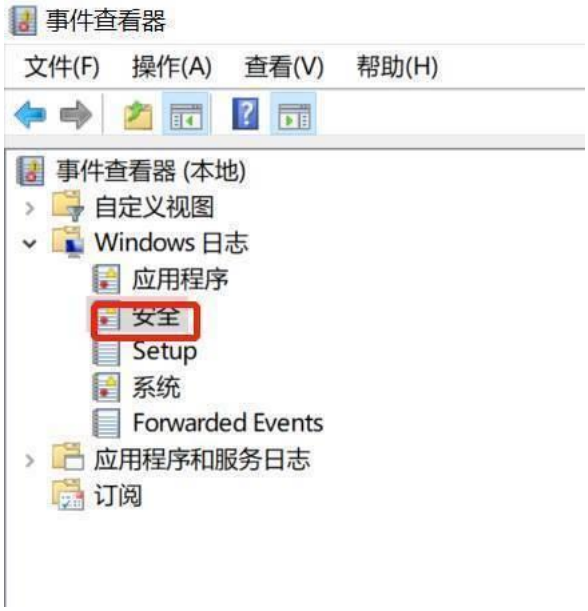
任先生 您好：

根据昨天的沟通，我将暂时归档此案例。
工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

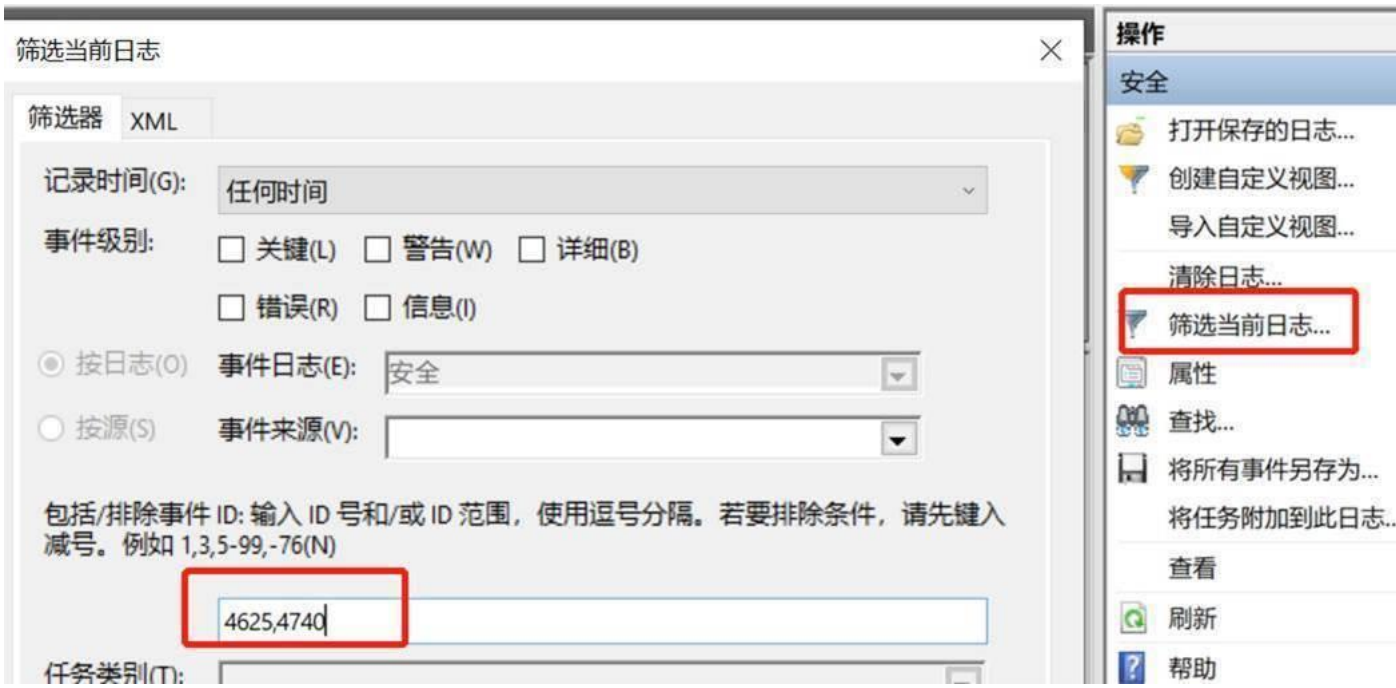
案例总结：

问题定义：
CMGE 系统在使用过程中出现帐户锁定情况。

排查方法：
在计算机出现锁定，等待 30 分钟自动解锁后，及时查看、备份系统安全日志。
1、右键左下角 Windows 图标，选择打开操作系统的事件查看器，定位到“事件查看器—Windows 日志—安全”，选中“安全”，查看系统审核日志。



