Index

Dokument:	**9000LM002DE140**
Titel:	**methodica LogzMon, Benutzerdokumentation**

Einführung

Was ist *LogzMon*?

Methodica ***LogzMon*** ist ein Werkzeug zur Anzeige und einfachen Überwachung von Log-Dateien. Die Dateien werden auf dem Web-Server gesucht und von dort gelesen. Die Ergebnisse werden an den Client übermittelt. Als Client dient ein Standard Web-Browser.

Haupt-Funktionen:

- Auflisten aller aktuellen Log-Dateien und beliebiger Text-Dateien (ASCII), auf die via den Web-Server (Apache, IIS, usw.) zugegriffen werden kann, für den LogzMon installiert worden ist.
- Anzeigen der Inhalte aktueller Log-Dateien und Archiv-Dateien.
- Farbliche Hervorhebung von Einträgen, die bestimmte Kriterien erfüllen (*Regex*[1]-Suchmuster).
- Überwachung aktiver Log-Dateien, automatische Aktualisierung des Datei-Inhalts.
  Im Modus 'Auto-Aktualisierung' das Senden von Meldungen an Syslog-Daemons, an e-Mail Boxen oder via SMS an Mobil-Telefone, wenn bestimmte Suchmuster im Datei-Inhalt gefunden werden.
- Begrenzen des benötigten Speicherplatzes client-seits durch Begrenzung der Anzahl gleichzeitig bearbeiteter Zeilen einer Datei.
- Über mehrere Seiten einer Datei navigieren.
- Einstellen vordefinierter Fenster-Grössen (z.B. für Notebook- und Desktop-Bildschirme).
- Sprach-Wahl (aktuell sind Englisch and Deutsch implementiert).

Wie funktioniert *LogzMon*?

Methodica ***LogzMon*** besteht aus server- und client-seitigen Komponenten.

Servers-seits sind dies PHP[2]-Skripte, Vorlagen und Konfigurations-Dateien.

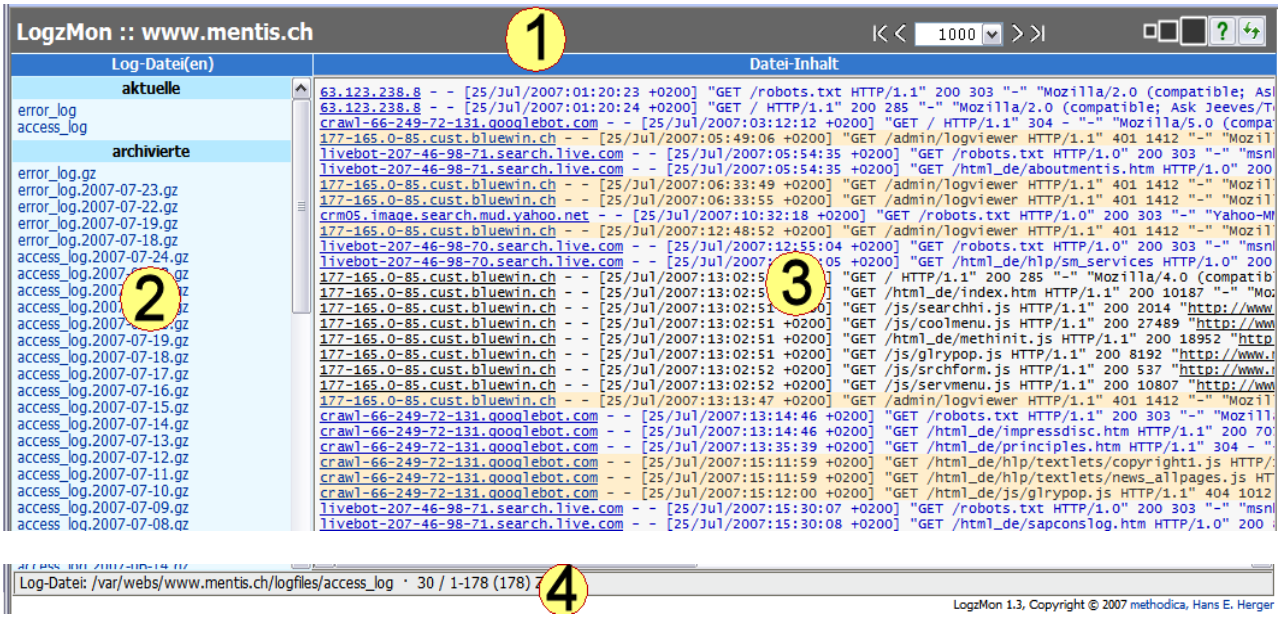
Die client-seitige Komponente (Web-Seiten) werden dynamisch, anhand einer Vorlage generiert und durch das server-seitige Haupt-Skript mit Inhalt versehen. Dabei kommen HTML-Code, Style-

