李先生，您好：

感谢您的反馈，经您的确认，目前问题已解决，此 case 将做关闭处理，以下为案例总结，请您知悉：

Case No：CAS-11061-X2B4F7

问题描述：

==========

用户反馈 V2020-L 和 V2022-L 版本系统连接 WIFI 后异常断开问题，接口人称涉及 10 多台设备，需要协助分析处理。

问题分析：

==========

从日志来看，wlan 发起 disconnect 的原因是 profile state change，存在另外一个 process rpc call wlan deleteprofile。发起该动作的 process 为 wlan_control.exe，已告知用户进行排查。

案例总结：

==========

用户明确问题已解决。经与用户沟通，该 case 将做关闭处理。后续如有其他任何问题，可随时与我们联系，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: 李小川 <lixc6@sz.icbc.com.cn>
发送时间: 2024 年 6 月 24 日 9:45
收件人: Li Qi <liqi@cmgos.com>
抄送: 许翔 <555104552@mails.icbc>
主题: 回复: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

已确认此为问题原因，谢谢！

-----原始邮件-----

发件人: "Li Qi" <liqi@cmgos.com>
发送时间: 2024-06-21 14:03:16
收件人: "李小川" <李小川.深圳分行金融科技部@工商银行.icbc>,"许翔" <许翔.软件开发中心系统一部 2@工商银行.icbc>
抄送: "ICBC_Notification" <ICBC_Notification@cmgos.com>
主题: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生 & 许先生:
经分析您上传的日志来看，wlan 发起 disconnect 的原因是 profile state change，存在另外一个 process rpc call wlan deleteprofile

Interface:Intel(R) Wi-Fi 6 AX201 160MHz
Interface GUID: b46a0c92-0e6e-4407-b7da-c19f974aa7ec
Connection Mode:**使用配置文件手动连接**
Profile:ASTROA0001
SSID:ASTROA0001
BSS Type:Infrastructure
Session Duration: 0 hours 0 minutes 48 seconds
Disconnect Reason:**网络被用户断开。**

EventId	Time	Message
8000	2024-06-18T10:23:18	[+]WLAN 自动配置服务已开始连接无线网络。
11000	2024-06-18T10:23:18	[+]已开始无线网络关联。
11001	2024-06-18T10:23:20	[+]无线网络关联成功。
11010	2024-06-18T10:23:20	[+]无线安全功能已启动。
12011	2024-06-18T10:23:20	[+]无线 802.1x 身份验证已开始。
2087	2024-06-18T10:23:20	[+]用户输入的凭据。
107	2024-06-18T10:23:43	[+]正在将用户名 000605538 的凭据发送到服务器。域:
100	2024-06-18T10:23:43	[+]用户 000605538 在域 中的身份验证成功。
2089	2024-06-18T10:23:43	[+]EAP 会话将在身份验证阶段完成。
100	2024-06-18T10:23:43	[+]EAP 方法类型 25 的身份验证成功。
12012	2024-06-18T10:23:43	[+]无线 802.1x 身份验证成功。
11005	2024-06-18T10:23:43	[+]无线安全功能成功。
8001	2024-06-18T10:23:43	[+]WLAN 自动配置服务已成功连接到无线网络。
11004	2024-06-18T10:24:06	[+]无线安全功能已停止。
8003	2024-06-18T10:24:06	[-]WLAN 自动配置服务已成功从无线网络断开。 网络适配器: Intel(R) Wi-Fi 6 AX201 160MHz 接口 GUID: {b46a0c92-0e6e-4407-b7da-c19f974aa7ec} 连接模式: 使用配置文件手动连接 配置文件名称: ASTROA0001 SSID: ASTROA0001 BSS 类型: Infrastructure 原因: 网络被用户断开。

查看 wlan profile 只看到 ICBCOTP 的 profile，没有看到有 ASTROA0001

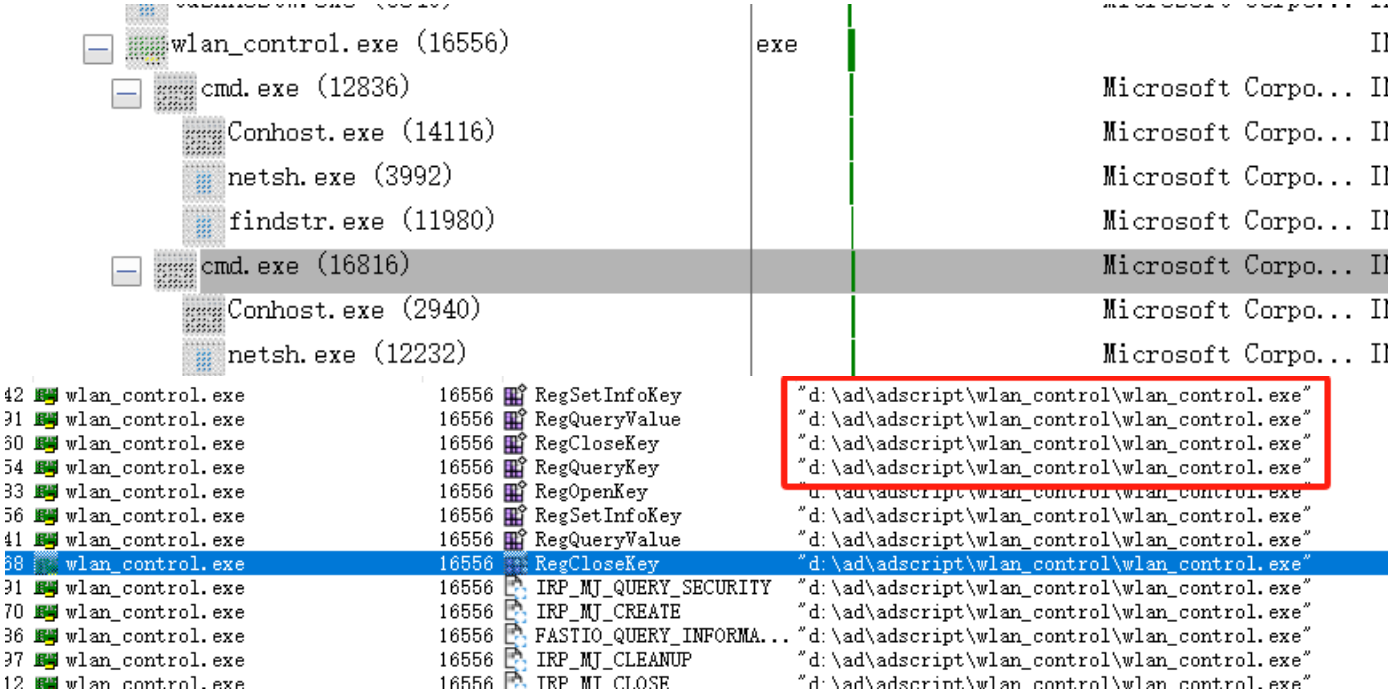
```
========================== 显示配置文件 ==========================
==================================================================


接口 WLAN 上的配置文件:

组策略配置文件(只读)
---------------------------
    <无>

用户配置文件
-------------
    所有用户配置文件 : ICBCOTP
```