2、选择“筛选当前日志”，在弹出的窗口中“所有事件 ID”那输入 4625,4740 筛选这两个事件 ID，选中某个事件，查看详细的事件信息，看能否查看到尝试使用错误的用户名或密码登录的 IP 或者某个应用程序来源。如下图类似示例。


筛选当前日志
筛选器
XML
记录时间(G):
任何时间
事件级别:
关键(L)
警告(W)
详细(B)
错误(R)
信息(I)
按日志(O)
事件日志(E):
安全
按源(S)
事件来源(V):
包括/排除事件 ID: 输入 ID 号和/或 ID 范围，使用逗号分隔。若要排除条件，请先键入减号。例如 1,3,5-99,-76(N)
4625,4740
任务类别(T):
操作
安全
打开保存的日志...
创建自定义视图...
导入自定义视图...
清除日志...
筛选当前日志...
属性
查找...
将所有事件另存为...
将任务附加到此日志...
查看
刷新
帮助

事件属性 - 事件 4625，Microsoft Windows security auditing.

常规 详细信息

失败信息:

失败原因: 未知用户名或密码错误。

状态: 0xC000006D

子状态: 0xC0000064

进程信息:

调用方进程 ID: 0x0

调用方进程名: -

网络信息:

工作站名: -

源网络地址: 146.48.10.120

源端口: 58632

详细身份验证信息:

登录进程: NtLmSsp

身份验证数据包: NTLM

传递服务: -

数据包名(仅限 NTLM): -

密钥长度: 0

登录请求失败时在尝试访问的计算机上生成此事件。

“使用者”字段指明本地系统上请求登录的帐户。这通常是一个服务(例如 Server 服务)或本地进程(例如 Winlogon.exe 或 Services.exe)。

“登录类型”字段指明发生的登录的种类。最常见的类型是 2 (交互式)和 3 (网络)。

“进程信息”字段表明系统上的哪个帐户和进程请求了登录。

“网络信息”字段指明远程登录请求来自哪里。“工作站名”并非总是可用，而且在某些情况下可能会留为空白。

日志名称(M):	安全		
来源(S):	Microsoft Windows secur	记录时间(D):	2020/8/25 17:27:48
事件 ID(E):	4625	任务类别(Y):	Logon
级别(L):	信息	关键字(K):	审核失败
用户(U):	暂缺	计算机(R):	DESKTOP-3TUGG8B

问题总结：
查看当前系统安全日志，没有显示调用账户锁定的计算机信息，锁定之前的日志信息没有查找到账户登录失败的日志。
重新配置安全日志自动存档，不覆盖旧的安全日志信息，后续观察是否再次出现账户锁定，再去分析新的日志。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2020 年 10 月 22 日 17:10
收件人: '任先生' <115891892@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [案例号: CAS-03109-T1M4W7] % 联想 OEM 用户-四川省通信管理局用户反馈账户锁定问题 % CMIT:0001510

任先生 您好:

循例询问，最近几天有没有再次出现账户锁定情况?
如果有问题出现，您可以通过邮件或者 400 热线联系我们。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2020 年 10 月 19 日 17:03
收件人: '任先生' <115891892@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [案例号: CAS-03109-T1M4W7] % 联想 OEM 用户-四川省通信管理局用户反馈账户锁定问题 % CMIT:0001510

任先生 您好：

您可以通过 CDUC 文件上传系统，把备份的系统日志信息发送给我们。

文件上传方法：
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。**如果出现类似错误提示，点击后退即可**
用户名：txglj
密码：txglj003

{"status":"error","message":"
×<\/a>\u63d0\u4f9b\u7684\u51ed\u636e\u4e0d\u6b63\u786e\u3002<\/div>"}

注意：添加文件，点击上传后，跳转到新的页面点击保存。

危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话: 400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2020 年 10 月 16 日 16:43
收件人: '任先生' <115891892@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [案例号: CAS-03109-T1M4W7]% 联想 OEM 用户-四川省通信管理局用户反馈账户锁定问题 %CMIT:0001510