[1] REGular EXpression – Regulärer Ausdruck. In der Unix-/Linux-Welt weit verbreitetes Format für Suchmuster.
[2] PHP: Hypertext Preprocessor

Sheets (CSS[3]) und JavaScript-Code zum Einsatz. Die erzeugten Web-Seiten sollten mit allen modernen Web-Browsern[4] korrekt angezeigt werden.

Client- und Server-Komponenten kommunizieren miteinander über AJAX Techniken. D.h. Ihr Browser muss JavaScript und – falls der Internet Explorer verwendet wird – die AJAX[5]-ActiveX-Komponente von Microsoft zulassen.

Die Client-Komponente



Elemente

1: Titel- und Konfigurations-Balken,
2: Übersichts-Fenster (Titel: “Log Datei(en)”),
3: Datei Window (Titel “Datei-Inhalt”) und
4: Status-Balken.

Das Übersichts-Fenster

Das Übersichts-Fenster zeigt aktuelle und Archiv-Dateien, die anhand der Konfiguration auf dem Server gefunden werden konnten.
Durch Anklicken des entsprechenden Datei- oder Archiv-Namens wählen Sie eine Datei aus. Archiv-Dateien (wie ZIP-Dateien) können ihrerseits mehrere Dateien enthalten. Sie werden angezeigt, sobald Sie auf den Namen einer solchen Archiv-Datei klicken. Solche, in Archiven enthaltene, Dateien werden ebenfalls durch Anklicken ausgewählt. Der Inhalt der ausgewählten Datei wird jeweils im Datei-Fenster angezeigt.

Das Datei-Fenster

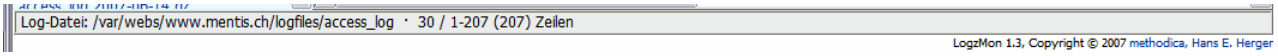
Im Datei-Fenster wird der (möglicherweise gefilterte) Inhalt der im Übersichts-Fenster ausgewählten Datei angezeigt.
Einzelne Zeilen können versteckt oder farblich hervorgehoben werden, je nachdem ob in der Konfigurations-Datei festgelegte Filter-Muster erkannt werden oder nicht.

[3] CSS: Cascading Style Sheets
[4] LogzMon wurde getestet mit Internet Explorer 6.0/7.0, Mozilla 1.7+, Firefox 1.5/2.0, Opera 8+.
[5] AJAX: Asynchronous JavaScript and XML (wenn auch LogzMon XML nicht verwendet.)

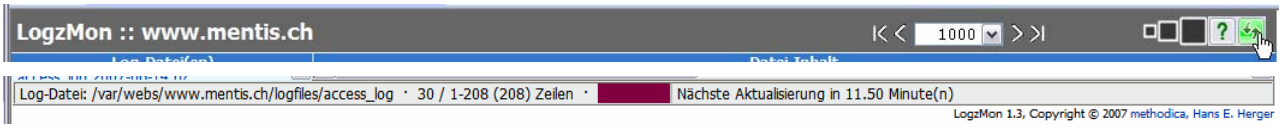
Der Status-Balken

Während auf dem Server die Dateien gesucht oder der Inhalt der ausgewählten Datei interpretiert wird, zeigt der Staus-Balken die obige Meldung an.

Sobald die Client-Seite erstmals geladen worden ist, zeigt der Status-Balken die Anzahl aktueller Dateien, die Anzahl Archiv-Dateien und die Anzahl in diesen Archiven enthaltenen Dateien (nur ZIP-Archive) an.



Ist der Inhalt einer Datei geladen, weist der Status-Balken die Anzahl angezeigter Zeilen, den Nummernbereich der verarbeiteten Zeilen und die Gesamtzahl der in der Datei enthaltenen Zeilen (in Klammern) aus.



Wird LogzMon im Modus ‘Auto-Aktualisierung’ betrieben, zeigt der Status-Balken zusätzlich die bis zur nächsten Aktualisierung verbleibenden Minuten textlich und mit einer einfachen Grafik an.

