

¿Dónde se almacenan los registros en el dispositivo de seguridad Cisco Email Security Appliance (ESA) y cómo puedo acceder a ellos?

Cisco Email Security Appliance (ESA) crea un directorio para cada suscripción de registro basado en el nombre de la suscripción de registro.

Formato de archivo de registro ESA

El nombre real del archivo de registro en el directorio está compuesto por el nombre del archivo de registro especificado por usted, la marca de hora cuando se inició el archivo de registro y un código de estado de un solo carácter.

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

LogSubscriptionNames se puede ver a través del comando **logconfig**:

```
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

Extensiones FI de registro adicionales

Los códigos de estado pueden mostrar una extensión de archivo como **.c** (que significa actual) o **.s** (que significa guardado)

Filename	Filesize	Filetype	Last modified
..			
gui.@20140503T030121.s	4,513,204	S File	5/15/2014 4:11:...
gui.@20140515T161631.s	1,631,058	S File	5/21/2014 2:28:...
gui.@20140523T160657.s	1,782,941	S File	6/3/2014 11:40:...
gui.@20140603T114631.s	9,045,245	S File	7/9/2014 4:46:0...
gui.@20140709T165145.s	10,472,670	S File	8/18/2014 3:55:...
gui.@20140818T155540.c	2,010,264	C File	8/20/2014 10:3...
gui.current	2,010,264	CURRENT ...	8/20/2014 10:3...

¿Cómo puedo acceder a los registros?

De forma predeterminada, hay dos métodos para recuperar los registros almacenados en el ESA: FTP o SCP.

Debe utilizar las mismas credenciales de inicio de sesión para la recuperación de registros que utiliza para autenticarse en el ESA para la administración.

Registros de acceso por FTP

FTP: Línea de comandos

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

FTP: cliente GUI

Un cliente FTP GUI como [Filezilla](#) se puede utilizar para 'arrastrar y soltar' desde el ESA a su máquina local.

Uso de FTP: Explorador web

También se puede utilizar cualquier navegador web compatible con FTP, como Mozilla Firefox, Google Chrome o Microsoft Internet Explorer.

Copiar registros a otro sistema a través de SCP

Uso de SCP:

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

Nota: Asegúrese de que tiene el servicio adecuado (FTP o SCP) habilitado en su ESA mediante el comando `interfaceconfig` en la CLI.