294924 [3]0FA0.0FF0::06/18/24-10:24:05.9298750 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] RpcCall DeleteProfile from client 12232
294930 [3]0FA0.0FF0::06/18/24-10:24:05.9299127 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] **Profile State changed. Profile: ASTROA0001 Update State: Deleted (Single SSID: false)**

295411 [3]0FA0.0F28::06/18/24-10:24:05.9353095 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] Disconnecting. Interface = Intel(R) Wi-Fi 6 AX201 160MHz. {b46a0c92-0e6e-4407-b7da-c19f974aa7ec}
295424 [3]0FA0.0F28::06/18/24-10:24:05.9353160 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] **Begin Disconnect API {b46a0c92-0e6e-4407-b7da-c19f974aa7ec}, Intel(R) Wi-Fi 6 AX201 160MHz**
295507 [3]0FA0.0F28::06/18/24-10:24:05.9353417 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] FSM Current state Connected , event Cmd_Disconnect {b46a0c92-0e6e-4407-b7da-c19f974aa7ec}, Intel(R) Wi-Fi 6 AX201 160MHz
296028 [2]0798.1044::06/18/24-10:24:05.9357623 [Microsoft-Windows-WiFiNetworkManager] WlanMgr - 已收到 wlan 通知: wlan_notification_acm_disconnecting
296612 [0] 0FA0.0F28::06/18/24-10:24:05.9366494 [extsta] assocmgr_c3623 ExtSTAIoctlDisconnect() - **IOCTL_DOT11_DISCONNECT**
296613 [0]0FA0.0F28::06/18/24-10:24:05.9366522 [Microsoft-Windows-NWiFi/Diagnostic] IOCTL_DOT11_DISCONNECT 0xFFFFC10ECB8EC010, {b46a0c92-0e6e-4407-b7da-c19f974aa7ec}
296655 [0] 0FA0.0F28::06/18/24-10:24:05.9367445 [WdiLib] Unknown_cxx00 WDI_TLV::GENERATOR::GenerateMessage() - [TRACE]Generate WDI_TASK_DISCONNECT
297845 [1] 0004.035C::06/18/24-10:24:05.9394050 [WdiLib] Unknown_cxx00 WDI_TLV::PARSER::ParseAggregateField() - [TRACE]Parsing WDI_INDICATION_DISASSOCIATION::WDI_TLV_DISCONNECT_DEAUTH_FRAME
297989 [7]0FA0.0FF0::06/18/24-10:24:05.9396074 [Microsoft-Windows-WLAN-Autoconfig/Diagnostic] Received Security Packet: PORT_DOWN {b46a0c92-0e6e-4407-b7da-c19f974aa7ec}, Intel(R) Wi-Fi 6 AX201 160MHz

从日志来看，**Profile: ASTROA0001 被删除了，**有可能会存在三方工具将 profile 删除
查看 promon 日志看到 10::24:04:9716190，cmd 执行了 netsh wlan delete profile name="ASTROA0001"，这个 cmd 是被 wlan_control.exe 调用起来的，看上去它会在定期或者在无线连上的时候检查所有用户配置文件
10:24:04.9716190 cmd.exe 16816 Load Image 5768 C:\Windows\SysWOW64\cmd.exe SUCCESS Image Base: 0x11e0000, Image Size: 0x59000 0.0000000 C:\Windows\system32\cmd.exe /c **netsh wlan delete profile name="ASTROA0001"**
10:24:04.9717666 cmd.exe 16816 Load Image 5768 C:\Windows\System32\ntdll.dll SUCCESS Image Base: 0x7ffec6860000, Image Size:

0x1ee000 0.0000000 C:\Windows\system32\cmd.exe /c netsh wlan delete profile name="ASTROA0001"
10:24:04.9718881 cmd.exe 16816 Load Image 5768 C:\Windows\SysWOW64\ntdll.dll SUCCESS Image Base: 0x77730000, Image Size: 0x19d000
0 0.0000000 C:\Windows\system32\cmd.exe /c netsh wlan delete profile name="ASTROA0001"



路径为：D:\ad\adscript\wlan_control\wlan_control.exe，请查看此应用是否正常，执行逻辑中不要去 delete profile

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2024 年 6 月 12 日 15:05
收件人: '李小川' <lixc6@sz.icbc.com.cn>; '许翔' <555104552@sdc.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>

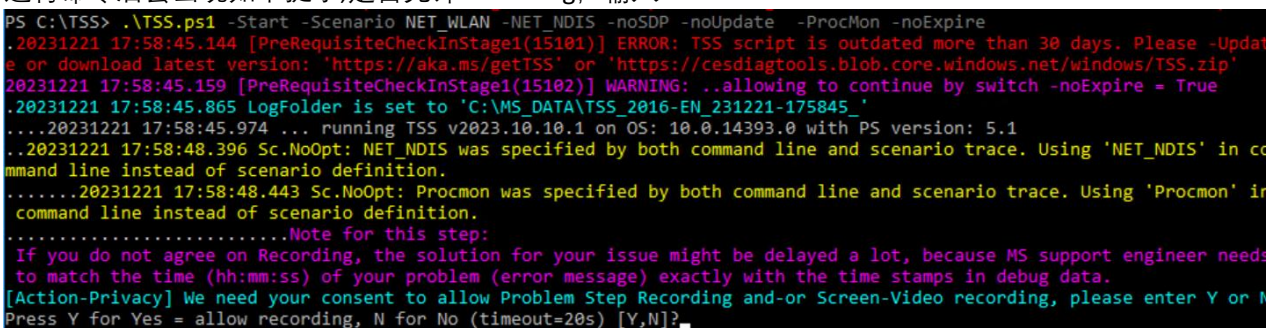
主题: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生 & 许先生:
查看您分析的网络报告，从网络包来看，是终端主动发起的 deauthentication 报文。关于报告中提到的 1015 事件，一般意味着配置应用到了网络接口上，目前看不出来和断联有什么关系。因此还是按照之前的邮件内容进行 TSS 的收集，供后续分析。