Der Titel- und Kofigurations-Balken

Er enthält folgende Elemente:

- Werkzeug-Name (“LogzMon”),
- Hostname (“www.mentis.ch” im gezeigten Beispiel),
- Das Navigations-Werkzeug,
- Die Fenstergrössen-Wahl,
- Den Aktions-Schalter ‘Hilfe’,
- Den Aktions-Schalter ‘Auto-Aktualisierung’

Der Werkzeug-Name

Bei Anklicken des Werkzeug-Namens wird auf geprüft, ob eine neuere Version zum Download bereit steht. Falls dies zutrifft, werden Sie zu einer Seite geführt, von der der LogzMon herunter geladen werden kann. Diese Funktion setzt Internet-Zugang voraus.

Der Hostname

Der Name des Hosts, der durch LogzMon überwacht wird. Üblicherweise werden Sie zur Hauptseite geführt, sobald sie den Hostnamen anklicken. Die entsprechenden Einstellungen werden in der Konfigurations-Datei vorgenommen.

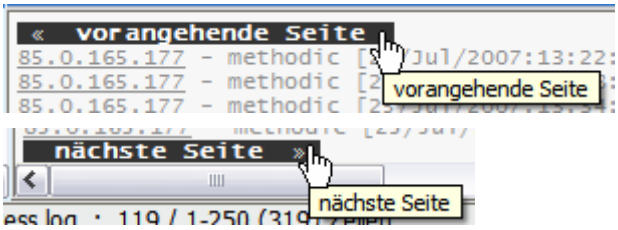
Das Navigations-Werkzeug

Das Navigations-Werkzeug erlaubt, die Anzahl pro Anfrage bearbeiteter Zeilen einzuschränken und über die so festgelegten Inhalts-Seiten hinweg zu navigieren.
Wenn alle in einer Datei enthaltenen Zeilen an den Client übermittelt werden, könnte mehr Speicher als auf der Client-Maschine vorhanden, nötig sein. In solchen Fällen empfehlen wir Ihnen, die Anzahl bearbeiteter Zeilen einzuschränken. Insbesondere auch, wenn der Modus ‘Auto-Aktualisierung’ eingeschaltet ist, würde sonst die Anzahl übermittelter Zeilen sukzessive anwachsen.

Eine Drop-Down-Liste bietet Werte zwischen 250 und 75000 und ALL (=alle) Zeilen zur Auswahl an. Standard-Wert ist: 1000 Zeilen.

- Die Navigations-Schalter sind (von links nach rechts):
- Gehe zur ersten Seite,
- Gehe eine Seite zurück,
- Gehe eine Seite vorwärts,
- Gehe zur letzten Seite.

Alternativ dazu können Sie auf die Links klicken, die (wenn sinnvoll) oben und untern im Datei-Fenster eingeblendet sind:



Haben Sie eine Zeilen-Beschränkung eingestellt, wird der zugehörige Wert automatisch wieder eingestellt, sobald Sie LogzMon das nächste Mal vom gleichen Server aufrufen. (Dies gilt, solange Cookies zugelassen und nicht wieder gelöscht worden sind.)

Die Fenstergrössen-Wahl

Drei Fenstergrössen, unter denen Sie auswählen können, sind voreingestellt:

- **Klein**:
  Wahrscheinlich die beste Grösse für Notebooks. Die verwendeten Fonts sind ebenfalls entsprechen kleiner.
- **Mittel**:
  Standard-Fenstergrösse. Geeignet für die meisten Desktops.
- **Gross**:
  Für Desktops mit grossen Bildschirmen. Auf vielen Geräten entspricht diese Fenstergrösse etwa dem Vollbild-Modus.

Haben Sie eine Fenstergrösse gewählt, wird diese Grösse automatisch wieder eingestellt, sobald Sie LogzMon das nächste Mal vom gleichen Server aufrufen. (Dies gilt, solange Cookies zugelassen und nicht wieder gelöscht worden sind.)

Der Aktions-Schalter 'Hilfe'

Zeigt eine kurze Bedienungsanleitung der Client-Komponente an.