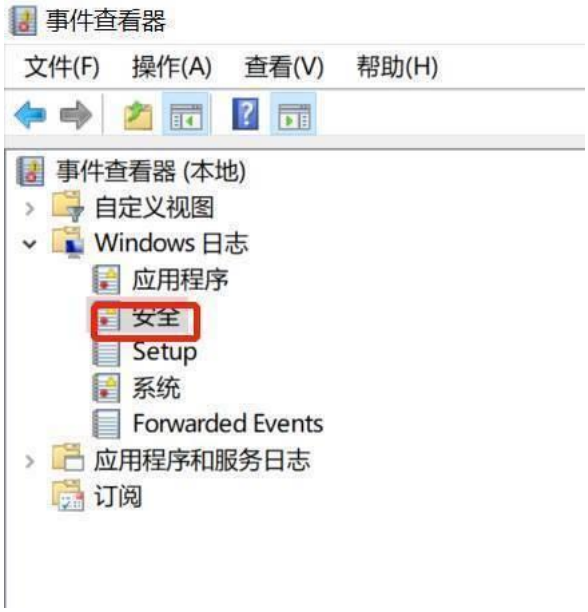
任先生 您好：

根据刚才的沟通，我将暂时归档此案例。
工单的归档并不会影响我们为您提供技术支持服务，如您有其他问题，您可以致电技术支持热线 4008180055。

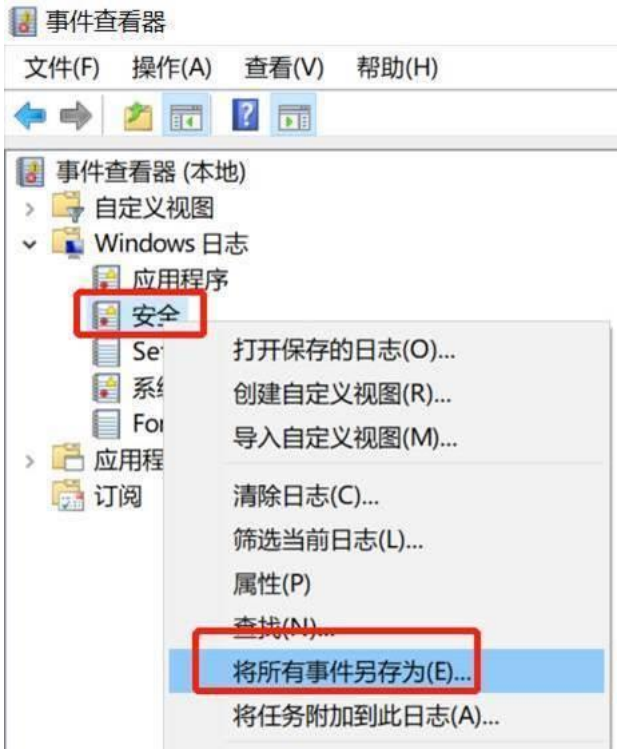
案例总结：

问题定义：
CMGE 系统在使用过程中出现帐户锁定情况。

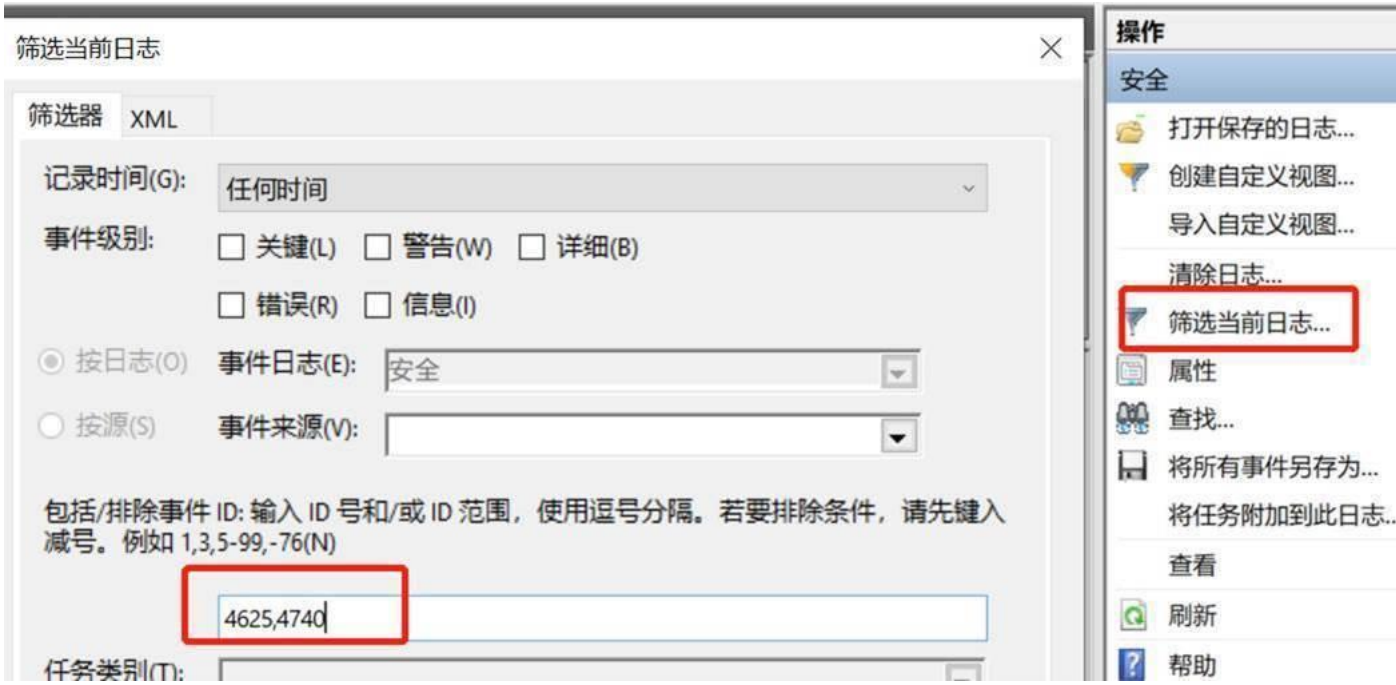
排查方法：
在计算机出现锁定，等待 30 分钟自动解锁后，及时查看、备份系统安全日志。
1、右键左下角 Windows 图标，选择打开操作系统的事件查看器，定位到“事件查看器—Windows 日志—安全”，选中“安全”，查看系统审核日志。



