

# 从CES ESA和CMD的GUI下载日志

## 目录

[简介](#)

[先决条件](#)

[从GUI下载日志](#)

[从CMD下载日志](#)

[相关信息](#)

## 简介

本文档介绍如何通过命令行(CMD)从安全邮件云网关(CES)的图形用户界面(GUI)下载日志。

## 先决条件

具有管理员或云管理员权限的用户帐户。

## 从GUI下载日志

- 1.登录到CES邮件安全设备(ESA)实例的GUI，然后导航到**系统管理**>日志订用。
- 2.注意浏览器中看到的URL(例如：[System Administration Log Subscriptions](#))
- 3.接下来，您需要查看**日志设置**列，并查找要下载的日志。在本示例中，请使用mail\_logs。

| Configured Log Subscriptions |                                   |                   |              |                                       |        |
|------------------------------|-----------------------------------|-------------------|--------------|---------------------------------------|--------|
| Add Log Subscription...      |                                   |                   |              |                                       |        |
| Log Settings                 | Type ▲                            | Rollover Interval | Size         | All <input type="checkbox"/> Rollover | Delete |
| amp                          | AMP Engine Logs                   | None              | 192K         | <input type="checkbox"/>              |        |
| amparchive                   | AMP Archive                       | None              | 64K          | <input type="checkbox"/>              |        |
| antispam                     | Anti-Spam Logs                    | None              | 10.1M        | <input type="checkbox"/>              |        |
| antivirus                    | Anti-Virus Logs                   | None              | 3.1M         | <input type="checkbox"/>              |        |
| asarchive                    | Anti-Spam Archive                 | None              | 64K          | <input type="checkbox"/>              |        |
| authentication               | Authentication Logs               | None              | 42.5M        | <input type="checkbox"/>              |        |
| avarchive                    | Anti-Virus Archive                | None              | 64K          | <input type="checkbox"/>              |        |
| bounces                      | Bounce Logs                       | None              | 192K         | <input type="checkbox"/>              |        |
| cli_logs                     | CLI Audit Logs                    | None              | 35.6M        | <input type="checkbox"/>              |        |
| config_history               | Configuration History Logs        | None              | 18.4M        | <input type="checkbox"/>              |        |
| csn_logs                     | CSN Logs                          | None              | Not computed | <input type="checkbox"/>              |        |
| ctr_logs                     | CTR Logs                          | None              | Not computed | <input type="checkbox"/>              |        |
| dip                          | DLP Engine Logs                   | None              | 192K         | <input type="checkbox"/>              |        |
| eaas                         | Advanced Phishing Protection Logs | None              | 128K         | <input type="checkbox"/>              |        |
| encryption                   | Encryption Logs                   | None              | 192K         | <input type="checkbox"/>              |        |
| error_logs                   | IronPort Text Mail Logs           | None              | 192K         | <input type="checkbox"/>              |        |
| euq_logs                     | Spam Quarantine Logs              | None              | 192K         | <input type="checkbox"/>              |        |
| euqgui_logs                  | Spam Quarantine GUI Logs          | None              | 192K         | <input type="checkbox"/>              |        |
| ftpd_logs                    | FTP Server Logs                   | None              | 192K         | <input type="checkbox"/>              |        |
| gmarchive                    | Graymail Archive                  | None              | 64K          | <input type="checkbox"/>              |        |
| graymail                     | Graymail Engine Logs              | None              | 2.7M         | <input type="checkbox"/>              |        |
| gui_logs                     | HTTP Logs                         | None              | 10.9M        | <input type="checkbox"/>              |        |
| ipr_client                   | IP Reputation Logs                | None              | 448K         | <input type="checkbox"/>              |        |
| mail_logs                    | IronPort Text Mail Logs           | None              | 14.7M        | <input type="checkbox"/>              |        |