Der Aktions-Schalter ‚Auto-Aktualisierung'

Dieser Schalter lässt Sie den Modus 'Auto-Aktualisierung' EIN- respektive AUS-schalten. Er hat einen grünen Hintergrund, wenn der Zustand EIN ist.
Im Modus 'Auto-Aktualisierung' setzt der Client automatisch nach jeweils 12 Minuten (720 Sekunden; dieser Wert kann in der Konfigurations-Datei geändert werden) eine Anfrage zur Aktualisierung der gewählten Datei ab.
Aktionen (siehe 'Konfigurations-Datei' unten) werden nur in diesem Modus und jeweils nur für gegenüber der vorangehenden Anfrage neue Zeilen berücksichtigt.

Die Konfigurations-Datei

Sie ist auf dem Server unter dem Namen "*logviewer_config.inc.php*" gespeichert. Sie enthält PHP-Code, der zur Laufzeit eingebunden und ausgeführt wird.
Deshalb folgt ihr Inhalt den Syntax-Regeln von PHP.

WARNUNG:
Die Konfigurations-Datei wird zur Laufzeit direkt eingebunden und als PHP-Code ausgeführt. Deshalb wird, entdeckt der PHP-Interpreter Syntax-Fehler in dieser Datei, üblicherweise auch die Ausführung des Hauptskripts abgebrochen. Seien Sie also sehr vorsichtig beim Editieren!

Die Abschnitte der Konfigurations-Datei:
- Logfiles (Log-Dateien),
- Logdirs (Verzeichnisse mit Log-Dateien,
- Archivedirs (Verzeichnisse mit Archiv-Dateien),
- Filters (Filter für Hervorhebung und Aktionen),
- Filtersets (Sets von Filtern für Hervorhebung und Aktionen nach Dateien),
- Actions, (Aktionen)
- Generelle Konstanten (defines).

Unterschiedliche Konfigurationen können in einer Datei zusammengefasst und bedingt ausgeführt werden. Dazu sind die Kommentarzeilen '*if ($user==…) { … }*' zu aktivieren und muss beim ersten Aufruf der Parameter '*user=user_name*' angegeben werden.
Z.B.: *https://www.ihrserver.com/admin/logviewer/logviewer.php?user=ADMINISTRATOR*.

Logfiles

Zweck:

Liste von Dateinamen (inkl. Pfad), die zwingend im Übersichtsfenster angezeigt werden sollen.

Syntax:

```
$logfiles = array (
      array ('full_filename','identifier'),
      array (…),
      …
);
```

Wobei:

full_filename	ist der Name der anzuzeigenden Datei inkl. des vollständigen Verzeichnis-Pfades.. Z.B..: '*F:\web\logs\syslog_catchall.txt*' oder '*/var/www/www.yourhost.com/logs/syslog_current.txt*'
identifiler	Eine (fakultative) Kennung, die mit dem Datei-Namen zusammen angezeigt werden soll. Dies kann hilfreich sein, wenn gleichnamige Dateien aus unterschiedlichen Verzeichnissen einbezogen werden sollen.

LogDirs

Zweck:

Liste von Verzeichnissen, deren Dateien als (aktuelle) Log-Dateien im Übersichts-Fenster angezeigt werden sollen. Nur Dateien mit einer Endung, die der Konstante '*logext*' entspricht, werden dabei berücksichtigt.

Syntax:

```
$logdirs = array (
```

```
      array ('directory_name','identifier'),
      array (..),
      …
);
```

Wobei:

directory_name	Verzeichnis-Name. Z.B..: '*F:\web\www.yourhost.com\logs*' oder '*/var/www/www.yourhost.com/logs*' Bitte **kein** abschliessendes Slash- oder Back-Slash-Zeichen angeben.
identifier	Eine (fakultative) Kennung, die mit dem Datei-Namen zusammen angezeigt werden soll. Dies kann hilfreich sein, wenn gleichnamige Dateien aus unterschiedlichen Verzeichnissen einbezogen werden sollen.

ArchiveDirs

Zweck:

Liste von Verzeichnissen, deren Dateien als Archiv-Dateien im Übersichts-Fenster angezeigt werden sollen. Nur Dateien mit einer Endung, die der Konstante '*arcext*' entspricht, werden dabei berücksichtigt.

Syntax:

```
$archivedirs = array (
      array ('directory_name','identifier'),
      array (…),
      …
);
```

Wobei:

directory_name	Verzeichnis-Name Z.B..: '*F:\web\www.yourhost.com\logs\archive*' oder '*/var/www/www.yourhost.com/logs/archive*' Bitte **kein** abschliessendes Slash- oder Back-Slash-Zeichen angeben.
identifier	Eine (fakultative) Kennung, die mit dem Datei-Namen zusammen angezeigt werden soll. Dies kann hilfreich sein, wenn gleichnamige Dateien aus unterschiedlichen Verzeichnissen einbezogen werden sollen.