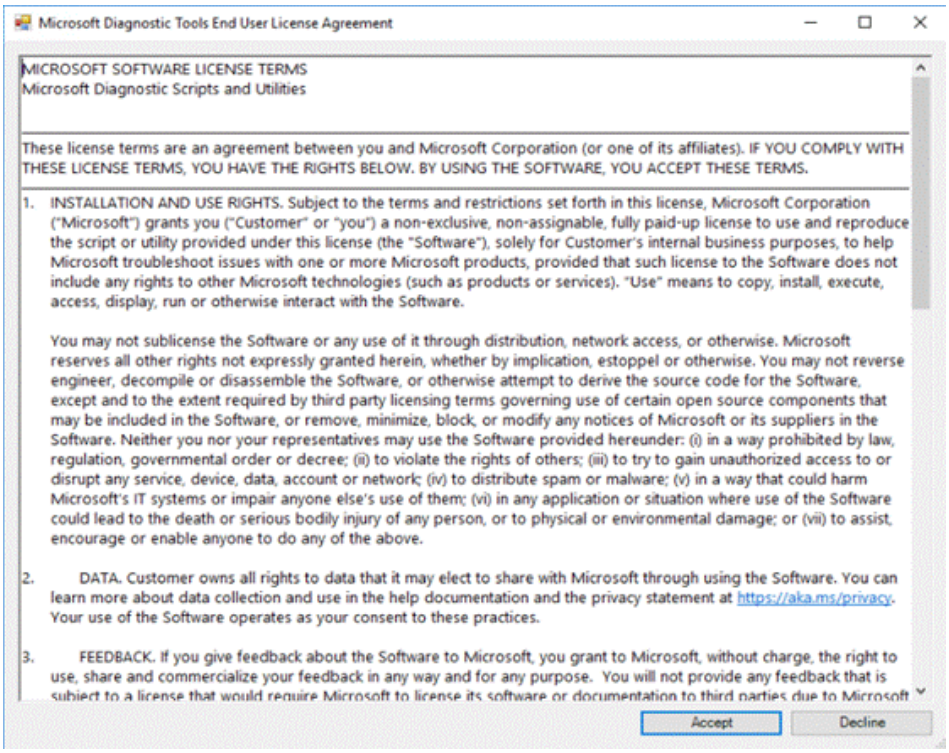
请继续协助收取下面的日志:
1.请先从这个链接下载 TSS 工具到有问题的客户端，并解压缩。
https://cduc.cmgos.com/download.php?id=1345&token=aXNDZiNVUb0rmJdXaQ2IcLi0naWSf6BP

2. 在客户端使用管理员账号运行 Powershell , cd 到解压的 TSS 路径下，然后执行命令:
Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force
.\TSS.ps1 -Start -Scenario NET_WLAN -noSDP -noUpdate