4.使用步骤2中的URL进行修改：

a.删除/log\_subscriptions。

b.在URL的末尾附加/log\_list?log\_type=<logname>，其中<logname>替换为Log Settings下显示的内容

列。

c.将dhXXXX-esa1.iphmx.com替换为ESA的完全限定域名(FQDN)。

**注意：**如果使用mail\_logs作为示例，[System Administration Log Subscriptions](#)将变为[System Administration Log List](#)。

5.最后，导航到修改后的URL并登录。您将进入与图像所示类似的页面，然后单击文件，下载并保存文件。

## Log Subscriptions: IronPort Text Mail Logs

| IronPort Text Mail Logs |                           |        |  |
|-------------------------|---------------------------|--------|--|
| File Name               | Date                      | Size   | All<br><input type="checkbox"/> Delete |
| mail.current            | 23 Jul 21:12 (GMT -04:00) | 188.8K | N/A                                    |
| mail.@20200531T003609.s | 20 Jul 18:00 (GMT -04:00) | 9.1M   | <input type="checkbox"/>               |
| mail.@20200530T214546.s | 31 May 00:35 (GMT -04:00) | 304K   | <input type="checkbox"/>               |
| mail.@20200529T092702.s | 30 May 21:45 (GMT -04:00) | 253.3K | <input type="checkbox"/>               |
| mail.@20200505T141141.s | 29 May 09:26 (GMT -04:00) | 1.4M   | <input type="checkbox"/>               |
| mail.@20200505T141050.s | 05 May 14:11 (GMT -04:00) | 2.4K   | <input type="checkbox"/>               |
| mail.@20200428T045153.s | 05 May 14:10 (GMT -04:00) | 332.6K | <input type="checkbox"/>               |
| mail.@20200308T035509.c | 27 Apr 16:28 (GMT -04:00) | 0B     | <input type="checkbox"/>               |
| mail.@20200308T015502.c | 27 Apr 02:35 (GMT -04:00) | 0B     | <input type="checkbox"/>               |
| mail.@20200408T182454.c | 26 Apr 18:00 (GMT -04:00) | 35.3M  | <input type="checkbox"/>               |

< Back Delete

## 从CMD下载日志

确保您具有CES ESA的CLI访问权限。有关请求CLI访问的步骤，请参阅[客户CLI访问](#)一文。

建议使用 Putty SCP(PSCP)具有SSH访问权限以便提取日志：

1. 下载PSCP[下载PuTTY](#)
2. 打开在ESA上启用的代理配置，保持代理打开。

```
f15-ssh.ap.iphmx.com - PuTTY
Using username "dh-user".
Pre-authentication banner message from server:
| THIS SYSTEM IS RESTRICTED TO AUTHORIZED USERS FOR AUTHORIZED
| USE ONLY. UNAUTHORIZED ACCESS IS STRICTLY PROHIBITED AND MAY
| BE PUNISHABLE UNDER THE COMPUTER FRAUD AND ABUSE ACT OF 1986
| OR OTHER APPLICABLE LAWS. IF NOT AUTHORIZED TO ACCESS THIS
| SYSTEM, DISCONNECT NOW. BY CONTINUING, YOU CONSENT TO YOUR
| KEYSTROKES AND DATA CONTENT BEING MONITORED. ALL PERSONS ARE
| HEREBY NOTIFIED THAT THE USE OF THIS SYSTEM CONSTITUTES
| CONSENT TO MONITORING AND AUDITING.
End of banner message from server
Authenticating with public key "rsa-key-20211216"
```

```
127.0.0.1 - PuTTY
login as: bglesa
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
Last login: Wed Jan 26 05:01:43 2022 from 10.9.73.17
AsyncOS 14.0.0 for Cisco C100V build 698

Welcome to the Cisco C100V Secure Email Gateway Virtual

NOTE: This session will expire if left idle for 30 minutes. Any uncommitted
configuration changes will be lost. Commit the configuration changes as soon as
they are made.
(Machine esa1.hc905-75.ap.iphmx.com)>
```

3.运行CMD并键入：`pscp -P port -r <user>@localhost:/mail_logs/* /path/on/local/system`

1. 端口是之前为CLI访问配置的端口。
2. /mail\_logs/表示它下载该特定文件夹下的所有文件。
3. 如果只需要下载当前文件，请键入/mail\_logs/mail.current或所需的日志。
4. 输入命令后，在请求时输入密码。

命令示例：`pscp -P 2200 -r admin@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads`

```
C:\Users\beanand>pscp -P 2200 -r bglesa@127.0.0.1:/mail_logs/mail.current C:/Users/beanand/Downloads
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
mail.current | 16561 kB | 974.2 kB/s | ETA: 00:00:00 | 100%

C:\Users\beanand>pscp -P 2200 -r bglesa@127.0.0.1:/mail_logs/ C:/Users/beanand/Downloads
Keyboard-interactive authentication prompts from server:
| bglesa@esa1.hc905-75.ap.iphmx.com's password:
End of keyboard-interactive prompts from server
warning: remote host tried to write to a file called 'mail_logs'
when we requested a file called ''.
If this is a wildcard, consider upgrading to SSH-2 or using
the '-unsafe' option. Renaming of this file has been disallowed.
mail.@20211027T160541.c | 16562 kB | 828.1 kB/s | ETA: 00:00:00 | 100%
mail.current | 16562 kB | 2366.0 kB/s | ETA: 00:00:00 | 100%

C:\Users\beanand>
```

## 相关信息

- [思科邮件安全设备 — 最终用户指南](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。