Filters

Zweck:

Filter werden auf jede Zeile einer Datei angewendet, um…

- Hervorhebungen und
- Aktionen, die im Modus *Auto-Aktualisieren* auszuführen sind,

zu bestimmen.

Filter werden angewendet, wenn kein Filterset anwendbar ist.

Syntax:

```
$filters = array (
      array ('filter_regex','foreground','background','actions'),
      array (…),
      …
);
```

Wobei:

filter_regex ist das Filter-Muster als regulärer Ausdruck (Regex) ausgedrückt. Die Parameter *foreground* und *background* werden gewürdigt, wenn das Filter-Muster im Zeilen-Inhalt gefunden wird.
Unix-/ Linux-Benutzer kennen üblicherweise die Regeln nach denen ein regulärer Ausdruck gebildet wird. Zusätzliche Informationen dazu sind hier zu finden:
http://www.regular-expressions.info
http://www.amk.ca/python/howto/regex/.
http://de.wikipedia.org/wiki/Regulärer_Ausdruck
Meta-Zeichen müssen durch einen Back-Slash (\) eingeleitet werden, damit sie buchstäblich verwendet werden.
Die Meta-Zeichen sind: ^ $ * + ? {} [ ] \ | ( )
Mehrere Muster können durch das Pipe-Zeichen (|) aneinander gefügt werden.
Anstelle eines Musters kann auch der Name einer definierten Konstante, die als Wert das Muster enthält, angegeben werden.

foreground Einer dieser drei Werte:

- Der RGB-Code der Vordergrund-Farbe,
- Das Schlüsselwort *hide*, oder
- Ein leerer String (= keine Hervorhebung).

Ist der Parameter *foreground* = *hide*, werden Zeilen, bei denen *filter_regex* zutrifft, nicht angezeigt. Sonst werden solche Zeilen in der entsprechenden Vordergrund-Farbe angezeigt.
Das Format des RGB-Codes ist: #rrggbb, wobei

- rr = ROT-Anteil, hexadezimal (00..FF),
- gg = GRÜN-Anteil, hexadezimal (00..FF),
- bb = BLAU-Anteil, hexadezimal (00..FF).

background Einer dieser beiden Werte:

- Der RGB-Code der Hintergrund-Farbe,
- Ein leerer String (= keine Hervorhebung).

actions Der Name einer oder mehrerer Aktion(en), die im Modus *Auto-Aktualisierung* auszuführen sind. Mehrere Namen können, durch das Pipe-Zeichen (|) getrennt, aneinander gefügt werden.

Filtersets

Zweck:

Filter werden auf jede Zeile einer Datei angewendet, um…

- Hervorhebungen und
- Aktionen, die im Modus *Auto-Aktualisieren* auszuführen sind,

zu bestimmen.
Die Filter eines *Filterset* werden auf die Zeilen derjenigen Dateien angewendet, auf deren Namen das Muster *filterset_regex* zutrifft.
Nur das erste zutreffende Filterset wird angewendet.

Syntax:

```
$filterset = array (
   array ('filterset_regex',
      array ('filter_regex','foreground','background','actions'),
      array (…),
   ),
   array ('filterset_regex',
      array ('filter_regex','foreground','background','actions'),
      array (…),
```

```
    ),
);
```

Wobei:

filterset_regex	ist das Filter-Muster, als regulärer Ausdruck (Regex) ausgedrückt, das für die Selektion der Dateien verwendet wird, auf die die Filter-Regeln anzuwenden sind. Meta-Zeichen müssen durch einen Back-Slash (\) eingeleitet werden, damit sie buchstäblich verwendet werden. Die Meta-Zeichen: ^ $ * + ? {} [ ] \ | ( ) Mehrere Muster können durch das Pipe-Zeichen (|) aneinander gefügt werden. Anstelle eines Musters kann auch der Name einer definierten Konstante, die als Wert das Muster enthält, angegeben werden.
filter_regex …	Filter-Regel wie oben beschrieben, siehe *Filters*.
actions	Name(n) von im Modus *Auto-Aktualisieren* auszuführender Aktionen. Mehrere Aktions-Namen können, durch das Pipe-Zeichen (|) getrennt, aneinander gefügt werden.

