# 啟用SWG模組的最大調試日誌記錄

## 目錄



## 簡介

本檔案介紹如何在AnyConnect和思科安全使用者端(CSC)的安全Web閘道(SWG)模組上啟用最大偵錯記錄。

## 啟用最大調試日誌記錄的用例

排除以下問題時，在SWG模組上啟用最大調試日誌記錄：

- 通過強制網路門戶的熱點問題
- 外部域繞過清單未應用
- 間歇性的DNS或Web效能問題

## 在AnyConnect 4.10 MR7、CSC 5.0 MR2或更早版本上啟用最大調試日誌記錄

如果使用AnyConnect 4.10 MR7、CSC 5.0 MR2或更舊版本，請執行以下步驟。預設情況下，未啟用最大調試日誌記錄，並且無法通過Umbrella控制面板或ASA進行配置。必須手動添加"logLevel": "1"orgConfig，到檔案中的對象SWGConfig.json。如果您使用的是最新版本的AnyConnect或Cisco Secure

Client，請跳過此部分。

## SWGConfig.json的位置

- Windows(AnyConnect):

```
C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\
```

- Windows（安全客戶端）：

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

- macOS(AnyConnect):

```
/opt/cisco/anyconnect/umbrella/swg/
```

- macOS（安全客戶端）：

```
/opt/cisco/secureclient/umbrella/swg/
```

## 使調試日誌記錄具有永續性

修改的SWGConfig.json檔案僅保留到Cisco AnyConnect Umbrella模組進行下一個API同步為止。要保留此配置並防止API同步覆蓋此配置，請在資料夾中部署一個swg_org_config.flagUmbrella/data檔案。

1. 建立標誌檔案

    - **swg_org_config.flag** 在Umbrella Data資料夾中創建名為的新檔案。副檔名必須是 .flag.

    - Windows(AnyConnect):
    -
      ```
      C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\swg_org_config.fl
      ```

    - Windows（安全客戶端）：
    -
      ```
      C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\swg_org_config.flag
      ```

- macOS(AnyConnect):
- ```
  /opt/cisco/anyconnect/umbrella/data/swg_org_config.flag
  ```
- macOS（安全客戶端）：
- ```
  /opt/cisco/secureclient/umbrella/data/swg_org_config.flag
  ```

2. 複製和修改內容

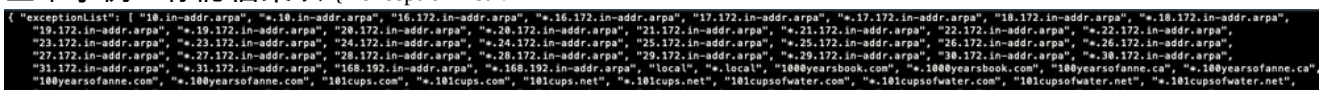
- 將對象內容從**orgConfig**檔案複製SWGConfig.json到檔案swg_org_config.flag。
- 附加為"logLevel": "1"。
- 舉例來說：

```
{
"exceptionList": [
"www.example.com",
"smh.com.au",
"*.smh.com.au",
"www.blue.com",
"*.www.blue.com",
"146.112.133.72"
// ...additional entries...
],
"failOpen": 1,
"logLevel": "1",
"swgAnycast": "146.112.255.50",
"swgDomain": "swg-url-proxy-https.sigproxy.qq.opendns.com",
"swgEchoService": "http://www.msftconnecttest.com/connecttest.txt"
}
```

- 確保標誌檔案以{ "exceptionList": [...]開頭，以"**SWGEchoService**": "**http://www.msftconecttest.com/connecttest.txt**"}結尾。
- 避免在對象之前或之後複製多餘的行。
- 錯誤地複製行(例如identity、 deviceId或)可adUserID能中斷SWG功能。

錯誤示例：標誌檔案包含鍵，例如**identity**、 deviceId或dUserID 在

正確示例：標誌檔案以 { "exceptionList":




*14970100184724*

3. 重新啟動服務

   - 重新啟動Cisco AnyConnect Secure Mobility Agent/Secure Client服務，重新啟動電腦，或者連線並斷開VPN。

4. 驗證設定

   - 在重新啟動或VPN連線/斷開連線後SWGConfig.json，開啟檔案以確認已設定SWG最大調試日誌級別。配置後，此條目將顯示在檔案中：

```
"logLevel": "1"
```