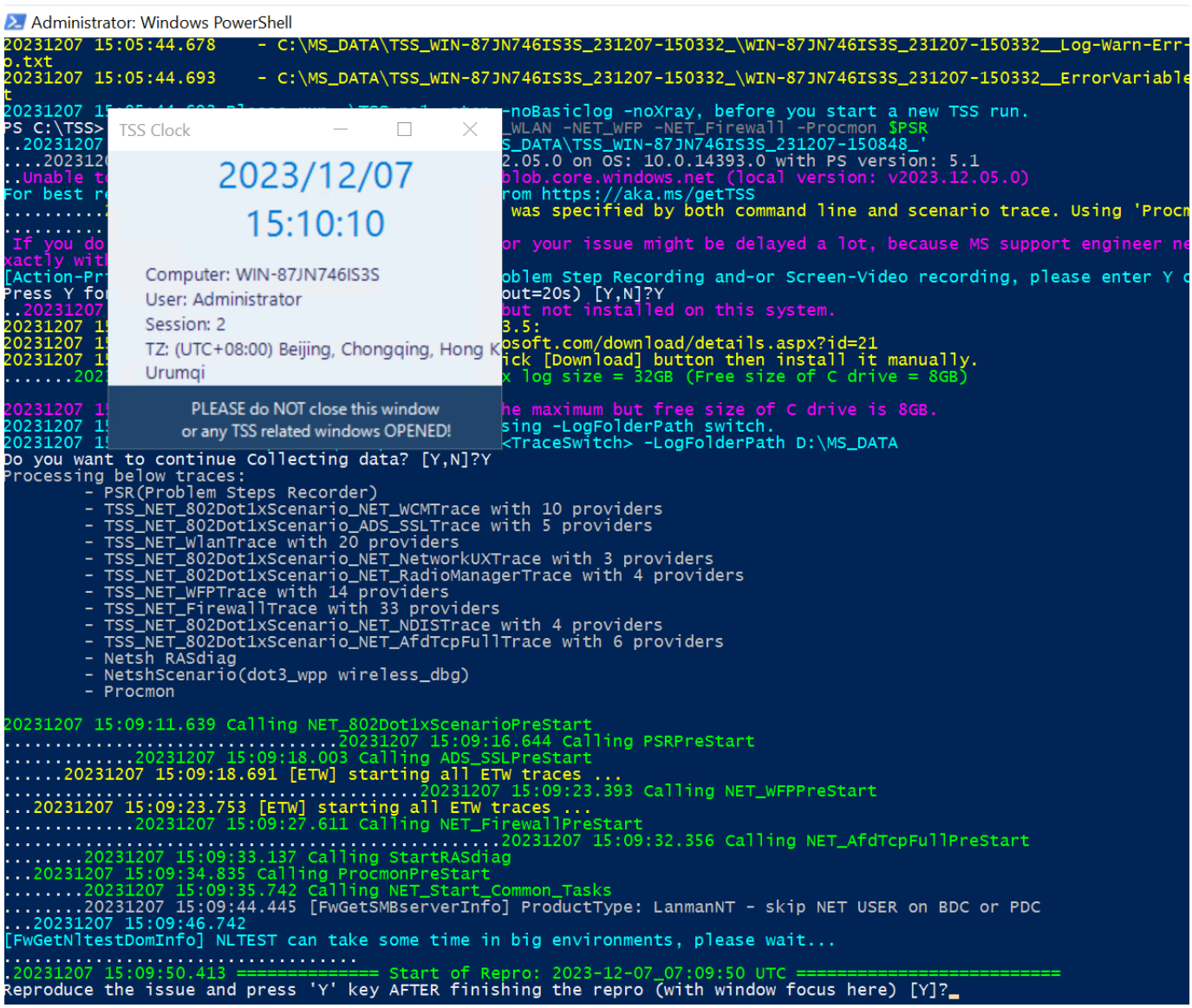
运行命令后会出现如下提示,是否允许 recording，输入 Y



3. 第一次运行 TSS 运行后，会出现 EULA 窗口，点击“Accept”继续，后续不会继续出现



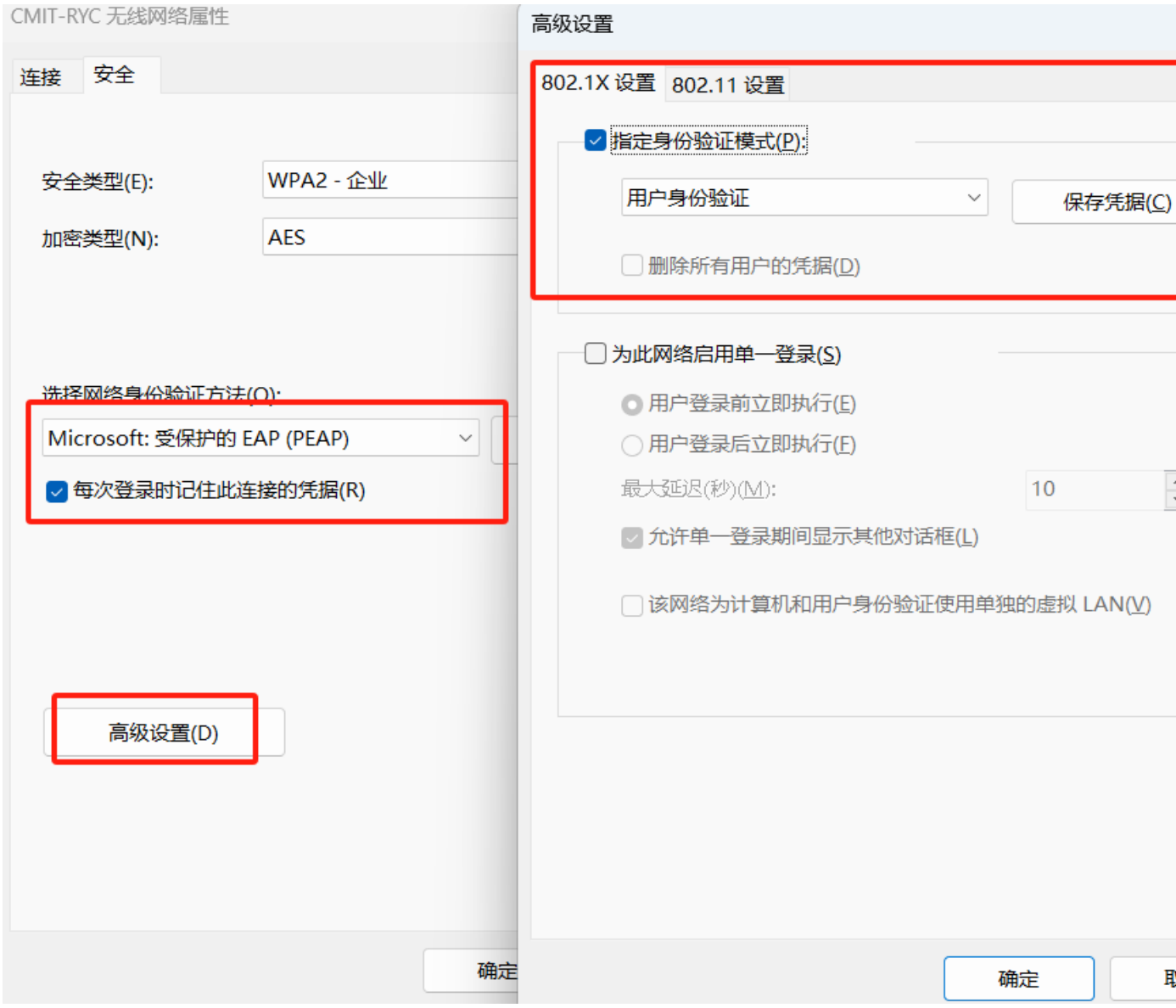
4.等 TSS 脚本运行完毕，到如下界面，到这一步**不要输入 Y，重新连接无线复现断开问题**:



5.问题复现后输入 Y 停止收集日志，等待脚本运行完毕，这可能需要一段时间，日志会存放在 c 盘下的 MS_DATA 文件夹下

6.**再收集一份正常连接的日志**

7.**wifi 设置的截图请提供一下**



李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信
CMIT

发件人: Li Qi
发送时间: 2024 年 4 月 11 日 13:25

收件人: '李小川' <lixc6@sz.icbc.com.cn>
抄送: 许翔 <555104552@sdc.com>; ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生，您好:
感谢您的反馈。您可以尝试分卷压缩上传或者通过别的工具（如百度网盘）给我也可以，谢谢

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: 李小川 <lixc6@sz.icbc.com.cn>
发送时间: 2024 年 4 月 11 日 12:44
收件人: Li Qi <liqi@cmgos.com>
抄送: 许翔 <555104552@sdc.com>
主题: 回复: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