Actions

Zweck:

Aktionen werden ausgeführt, wenn der Modus *Auto-Aktualisieren* EIN ist und das entsprechende Muster *filter_regex* (siehe *Filters* and *Filtersets*) mit dem Inhalt einer Datei-Zeile übereinstimmt.
Eine Aktion sendet eine Meldung an unterschiedliche Adressaten entsprechend einem dieser drei Aktions-Typen:

- SYSLOG: Sendet eine Meldung an einen Syslog-Daemon im Intranet oder Internet.
- SMTPMAIL: Sendet eine Meldung an eine e-Mail-Box über einen SMTP-Server,
- SMSCLICK: Sendet eine Kurzmeldung (SMS) an ein Mobil-Telefon über den SMS-Dienst von Clickatell. (Hinweis: Sie müssen bei Clickatell (http://www.clickatell.com) ein Konto eingerichtet und eine HTTP API-Nummer beantragt haben, um diesen Dienst zu nutzen).

Aktions-Typen sind als einfache Add-on-Module implementiert und lassen sich dadurch recht einfach erweitern.

Syntax:

```
$actions = array (
      array ('action_name','action_type',
             'action_parameters',
             'message_regex',
             'message_text'
      ),
      Array(…),
);
```

Wobei:

action_name	ist der Name Ihrer Wahl der Aktion. Er wird in Filter-Definitionen als Verweis verwendet.
action_type	ist einer der drei Typen *SYSLOG, SMTPMAIL oder SMSCLICK* wie oben beschrieben. Ein dem *action_type* entsprechendes Add-on-Modul nach dem Namens-Muster '*addon_*{action_type}.*php*' wird erwartet.
action_parameters	sind Parameter zuhanden der verschiedenen Add-on-Module und sind

deshalb jeweils je *action_type* unterschiedlich. Sie werden immer mittels des Pipe-Zeichens (|) aneinander gereiht.

SYSLOG: Format:

```
'facility|level|host|process|daemon_ip|daemon_port'
```

facility: Facility code. Z.B. 23 (= local 7).
level: Log level. Z.B.: 5 (= notice).
host: Host-Name oder IP-Adresse.
process: Prozess-Name.
daemon_ip: IP-Addresse des empfangenden Syslog-Daemon.
Daemon_port: Port-Nummer des empfangenden Syslog-Daemon.
(Als Protokoll wird immer UDP verwendet.)

Facilities

Facility-Name	Alternativer Name	Wert
Kernel	Kern	0
User		1
Mail		2
Daemon		3
Auth		4
Syslog		5
Lpr		6
News		7
UUCP		8
Cron		9
System0	Security	10
System1	FTP	11
System2	NTP	12
System3	Logaudit	13
System4	Logalert	14
System5	Clock	15
Local0		16
Local1		17
Local2		18
Local3		19
Local4		20
Local5		21
Local6		22
Local7		23

Levels

Level-Name	Alternativer Name	Wert
Emergency	Emerg	0
Alert		1
Critical	Crit	2
Error	Err	3
Warning	Warn	4
Notice		5
Information	Info	6
Debug		7

SMTPMAIL: Format:
`'from_name|from_address |to_name|to_address|subject'`

from_name: Name des Absenders im Klartext.
Z.B. `'Log Monitor'.`
from_address: Mailbox-Adresse des Absenders.
Z.B.: logzmon@yourhost.com
to_name: Name des Empfängers im Klartext.
to_address: Mailbox-Adresse des Empfängers.
Subject: Betreffzeile der e-Mail.
Z.B.: [LogzMon] Warnung

SMSCLICK: Format:
`'sender|recipient'`

sender: Absender-Kennung.
Z.B. `'LogzMon Ihrhost.com'.`
recipient: Mobil-Telefon-Nummer des Empfängers.
Z.B.: +491079999999.

