Wo werden Protokolle auf der Cisco E-Mail Security Appliance (ESA) gespeichert, und wie kann ich darauf zugreifen?

Die Cisco E-Mail Security Appliance (ESA) erstellt ein Verzeichnis für jedes Protokoll-Abonnement, das auf dem Namen des Protokoll-Abonnements basiert.

ESA-Protokolldateiformat

Der tatsächliche Name der Protokolldatei im Verzeichnis besteht aus dem von Ihnen angegebenen Protokolldateinamen, dem Zeitstempel beim Starten der Protokolldatei und einem einstelligen Statuscode.

```
/LogSubscriptionName/LogFilename.@timestamp.statuscode
```

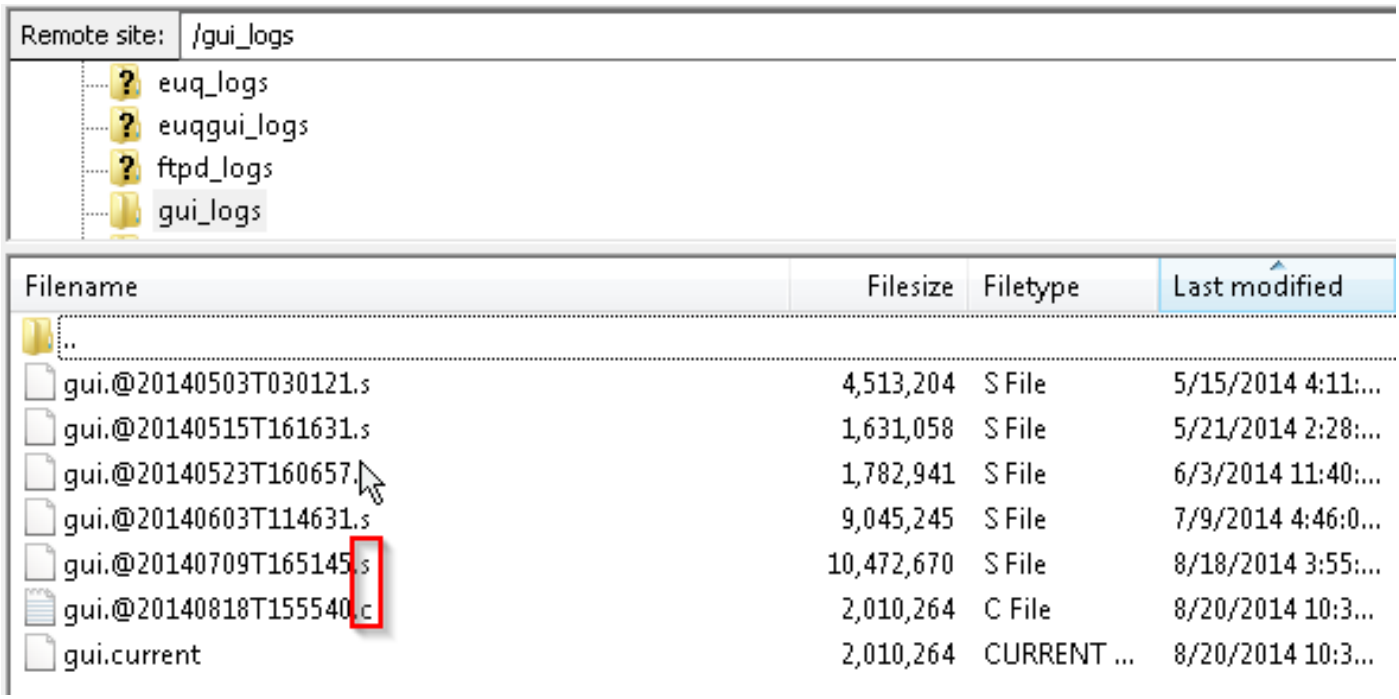
LogSubscriptionNames können über den Befehl **logconfig** angezeigt werden:

```
esa.example.com> logconfig

Currently configured logs:
   Log Name            Log Type                      Retrieval           Interval
 ---------------------------------------------------------------------------------
 1. TLStest             Injection Debug Logs          Manual Download     None
 2. Test                Domain Debug Logs             Manual Download     None
 3. amp                 AMP Engine Logs               Manual Download     None
 4. amparchive          AMP Archive                   Manual Download     None
 5. antispam            Anti-Spam Logs                Manual Download     None
 6. antivirus           Anti-Virus Logs               Manual Download     None
 7. asarchive           Anti-Spam Archive             Manual Download     None
 8. authentication      Authentication Logs           Manual Download     None
 9. avarchive           Anti-Virus Archive            Manual Download     None
10. bounces             Bounce Logs                   Manual Download     None
11. cli_logs            CLI Audit Logs                Manual Download     None
12. encryption          Encryption Logs               Manual Download     None
13. error_logs          IronPort Text Mail Logs       Manual Download     None
```

Zusätzliche Log-FIle-Erweiterungen

Statuscodes können eine Dateierweiterung anzeigen, z. B. .c (als aktuelle Version bezeichnet) oder .s (als gespeicherte Datei gekennzeichnet)



Wie kann ich auf die Protokolle zugreifen?

Standardmäßig gibt es zwei Methoden zum Abrufen der Protokolle, die in der ESA gespeichert sind: **FTP oder SCP.**

Sie sollten für den Protokollabruf dieselben Anmeldeinformationen verwenden, wie Sie für die Authentifizierung zur Verwaltung bei der ESA verwenden.

Zugriffsprotokolle über FTP

FTP: Befehlszeile

```
ftp hostname.example.com
cd /LogNameDirectory
get
```

FTP: GUI-Client

Ein GUI-FTP-Client wie Filezilla kann verwendet werden, um "per Drag-and-Drop" von der ESA auf Ihren lokalen Rechner zu ziehen.

FTP wird verwendet: Webbrowser

Jeder FTP-unterstützte Webbrowser wie Mozilla Firefox, Google Chrome oder Microsoft Internet Explorer kann ebenfalls verwendet werden.

Protokolle über SCP auf ein anderes System kopieren

Verwenden von SCP:

```
scp admin@mail3.example.com:/LogNameDirectory/LogFilename
```

Hinweis: Stellen Sie sicher, dass der richtige Service (FTP oder SCP) auf Ihrer ESA mithilfe des **Befehls interface**config in der CLI aktiviert ist.