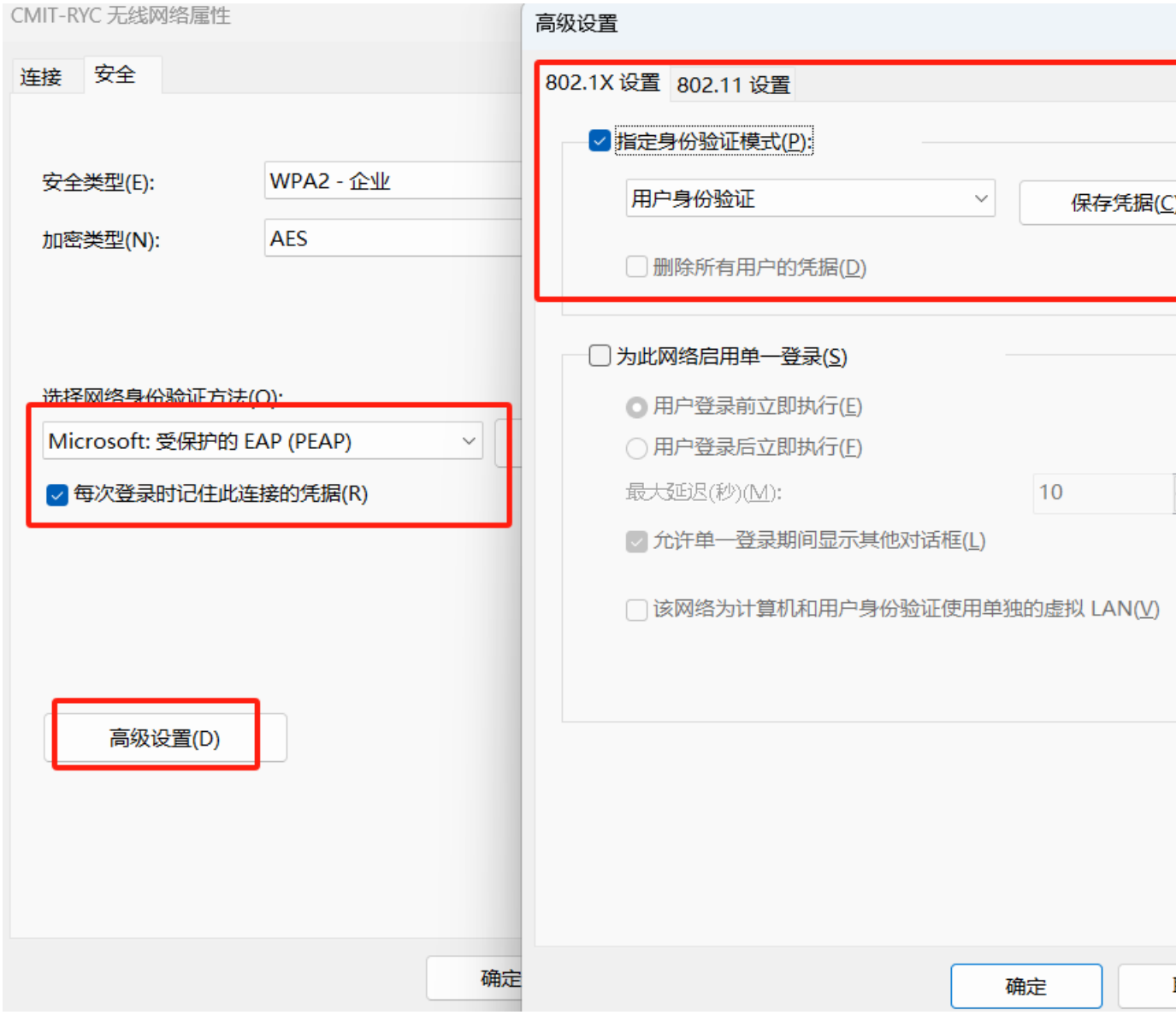
内网无法发出，压缩了也超了。

-----原始邮件-----

发件人: "Li Qi" <liqi@cmgos.com>
发送时间: 2024-04-11 09:53:42
收件人: "李小川" <李小川.深圳分行金融科技部@工商银行.icbc>
抄送: "许翔" <许翔.软件开发中心系统一部 2@工商银行.icbc>,"ICBC_Notification" <ICBC_Notification@cmgos.com>

主题: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生，您好:
电话未联系到您，您可以将日志压缩之后按如下方法上传。
再确认一下，当前需要收集的日志为 Procmon，Wifiwithcapi，Netmon 三种，分别在正常连接和意外断开两种场景下收取，共计 6 份日志。另外请将这张截图反馈给我。谢谢



日志上传:

您可以登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息

用户名：icbcli01

密码：icbcli01

添加文件后点击上传文件

注意，如果遇到如下所示页面，点击后退即可看到页面

==========

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: 李小川 <lixc6@sz.icbc.com.cn>
发送时间: 2024 年 4 月 10 日 18:17
收件人: Li Qi <liqi@cmgos.com>
抄送: 许翔 <555104552@sdc.com>
主题: 回复: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

附件太大了，日志几百兆到 1G 的，没法儿发呀。

TO 许翔

这个有没上门协助的?

-----原始邮件-----

发件人: "Li Qi" <liqi@cmgos.com>
发送时间: 2024-04-10 17:17:35
收件人: "win10 技术支持" <win10 技术支持.软件开发中心系统一部@工商银行.icbc>,"56900502@qq.com" <56900502@qq.com>,"李小川" <李小川.深圳分行金融科技部@工商银行.icbc>
抄送: "ICBC_Notification" <ICBC_Notification@cmgos.com>
主题: 【外来邮件，注意核实】回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生，您好:
请参照以下内容。
邮件附件请登录 https://cduc.cmgos.com 下载。