# 驗證並提供最大調試日誌

## Windows驗證

1. 開啟Windows事件檢視器。
2. 查詢與這些示例類似的日誌行。這表示已成功啟用最大調試日誌記錄。

   範例 1：

```
BRIDGE | Thread 1d18 | Connection : Resolved IP from 'swg-url-proxy-https.sigproxy.qq.opendns.com'
THREAD | Thread 1d18 | SetGUID '959bfe4d6fba87a65b433321c6748d761d9492cb'
```

   範例 2：將被代理的任何Web請求都會被記錄。未記錄根據內部/外部域清單繞過AnyConnect SWG的Web請求。

```
LISTEN | Thread 1d18 | Connection : Hostnames from KDF are login.live.com
```

3. 使用PowerShell命令將最大調試事件日誌(.evtx)轉換為txt:

```
Get-WinEvent -Path C:\Desktop\Umbrella.evtx | Format-Table -AutoSize | Out-File C:\Desktop\Umbrell
```

## macOS驗證

在Mac OSX上，可以使用此命令檢視調試日誌記錄（您可以進行升級或以文本格式寫入）。

1. 執行命令：

```
>log show --predicate 'subsystem contains "com.cisco.anyconnect.swg" || senderImagePath endswith "
```

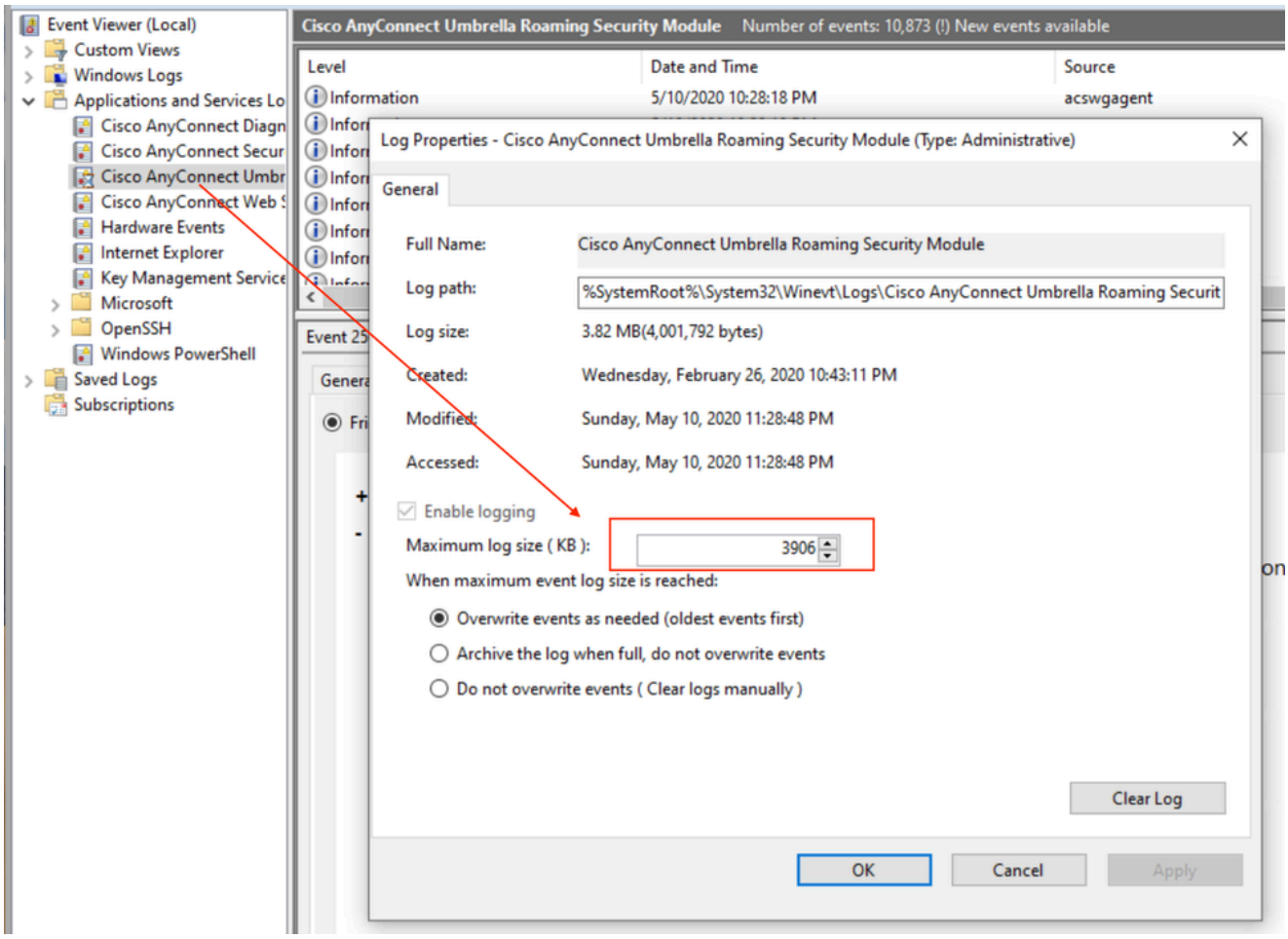
   - 在啟用最大調試日誌記錄時瀏覽purple.com時的輸出示例：

```
2022-09-19 10:51:15.627229+1000 0x16b121 Default 0x0 98970 0 acswgagent: Connection : Hostna
```

