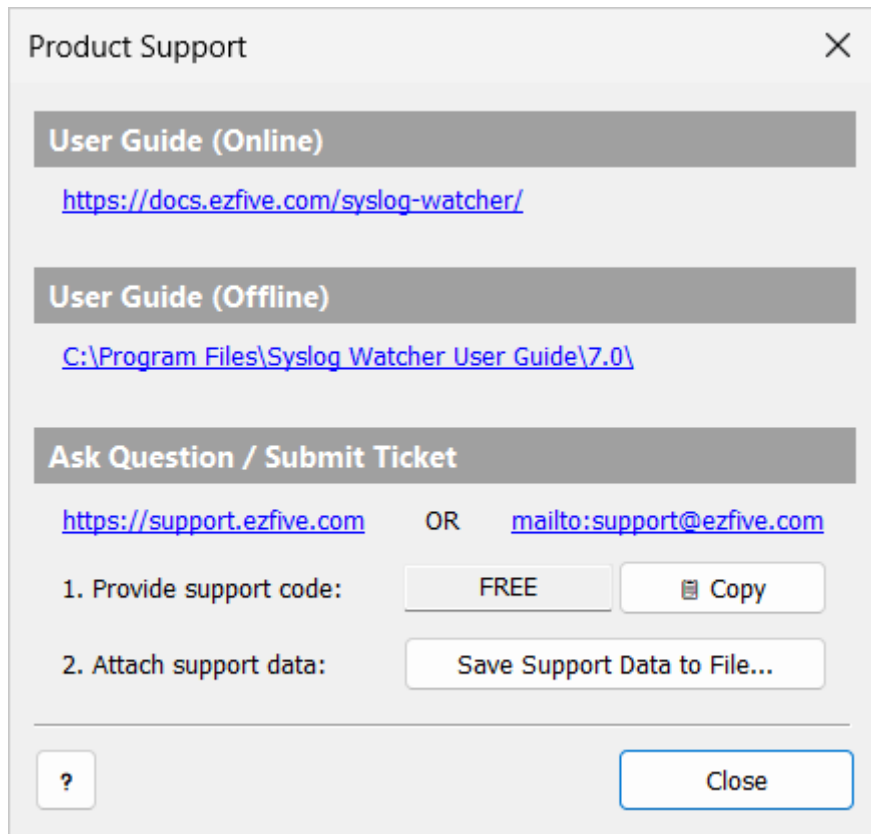
- [What's New in Version 7](#)
- [Storage Maintenance and Archive](#)

- [Secret Strings](#)

Technical Support

The **Product Support** window shows how to reach EZ5 technical support and what to send with a question.

In the **General** section of the main toolbar, click  **Support**.



Product Support window

Ask a Question or Submit a Ticket

1. Contact EZ5 in one of these ways (links under **Ask Question / Submit Ticket**):
 - Support portal: <https://support.ezfive.com>
 - Email: support@ezfive.com
2. Next to **1. Provide support code:**, click  **Copy** and paste the code into your message. The code identifies your license, so EZ5 can help you more effectively.
3. Next to **2. Attach support data:**, click **Save Support Data to File...** and attach the saved **.zip** file.



If the file is larger than 10 MB, open a ticket first. EZ5 then provides a secure shared folder for the upload.

Support Data File

The support data file is a zip archive of some Syslog Watcher Server work folders in `C:\ProgramData\SyslogWatcher7`. It contains the collector, server, feature, and storage configuration, the diagnostic records, and the installed licenses.



The support data file does not contain syslog messages, secret strings, TLS certificates, or remote access users.

User Guide

The **Product Support** window links to two copies of this User Guide:

- | | |
|-----------------------------|---|
| User Guide (Online) | Opens the guide on the web: https://docs.ezfive.com/syslog-watcher/ |
| User Guide (Offline) | Shows the folder of the installed offline guide. Click it to open the guide in the browser. If the guide is not installed, the link reads Not installed and opens the download page. |

The offline guide is a separate installer, `SyslogWatcher-7.0-UserGuide-enNN.msi`, where `enNN` is the publication number. Download it from ezfive.com/syslog-watcher/downloads/ and run it on each computer with Manager.

When the offline guide is installed, **Help** in Manager opens its pages from disk. Otherwise, Help opens the online guide.



Install the offline guide on computers without Internet access. Manager reads it when it starts, so restart Manager after the installation.

The User Guide is also available as a PDF file for reading or printing. Download it from the same [download page](#).

Related Topics

- [Diagnostic Records \(Collector\)](#)
- [Server Diagnostics](#)
- [Troubleshooting](#)