Enable Maximum Debug Logging on AnyConnect SWG Module

Contents

Introduction

This document describes how to enable maximum debug logging on the Secure Web Gateway (SWG) module for AnyConnect and Cisco Secure Client (CSC).

Use Cases for Enabling Maximum Debug Logging

Enable maximum debug logging on the SWG module when troubleshooting issues such as:

- Hotspot problems via Captive Portal
- External Domain Bypass List not applying
- Intermittent DNS or web performance issues

Enable Maximum Debug Logging on AnyConnect 4.10 MR7, CSC 5.0 MR2, or Older

If you use AnyConnect 4.10 MR7, CSC 5.0 MR2, or an older version, perform these steps. By default, maximum debug logging is not enabled, and configuration is not possible via the Umbrella dashboard or ASA. You must manually add `"logLevel": "1"` to the `orgConfig` object in the `SWGConfig.json` file. If you are using latest version of AnyConnect or Cisco Secure Client, please skip this section.

Location of SWGConfig.json

- Windows (AnyConnect):

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

- Windows (Secure Client):

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

- macOS (AnyConnect):

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

- macOS (Secure Client):

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

Make Debug Logging Persistent

The modified SWGConfig.json file remains only until the next API sync by the Cisco AnyConnect Umbrella module. To persist this configuration and prevent it from being overwritten by API sync, deploy a swg_org_config.flag file in the Umbrella/data folder.

1. **Create the Flag File**

   - Create a new file named **swg_org_config.flag** in the **Umbrella Data** folder. The file extension must be .flag.

   - Windows (AnyConnect):

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

   - Windows (Secure Client):

   - ```
     C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\swg_org_config.flag
     ```

   - macOS (AnyConnect):

-

  `/opt/cisco/anyconnect/umbrella/data/swg_org_config.flag`

- macOS (Secure Client):
-

  `/opt/cisco/secureclient/umbrella/data/swg_org_config.flag`

2. **Copy and Modify Content**

   - Copy the contents of the **orgConfig** object from the SWGConfig.json file to the swg_org_config.flag file.
   - Append with "logLevel": "1".
   - For example:

```
{
"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"
}
```

   - Ensure the flag file starts with { "exceptionList": [...] and ends with "**SWGEchoService": "http://www.msftconecttest.com/connecttest.txt"}.**
   - Avoid copying extra lines before or after the object.
   - Incorrectly copying lines such as identity, deviceId **,** or adUserID can break SWG functionality.

Incorrect Example: The flag file contains keys like **identity**, deviceId, or dUserID prior to the { "exceptionList":

Correct Example: The flag file starts with { "exceptionList":

3. **Restart Service**

    - Restart the Cisco AnyConnect Secure Mobility Agent/Secure Client service, reboot the machine, or connect and disconnect the VPN.

4. **Verify Configuration**

    - After restart or VPN connect/disconnect, open the SWGConfig.json file to confirm the SWG max debug log level is set. When configured, this entry appears in the file:

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

Verification and Providing Maximum Debug Logs

Windows Verification

1. Open **Windows Event Viewer**.
2. Look for log lines similar to these examples. This indicates Max Debug logging has been enabled successfully.

    Example 1:

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

    Example 2: Any web request being proxied is logged. Web requests bypassing AnyConnect SWG as per Internal / External Domain List is not logged.

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

3. Use the PowerShell command to convert max debug event logs (.evtx) into txt:

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

macOS Verification

On Mac OSX, the debug logging can be viewed with this command (you can grep or write them in txt).

1. Run the command:

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

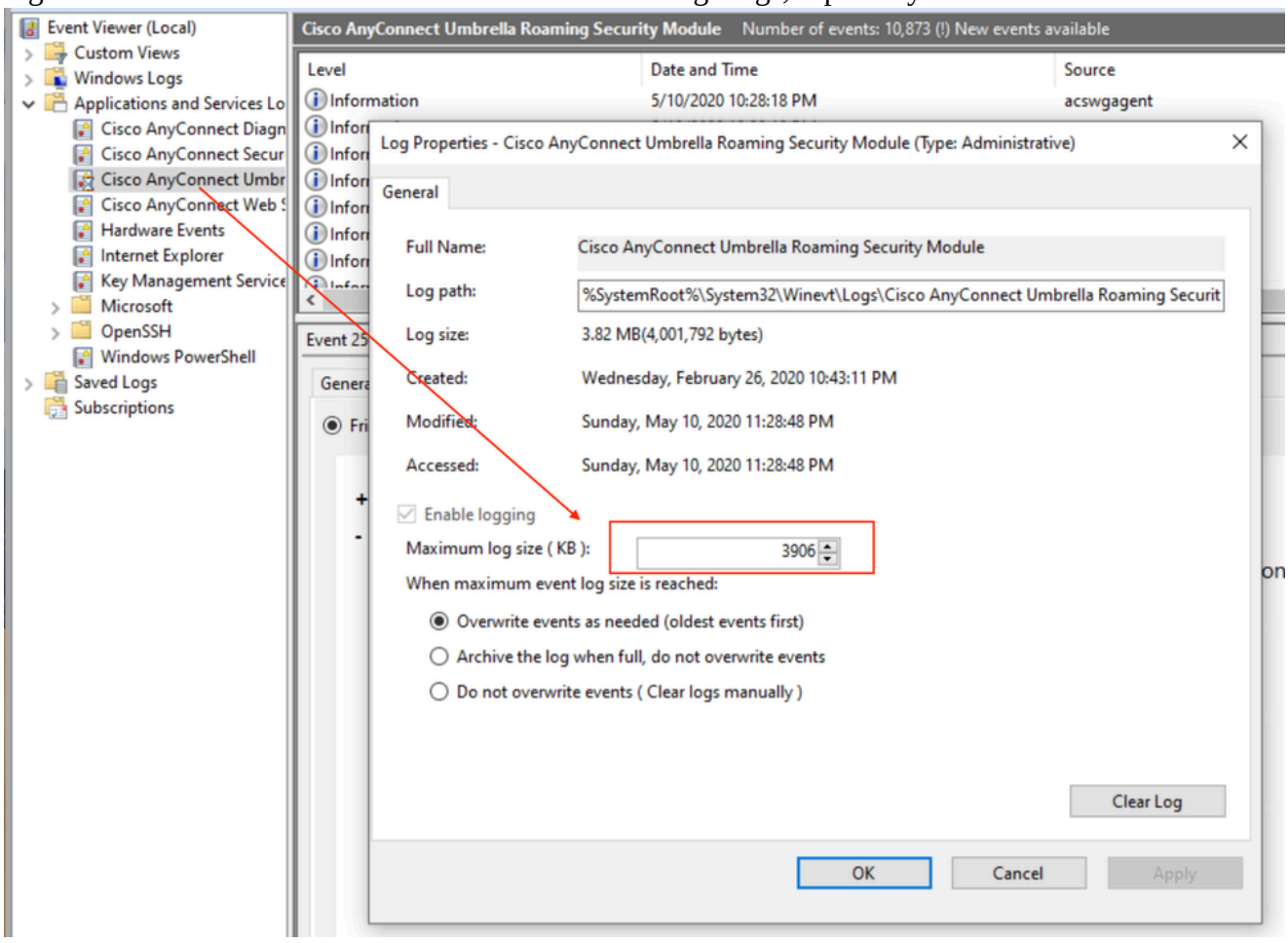
- Example output when browsing purple.com while Max Debug logging is enabled:

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

2. The AnyConnect DART Bundle includes Maximum Debug logs. After verifying enablement, recreate the issue, record the timestamp, user experience, and domain in question, and provide this information along with the DART Bundle to support.

Additional Notes

- Maximum debug logging generates verbose logs. Configure the Umbrella Roaming Security Module log size in Windows Event Viewer to accommodate large logs, especially for intermittent issues.



360056784112

- Remove or rename the swg_org_config.flag file to disable Max Debug logging when troubleshooting is complete.

