

Logauswertung

Zur Ansicht der einzelnen Logdateien auf der mp-Firewall wurde die Systemrolle *revision* geschaffen. Mit diesem Zugang haben Sie die Möglichkeit sich das Firewall-Log, die Zugangslogs sowie sämtliche Systemmeldungen anzeigen zu lassen.

ACHTUNG: Der dauerhafter Betrieb der mp-Firewall ist für den ordnungsgemäßen Ablauf im System notwendig, da die Log-Dateien in der Nacht aufgeräumt werden.

Firewall- und Zugangs-Log

Um den Status des Revisors zu erlangen, müssen Sie sich bei der Anmeldung auf der mp-Firewall mit dem Benutzernamen *revision* und dem zugehörigen Passwort anmelden.

Als Revisions-Benutzer stehen folgende Optionen zur Verfügung:

| | |
|------------------|---|
| Ende | Verlassen des Menüs. |
| ----- | |
| Firewall gestern | Firewall-Log-Dateien des vergangenen Tages. |
| Firewall Woche | Firewall-Log-Dateien der vergangenen Woche. |
| Firewall dauer | Alle verfügbaren Firewall-Log-Dateien auf dem System. |
| ----- | |
| Benutzer heute | Anzeige der Benutzeranmeldungen an der mp-Firewall des jeweiligen Tages. |
| Benutzer zuletzt | Anzeige aller Benutzeranmeldungen an der mp-Firewall, die in der Log-Datei verfügbar sind. |
| Benutzer gesamt | Anzeige der Anmeldezeiten von Benutzern an der mp-Firewall mit Anmelde- und Abmeldezeit sowie einer Statusanzeige für noch angemeldete Benutzer. Weiterhin kann hier nachvollzogen werden, von welcher IP-Adresse die Verbindung aufgebaut wurde. |
| ----- | |
| Direkt | Statische Anzeige aller verfügbaren Log-Dateien auf der mp-Firewall. |
| Fortlaufend | Fortlaufende Anzeige verfügbarer Log-Dateien auf der mp-Firewall. |

Protokolldateien statisch und fortlaufend

Die Ansicht der einzelnen Log-Dateien auf der mp-Firewall kann statisch oder fortlaufend geschehen. Für eine statische bzw. fortlaufende Ansicht stehen folgende Protokolle zur Verfügung:

| Log-Bezeichnung | statisch | fortlaufend | Beschreibung |
|-----------------|----------|-------------|--|
| auth.log | x | x | Alle Meldungen im Zusammenhang mit der Authentifizierung |
| kern.log | x | x | Alle Systemmeldungen |
| last.log | x | - | Letzte Anmeldungen am System |
| mail.log | x | x | Logdatei, die im Zusammenhang mit dem Mailserver erstellt wird. Darin enthalten sind Meldungen zu den amavisd-Mailfiltern und zum postfix Mailserver |

| Log-Bezeichnung | statisch | fortlaufend | Beschreibung |
|-----------------------|----------|-------------|--|
| squid/access.log | x | x | Meldungen, die im Zusammenhang mit dem squid-Proxy erzeugt wurden |
| squid/cache.log.x | x | x | Alle Meldungen, die vom Squid-Proxy erzeugt werden |
| clamav/clamav.log.x | x | x | Alle Meldungen, die von dem clamav-Virens Scanner erzeugt wurden |
| clamav/freshclam.log | x | x | Meldungen, die im Zusammenhang mit dem Update de clamav-Virens Scanner bzw. dem Update der Virensignaturen erzeugt wurden. |
| mysql/mysql-bin.00x | x | - | Meldungen, die von der MySQL-Datenbank erzeugt wurden |
| mysql/mysql-bin.index | x | - | Indexdatei zu den MySQL-Logdateien |
| admin/backuser | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>backuser</i> ausgeführt wurden |
| admin/config | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>config</i> ausgeführt wurden |
| admin/maint | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>maint</i> ausgeführt wurden |
| admin/root | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>root</i> ausgeführt wurden |
| admin/security | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>security</i> ausgeführt wurden |
| admin/update | x | x | Potokolldatei über alle Schritte, die von der Systemrolle <i>update</i> ausgeführt wurden |

From:

<https://help.m-privacy.de/> -

Permanent link:

<https://help.m-privacy.de/doku.php/tightgate-firewall:logauswertung>Last update: **2026/05/11 07:48**