账号信息如下：

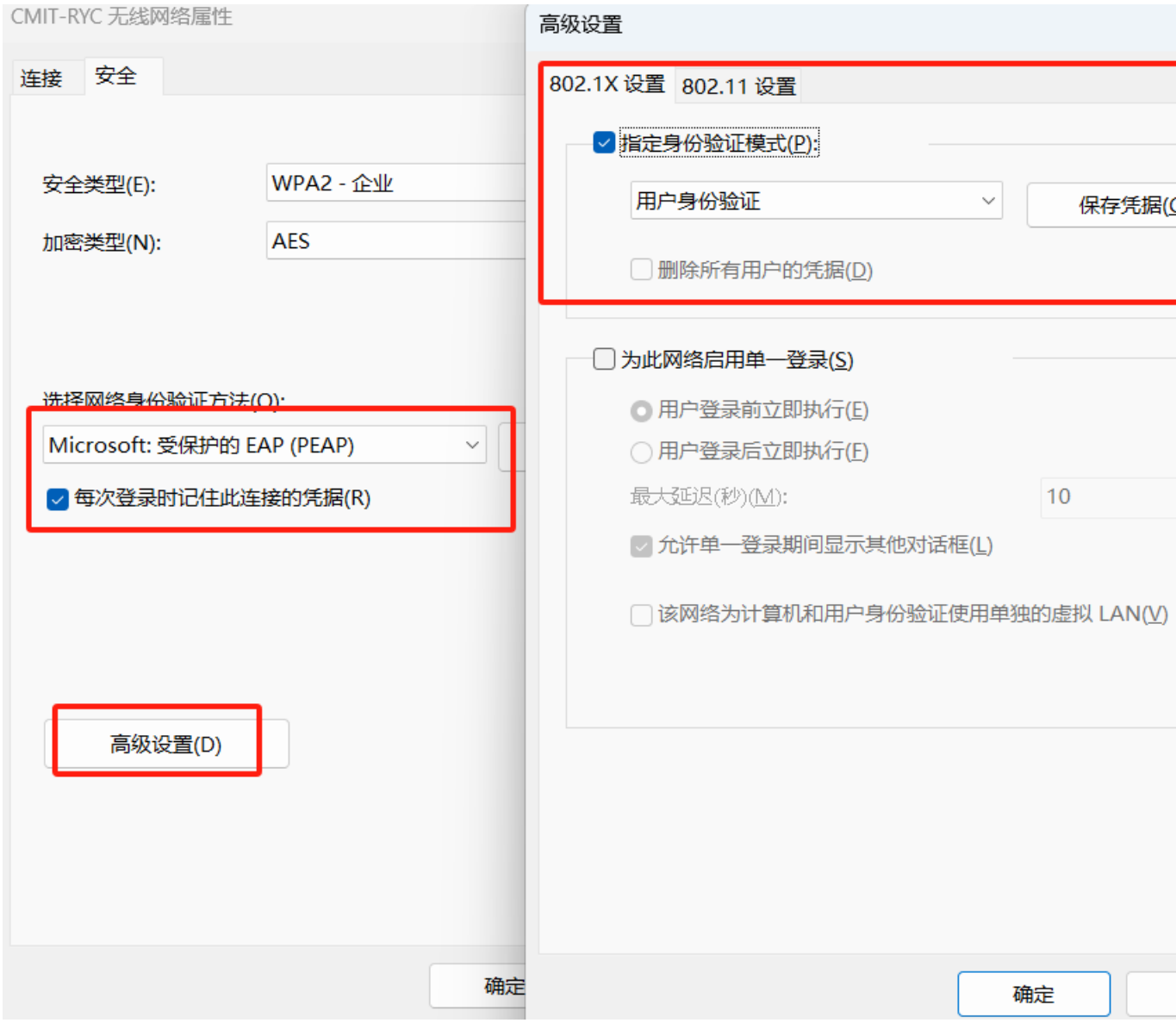
用户名：icbcli01

密码：icbcli01

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2024 年 4 月 2 日 15:41
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>; '56900502@qq.com' <56900502@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生，您好：
如刚才沟通，我将于 17 点和您联系，请查看如下截图设置，并反馈设置截图：



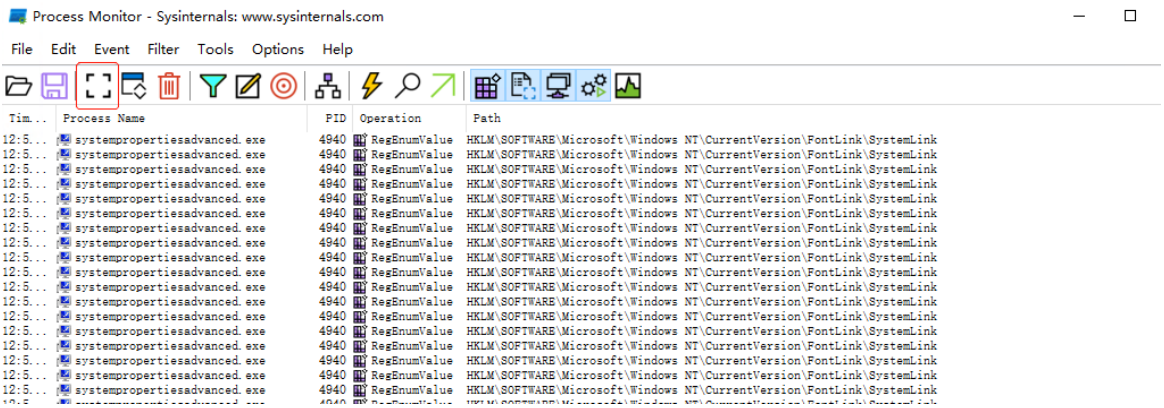
- 请按照如下方式收取日志：

1. 请从附件下载 WLANwith capi2.txt 文件，并将其后缀名更改为.bat.
2. 右击改 BAT 文件，请以管理员身份运行。
3. 在看到以下界面时，离开 CMD 页面，尝试**重现 WIFI 连接后断开的问题以及正常连接 WIFI**。
4. 问题重现后，回到 CMD 页面，按任意键继续日志收集

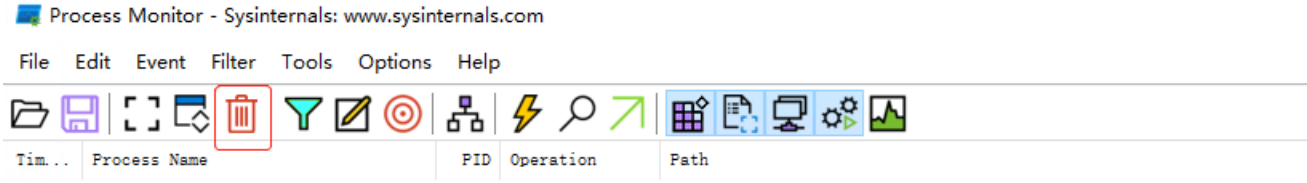
日志收集完成，请将 C:\mslog 和 c:\drivers_tablet.etl 文件上传给我做分析。谢谢!

- 请按如下步骤收取 procmon 日志：

1. 下载附件工具并保存至本地
2. 解压完成后，双击执行 procmon64.exe
3. 显示如下界面，并点击 capture 按钮，先暂停收集，准备进行捕获



4. 点击 clear 按钮，清空当前窗口，重新点击 capture 按钮，开始捕获



5. 再次点击 capture 按钮，复现 **WIFI 连接后断开的情况和正常连接 WIFI 的两种情况**后点击停止捕获
6. 点击 File menu, 点击 Save. 选择"All events" and "Native Process Monitor Format (PML)" 点击 OK

- 请在**正常与问题两台电脑**上按照以下步骤收集网络包。

1) 请安装网络收集工具，地址如下。

http://www.microsoft.com/download/en/details.aspx?id=4865

2) 请在客户端运行 network monitor, 并在此页面选择无线网卡 （如下图）。新建一个 Capture (New Capture)。然后点击 Start 开始抓包。然后按照 process monitor 的收集方法收集 process monitor。，

Properties | P-Mode

Friendly Name	Description	IPv4 Address	IPv6 Address
☑ Ethernet	Intel(R) Ethernet Connection I219-LM	None	fe80::587:ac1:9a7d:d9cf%15
☐ Ethernet 2	ThinkPad Cable dock	None	None
☑ Ethernet 4	PANGP Virtual Ethernet Adapter	None	fe80::c905:cb5d:84b5:bc68%20
☑ Local Area Connection* 1	Microsoft Wi-Fi Direct Virtual Adapter #2	None	fe80::d1e9:ff31:3c31:7b2%11
☑ Local Area Connection* 9	Microsoft Wi-Fi Direct Virtual Adapter	None	fe80::cce7:1ea0:9202:739%7
☑ Teredo Tunneling Pseudo-Interface	Microsoft Teredo Tunneling Adapter	None	2001:0:9d38:6abd:1cc4:c930:5823:
☑ Wi-Fi	Intel(R) Dual Band Wireless-AC 8260	10.86.152.50	2404:f801:18:43c:e1a2:908d:3a80:

日志上传：

您可以登陆 https://cduc.cmgos.com，通过数据上传系统上传您所收集的日志信息

用户名：icbcli01

密码：icbcli01

添加文件后点击上传文件

注意，如果遇到如下所示页面，点击后退即可看到页面

==========

==========

在向 CMIT 提供日志和数据前，请阅读并接受邮件下方隐私声明。

隐私声明

为向您提供本产品的相关技术支持及相关服务，您需要在同意本声明的前提下向神州网信提供为解决系统故障必要的数据和信息，包括但不限于与您相关的个人数据和隐私信息。通常情况下，我们仅需要如下数据以使我们的服务能够更好地满足您的需求：内存转储文件、注册表信息、组策略信息、事件日志、安装应用列表、驱动信息、网络日志或系统补丁等。