message_regex Regex-Muster, das auf den Zeilen-Inhalt angewendet wird.
Z.B.:
`'\A([\d]{1,3}\.[\d]{1,3}\.[\d]{1,3}\.[\d]{1,3}) (.*) 401 401'`
…würde mit einer IP-Adresse, gefolgt von beliebigem Text und den Return-Codes '401 401', übereinstimmen. Zwei Text-Partikel, $1 und $2 (festgelegt durch die beiden Ausdrücke in Klammern), können anschliessend referenziert werden, wobei $1 für die IP-Adresse und $2 für den Text zwischen der IP-Adresse und den Return-Codes steht.
Falls keine Text-Partikel referenziert werden sollen, verwenden Sie als Regex-Muster am besten `'.*',` was 'beliebigen Text' bedeutet.
Meta-Zeichen müssen durch einen Back-Slash (\) eingeleitet werde, damit sie buchstäblich verwendet werden.
Die Meta-Zeichen: ^ $ * + ? {} [ ] \ | ( )
Mehrere Muster können durch das Pipe-Zeichen (|) aneinander gefügt werden.
Anstelle eines Musters kann auch der Name einer definierten Konstante, die als Wert das Muster enthält, angegeben werden.

message_text Meldungstext. Kann optional Referenzen auf Text-Partikel (wie $1,$2…$n) des Regex-Musters, wie oben beschrieben, enthalten.
Z.B.:
`'Zugriffsversuch auf geschützten Bereich von IP=$1.\n\n$line'`
Folgende Standard-Text-Partikel können ebenfalls referenziert werden:

- $0: Der gesamte String, der mit dem Suchmuster übereinstimmt,
- $line: Der gesamte Zeilen-Inhalt,
- $file: Der Name der aktuellen Datei.

Defines

Zweck:

Konstanten festlegen.
Praktisch alle der unten aufgeführten Konstanten sind obligatorisch; die Werte sind wählbar.

Syntax:

```
Define ('constant_name', 'constant_value');
```

Wobei:
constant_name dieser Liste entspricht:

logext	Namenserweiterung(en) der (aktuellen) Log-Dateien, begrenzt durch Unterstriche (_). Sollen Dateien ohne Erweiterungen einbezogen werden, kann dies durch zwei Unterstriche(__) angegeben werden. Verwendet zusammen mit den Definitionen des Abschnitts *'Logdirs*'. Z.B.: `define('logext', '_log_lg_');` Obligatorisch.
arcext	Namenserweiterung(en) der Archiv-Dateien, begrenzt durch Unterstriche (_). Sollen Dateien ohne Erweiterungen einbezogen werden, kann dies durch zwei Unterstriche(__) angegeben werden. Verwendet zusammen mit den Definitionen des Abschnitts '*Archivedirs*'. Z.B.: `define('arcext', '_gz_');` Obligatorisch.
language	Sprachcode (2-stellig). Momentan gültig sind: `'en'=English, 'de'=Deutsch` Obligatorisch.
refresh_interval_seconds	Im Modus 'Auto-Aktualisierung' das Intervall in Sekunden zwischen zwei Aktualisierungen. (Z.B. 720 = 12 Minuten). Obligatorisch.
refresh_test_milliseonds	Im Modus 'Auto-Aktualisierung' das Intervall in Millisekunden zwischen zwei Prüfungen, ob eine Aktualisierung nötig ist. (Z.B. 30000 = ½ Minute). Obligatorisch.
size	Bevorzugte Fenstergrösse. Mögliche Werte sind: `small, medium=standard, large` Der Benutzer kann diese Fenstergrössen im Browser abweichend von diesem Wert wählen. Obligatorisch.
host_name	Name des Host, den Sie mit LogzMon überwachen. Obligatorisch.
host_name_url	Hyperlink zur Web-Site des Host, der verwendet wird, wenn der Benutzer den Hostnamen anklickt. Obligatorisch.
SuppressIpLookups	Wenn eine Zeile einer Log-Datei eine IP-Adresse enthält, wird diese mit einem Hyperlink zum Nachschlagen[6] versehen. Dies kann dadurch unterdrückt werden, dass dieser Konstanten der Wert *true* (ohne Hochapostrophes) zugewiesen wird. Obligatorisch.
SuppressHttpLookups	Wenn eine Zeile einen (aufgelösten) Hostnamen enthält, wird dieser mit einem Hyperlink zum Nachschlagen [6] versehen. Dies kann dadurch unterdrückt werden, dass dieser Konstanten der Wert *true* (ohne Hochapostrophes) zugewiesen wird. Obligatorisch.

[6] Dank an www.domaintools.com für diese Funktionalität!

beliebige andere	Zur Verwendung mit z.B. *filter-, filtersets- Definitionen,* oder beliebigen anderen Konfigurations-Definitionen nach Ihrer Wahl. Achten Sie darauf, dass Sie Referenzen auf solche Konstanten immer ohne Hochapostrophes angeben Fakultativ.