2. AnyConnect DART捆綁包包括最大調試日誌。驗證啟用後，重新建立問題，記錄時間戳、使用者體驗和涉及的域，並將此資訊與DART捆綁包一起提供支援。

## 附加說明

- 最大調試日誌記錄會生成詳細日誌。在Windows事件檢視器中配置Umbrella漫遊安全模組日誌大小以容納大型日誌，特別是對於間歇性問題。




360056784112

- 完成故障排除後swg_org_config.flag，刪除或重新命名檔案以禁用最大調試日誌記錄。

# 在CSC 5.0 MR3和AC 4.10 MR8或更高版本上啟用最大調試日誌記錄

## 概觀

從CSC 5.0 MR3和AC 4.10 MR8開始，debug logging enablement使用更簡單的過程。

變更

- 將檔案SWGConfigOverride.json（包含靜態內容）複製到SWG資料夾以啟用偵錯記錄。
- 無需從複製或修改orgConfigSWGConfig.json。此檔案的內容不會將組織更改為組織。
- 不依賴於DNS模組以執行配置同步或從標籤檔案讀取。檔案SWGConfig.json保持原樣。

## 啟用調試日誌記錄

中的配置值優先於中的值（如果存在），但只能包含和覆蓋兩個配置 — logLevel（用於啟用/禁用調試日誌記錄）和自動調**SWGConfigOverride.json**整(用於啟用/禁用傳送緩衝區自動調SWGConfig.json. The **SWGConfigOverride.json** 整)。

1. 要啟用調試日誌記錄，請SWGConfigOverride.json複製以下內容：

```
{"logLevel": "1"}
```

- 要同時啟用調試日誌記錄和自動調整，請使用：

```
{"logLevel": "1", "autotuning": "1"}
```

2. 放在**SWGConfigOverride.json**SWG資料夾中：

- Windows(AnyConnect):
  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\`
- Windows（安全客戶端）：
  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\`
- macOS(AnyConnect):
  `/opt/cisco/anyconnect/umbrella/swg/`
- macOS（安全客戶端）：
  `/opt/cisco/secureclient/umbrella/swg/`

3. 重新啟動SWG或Umbrella服務，或重新啟動系統。

- macOS:停止並啟動AnyConnect或安全客戶端代理。
- Windows:通過服務MMC管理單元(「開始」>「運行」>「Services.msc」)重新啟動或停止/啟動安全Web網關（4.10.x版中的acswgagent在5.x版中生成/csc_swgagent）服務。

---

附註：仍支援啟用調試日誌記錄的舊方法，並且仍然可以遵循該方法，並且它是5.0 MR3或4.10 MR8以上客戶端的唯一選項。

---

# 配置與操作說明

- 檔案SWGConfig.json（區分大小寫）。使用"logLevel": "1"，雙引號。
- 值logLevel是字串1，而不是整數，因此它必須是帶雙引號的"1"。
- 文件swg_org_config.flag，必須具有.flag副檔名，不.txt是。
- 最大調試日誌記錄會生成非常詳細的日誌。僅當由Umbrella支援工程師請求時，啟用最大調試日誌記錄。
- 檔案swg_org_config.flag包含繞過的域的靜態清單，並且不會與Dashboard > Deployments > Domain Management中列出的外部域同步。

## 相關資訊

- 思科技術支援與下載
- Cisco Secure Access幫助中心
- Cisco SASE設計手冊

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。