神州网信承诺将采取商业上可行及必要措施保护用户提供给神州网信的数据和信息，且仅在解决问题过程中使用。

神州网信保证不对外公开或向第三方提供、公开或共享您提供的数据和信息。

在以下情况下，神州网信对您的数据和信息的披露将不视为违约，具体包括：

(1) 神州网信已获得您的明确授权；

(2) 根据适用法律的要求，神州网信负有披露义务的；

(3) 司法机关或行政机关基于法定程序要求神州网信提供的；

(4) 为维护社会公共利益及神州网信合法权益，在合理范围内进行披露的。

(5) 为了解决您的系统故障问题，神州网信可能会与神州网信的分包商披露您提供的数据和信息。在此情况下，第三方会承担与神州网信同等的隐私保护责任的，神州网信会在合理范围内对您的信息进行披露。

如果您欲提供的数据和信息中包含对您重要的保密信息以及商业秘密，在您向神州网信提供上述数据和信息前，务必对上述数据和信息进行脱敏处理，否则请不要提供该信息给神州网信。作为一家商业软件公司，神州网信在商业可行的前提下，已为用户的数据和信息保护做了极大的努力，但是仍然不能保证现有的安全技术措施使您的数据和信息等不受任何形式的损失。您对上述情况充分知情，且不会因此追究神州网信的法律责任。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2024 年 3 月 29 日 11:24
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>; '56900502@qq.com' <56900502@qq.com>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

李先生，您好：

如昨天电话沟通，当前您遇到的问题与之前行内遇到的“OTP 首次无法接问题”，有相似之处。因此请先参照之前案例处理的结论来进行排查，以下为之前案例的总结文档，供您参考：

问题描述：

==========

首次无法连接 OTP 无线，连接后报错。

报错提示为：无法连接到这个网络

目前所有 OEM 的出厂设备均出现此问题，设备包括联想、戴尔。

基于问题用户反馈的问题，对反馈问题进行复现。该场景描述如下：

用户（或 OEM 厂商）使用符合工行要求的定制版镜像安装操作系统

连接有线，创建并使用本地管理员账号登陆操作系统，并进行加域操作

重启电脑，使用域用户账号登陆操作系统，并安装配置必要的 OA 软件，安装配置过程尚不明确（其中是否连接过有线，是否连接过 ewifi-工行通过域认证的无线网络，是否访问过文件服务器均不确定）

再次重启电脑，成功登陆之后，在不连接有线的情况下，连接 OTP 无线，无法连接

问题分析：

==========

通过案例描述，有两个重点：

1，首次连接 OTP 出现连接问题

2，OEM 出厂设备有此问题

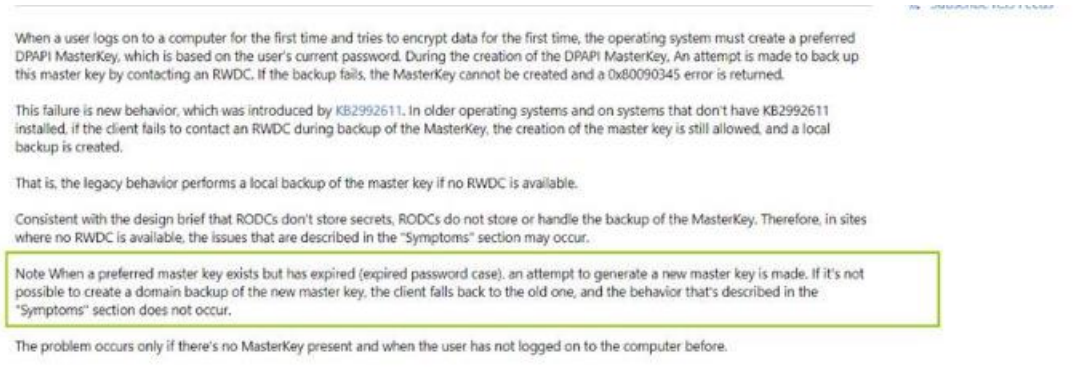
经分析与 master key 的创建有关，以下为 master key 的相关介绍：

Master key 用来加密机密数据，例如，记住的用户名和密码，证书私钥，还有一些应用 call 到 DPAPI 需要加密的数据。

master key 的创建仅当 DPAPI 接口调用到 CryptProtectData、CryptUnProtectData 两个函数时才会发生，因此在此问题上确认不会是因为初始镜像定制上的不同而造成。而是在入域进入系统之后的配置行为导致。以下列出一些可以创建 master key 的常见应用，供您参考：

- EFS 文件加密
- 存储无线连接密码
- Windows Credential Manager
- Internet Explorer
- Google Chrome

如果 master key 失效（master key 的有效期为 3 个月），系统会再次创建 master key。



When a user logs on to a computer for the first time and tries to encrypt data for the first time, the operating system must create a preferred DPAPI MasterKey, which is based on the user's current password. During the creation of the DPAPI MasterKey, An attempt is made to back up this master key by contacting an RWDC. If the backup fails, the MasterKey cannot be created and a 0x80090345 error is returned.

This failure is new behavior, which was introduced by KB2992611. In older operating systems and on systems that don't have KB2992611 installed, if the client fails to contact an RWDC during backup of the MasterKey, the creation of the master key is still allowed, and a local backup is created.

That is, the legacy behavior performs a local backup of the master key if no RWDC is available.

Consistent with the design brief that RODCs don't store secrets, RODCs do not store or handle the backup of the MasterKey. Therefore, in sites where no RWDC is available, the issues that are described in the "Symptoms" section may occur.

Note When a preferred master key exists but has expired (expired password case), an attempt to generate a new master key is made. If it's not possible to create a domain backup of the new master key, the client falls back to the old one, and the behavior that's described in the "Symptoms" section does not occur.

The problem occurs only if there's no MasterKey present and when the user has not logged on to the computer before.