Enable Maximum Debug Logging on CSC 5.0 MR3 and AC 4.10

MR8 or Later

Overview

Starting with CSC 5.0 MR3 and AC 4.10 MR8, debug logging enablement uses a simpler process.

Changes

- Copy the SWGConfigOverride.json file (with static content) to the SWG folder to enable debug logging.
- No need to copy or modify the orgConfig from SWGConfig.json. The contents of this file won't change org to org.
- No dependency on the DNS module to perform config sync or read from the flag file. The SWGConfig.json file remains untouched.

Enable Debug Logging

The config value in **SWGConfigOverride.json** takes precedence over the value (if present) in SWGConfig.json. The SWGConfigOverride.json can contain and override only two configs – logLevel (to enable/disable debug logging) and autotuning (to enable/disable send buffer autotuning).

1. To enable debug logging, copy SWGConfigOverride.json with the content:

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

   - To enable both debug logging and autotuning, use:

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

2. Place **SWGConfigOverride.json** in the SWG folder:

- Windows (AnyConnect):

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

- Windows (Secure Client):

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

- macOS (AnyConnect):

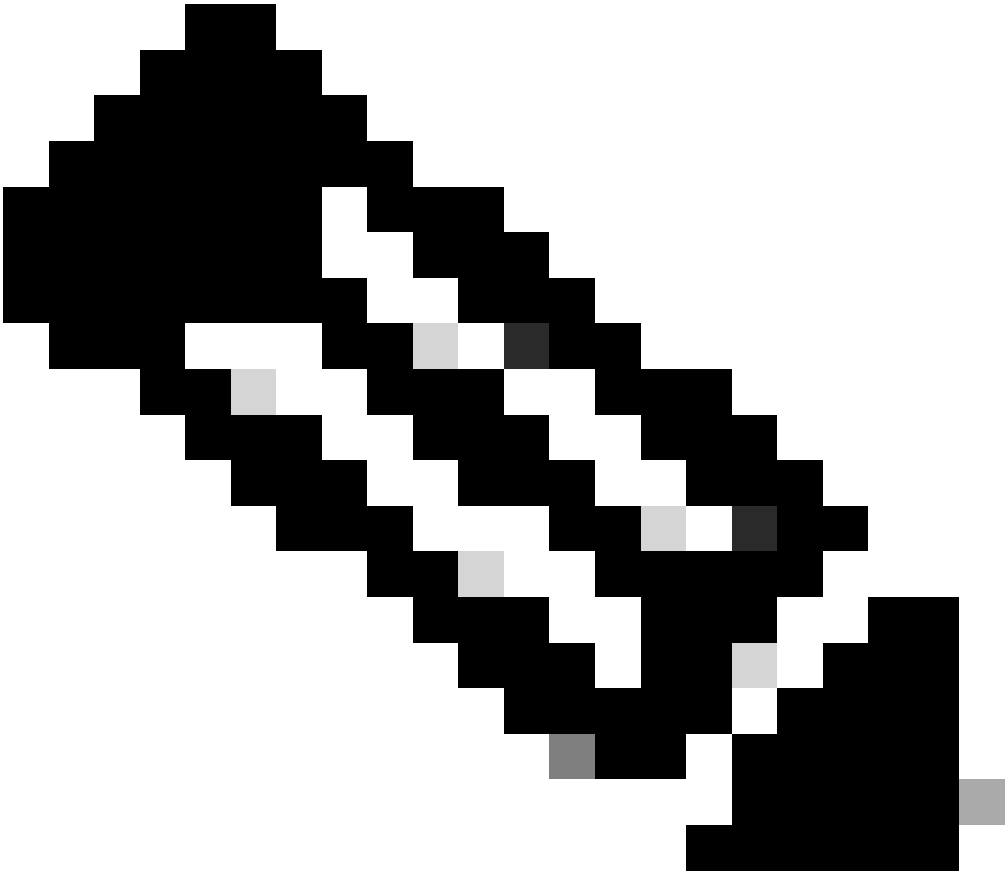
  `/opt/cisco/anyconnect/umbrella/swg/`

- macOS (Secure Client):

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

3. Restart the SWG or Umbrella service, or restart the system.

- macOS: Stop and start the AnyConnect or Secure Client agent.
- Windows: Restart or stop/start the Secure Web Gateway (acswgagent in 4.10.x builds /csc_swgagent in 5.x builds) service via the Services MMC snap-in (**Start > Run > Services.msc**).



Note: The older method of enabling debug logging is still supported and can still be followed and is the only option for clients older than 5.0 MR3 or 4.10 MR8.

Configuration and Operational Notes

- The SWGConfig.json file is case sensitive. Use "logLevel": "1" with double quotes.
- The logLevel value is a string 1, not an integer, therefore it has to be "1" with double quotes.
- The swg_org_config.flag file must have a .flag extension, not .txt.
- The max debug logging generates extremely detailed logs. Enable maximum debug logging only if requested by an Umbrella Support engineer.
- The swg_org_config.flag file contains a static list of bypassed domains and does not sync with External Domains listed in **Dashboard > Deployments > Domain Management**.