解决方案：

==========

由于解决该问题最主要的操作是 master key 的创建，只要 master key 成功创建，即可正常访问 OTP 无线网络。诚如上述提到的可以创建 master key 的常见应用，建议使用 Windows Credential Manager。通过手动添加 windows 凭据的

方式创建 master key，进而连接无线。该解决方案在现场也已得到验证。以下是手动添加 windows 凭据的命令行操作，您可以编译成脚本进行操作：

CMD 命令行举例：cmdkey /generic:test1 /user:testuser /pass:testpwd

另外发现 OS 在工行的大基线定制内容中禁用了”同步主机_<xxxxx>”的服务，具体实现手段为设置注册表键值：

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OneSyncSvc，

start 设置值为 3（初始值为 2）.该服务的禁用，阻止 master key 的创建，经现场验证，将此服务开启后，可以正常创建 master key，并成功连接 OTP 无线

临时解决方案说明：

==========

关于 master key 在使用域用户环境下的创建条件：在微软 2014 年 11 月 11 日发布的 MS14-066 中有相关说明：必须保持正常与 RWDC 的通讯情况下，才能成功在本地创建 mastkey。如不需 RWDC，则需要启用 masterkey 的本地备份，即添加名为“ProtectionPolicy”且值为“1”的 DWORD 值添加到以下注册表子项：

HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Protect\Providers\df9d8cd0-1501-11d1-8c7a-00c04fc297eb

具体可参见以下链接：

https://support.microsoft.com/zh-cn/help/2992611/ms14-066-vulnerability-in-schannel-could-allow-remote-code-execution-n

https://support.microsoft.com/en-sg/help/3205778/dpapi-masterkey-backup-failures-when-rwdc-isn-t-available

关于该操作的 risk：

- 如果不设置 ProtectionPolicy 注册表键值，那么创建 master key 会在本地和 RWDC 上同时创建，如果由于某些原因找不到 RWDC 会导致 Master key 创建失败，进而导致加密数据失败。
- 如果设置 ProtectionPolicy 注册表键值，那么创建 master key 也同样会在本地和 RWDC 同时创建，在这种设置下如果 RWDC 连接失败，不会影响 master key 的创建，但是 master key 只会在本地创建，之后也不会同步到 DC 上。

由于某些原因如果新的密码无法解密 master key，那么系统会从密码历史记录中获取老的密码解密 master key。密码历史记录使用当前密码加密。这种场景不适用于密码重置，如果密码重置历史记录也无法获取。

The other question you might have is how does DPAPI access MasterKeys after a user changes his or her password? The answer is again a two-step process. First, DPAPI hooks into the password-changing module and when a user's password is changed, all MasterKeys are re-encrypted under the new password. Second, the system keeps a "Credential History" file in the user's profile directory. When a user changes his or her password, the old password is added to the top of this file and then the file is encrypted by the new password. If necessary, DPAPI will use the current password to decrypt the "Credential History" file and try the old password to decrypt the MasterKey. If this fails, the old password is used to again decrypt the "Credential History" file and the next previous password is then tried. This continues until the MasterKey is successfully decrypted.

如果 master key 无法解密，可能出现的影响如下。

- 凭据管理的历史凭据无法使用。
- 用户证书的私钥无法使用，如果有 EFS 加密那么可能导致 EFS 加密的数据无法解密。
- 三方程序调用 DPAPI 加密的数据无法获取。

综上所述，可能存在的 risk 为：用户密码被重置并且 DC 上没备份，可能会导致 master key 无法读取。只能手动重新创建，或者密码重置为之前的旧密码也可以恢复 master key 的访问。

具体可参见以下链接：https://docs.microsoft.com/en-us/previous-versions/ms995355(v=msdn.10)

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

神州网信 CMIT

发件人: Li Qi
发送时间: 2024 年 3 月 25 日 14:30
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

许先生，您好:

如刚才电话沟通，目前用户已联系内部网络组处理，暂不需要我们提供后续支持，因此经您的同意，此 case 做归档处理，以下为案例总结：

Case No：CAS-11061-X2B4F7

问题描述：

==========

用户反馈 V2020-L 和 V2022-L 版本系统连接 WIFI 后异常断开问题。

问题分析：

==========

用户将此问题转交内部网络组处理。

案例总结：

==========

经用户确认，暂不需要系统厂商的后续支持工作。经用户同意，该 case 将做归档处理，如有其他问题，可随时联系我们，谢谢。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: Li Qi
发送时间: 2024 年 3 月 19 日 17:57
收件人: ICBC 案例通知 <win10sup@sdc.icbc.com.cn>
抄送: ICBC_Notification <ICBC_Notification@cmgos.com>
主题: 回复: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

许先生，您好：

根据您反馈的问题，我谨以此封邮件阐述我们双方针对这个问题所涉及范围界定：

问题定义:

用户反馈 V2020-L 和 V2022-L 版本系统连接 WIFI 后异常断开问题，目前涉及 10 多台设备，需要协助分析处理。

问题范围:

我们将协助您分析处理上述问题，并对定义的问题给予最大的技术支持。

如果能及时解决问题，或问题属于产品设计的行为，或问题涉及到三方，我们将考虑关闭案例。如果存在多个问题，则我们考虑拆分案例进行分析。

接下来，我们将开始合作解决这个问题。如果您对以上的问题范围界定有任何异议，请尽快告知。如果您有其他任何疑问。也欢迎随时与我联系。

下一步动作：

请提供最终用户的联系方式以了解问题无线的配置及背景信息。

李琦 Li Qi
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务支持电话： 4008180055
电子邮箱 Email: liqi@cmgos.com

发件人: CRM 管理员 <crmadmin@cmgos.com>
发送时间: 2024 年 3 月 19 日 17:14
收件人: Li Qi <liqi@cmgos.com>
主题: [案例号:CAS-11061-X2B4F7] %|P1|ICBC|工行 CMGE 连接 WiFi 后异常断开问题% 案例重新分配 CMIT:0001125

Hi 李琦

一个案例已被重新分配给您，请及时处理。

案例号码： CAS-11061-X2B4F7
案例等级： P1
案例描述： 接到工行接口人许翔来电，反馈 V2020-L 和 V2022-L 版本系统连接 WIFI 后异常断开问题，接口人称涉及 10 多台设备，需要协助分析处理。
申请开启 P1 案例。

用户信息如下
单位：中国工商银行股份有限公司
联系人：许翔
电话：17606669571

邮箱：win10sup@sdc.icbc.com.cn
ACCESSID：25240869
创建人： 吴闫杰
创建时间： 2024/3/19 17:12

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。
This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。
This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.

-

此邮件信息仅供收件人查阅，所含任何评论、陈述或数据仅供收件人参考，若有改动，恕可能不另行通知。未经中国工商银行书面许可，请勿披露、复制、转载此邮件信息。任何第三方均不得查阅或使用此邮件信息。若您误收到本邮件，敬请及时通知发件人，并将邮件从您系统中彻底删除。发件人及中国工商银行均不对因邮件可能引发的损失负责。

This message is intended only for use of the addressees and any comment, statement or data contained herein is for the reference of the receivers only. Notification may not be sent for any revising related. Please do not disclose, copy, or distribute this e-mail without ICBC written permission. Any third party shall not read or use the content of this e-mail. If you receive this e-mail in error, please notify the sender immediately and delete this e-mail from your computer system completely.The sender and ICBC are not responsible for the loss caused possibly by e-mail.