2、右键选择“安全”日志，选择“将所有事件另存为”…，保存当前事件日志，防止日志被覆盖。



3、选择“筛选当前日志”，在弹出的窗口中“所有事件 ID”那输入 4625,4740 筛选这两个事件 ID，选中某个事件，查看详细的事件信息，看能否查看到尝试使用错误的用户名或密码登录的 IP 或者某个应用程序来源。如下图类似示例。



事件属性 - 事件 4625，Microsoft Windows security auditing.

常规 详细信息

失败信息:

失败原因: 未知用户名或密码错误。

状态: 0xC000006D

子状态: 0xC0000064

进程信息:

调用方进程 ID: 0x0

调用方进程名: -

网络信息:

工作站名: -

源网络地址: 146.48.10.120

源端口: 58632

详细身份验证信息:

登录进程: NtLmSsp

身份验证数据包: NTLM

传递服务: -

数据包名(仅限 NTLM): -

密钥长度: 0

登录请求失败时在尝试访问的计算机上生成此事件。

“使用者”字段指明本地系统上请求登录的帐户。这通常是一个服务(例如 Server 服务)或本地进程(例如 Winlogon.exe 或 Services.exe)。

“登录类型”字段指明发生的登录的种类。最常见的类型是 2 (交互式)和 3 (网络)。

“进程信息”字段表明系统上的哪个帐户和进程请求了登录。

“网络信息”字段指明远程登录请求来自哪里。“工作站名”并非总是可用，而且在某些情况下可能会留为空白。

日志名称(M):	安全		
来源(S):	Microsoft Windows secur	记录时间(D):	2020/8/25 17:27:48
事件 ID(E):	4625	任务类别(Y):	Logon
级别(L):	信息	关键字(K):	审核失败
用户(U):	暂缺	计算机(R):	DESKTOP-3TUGG8B

问题总结：
用户当前系统安全日志已经被覆盖，无法查看到账户锁定原因，告知用户具体查看、操作方法，当再次出现账户锁定时及时保存系统安全日志，分析日志定位锁定原因。

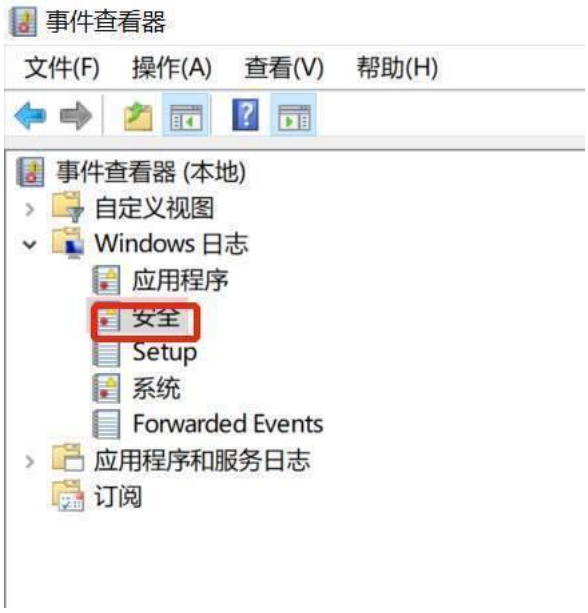
危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang
发送时间: 2020 年 10 月 16 日 15:42
收件人: 任先生 <115891892@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复: [案例号: CAS-03109-T1M4W7] % 联想 OEM 用户-四川省通信管理局用户反馈账户锁定问题 % CMIT:0001510

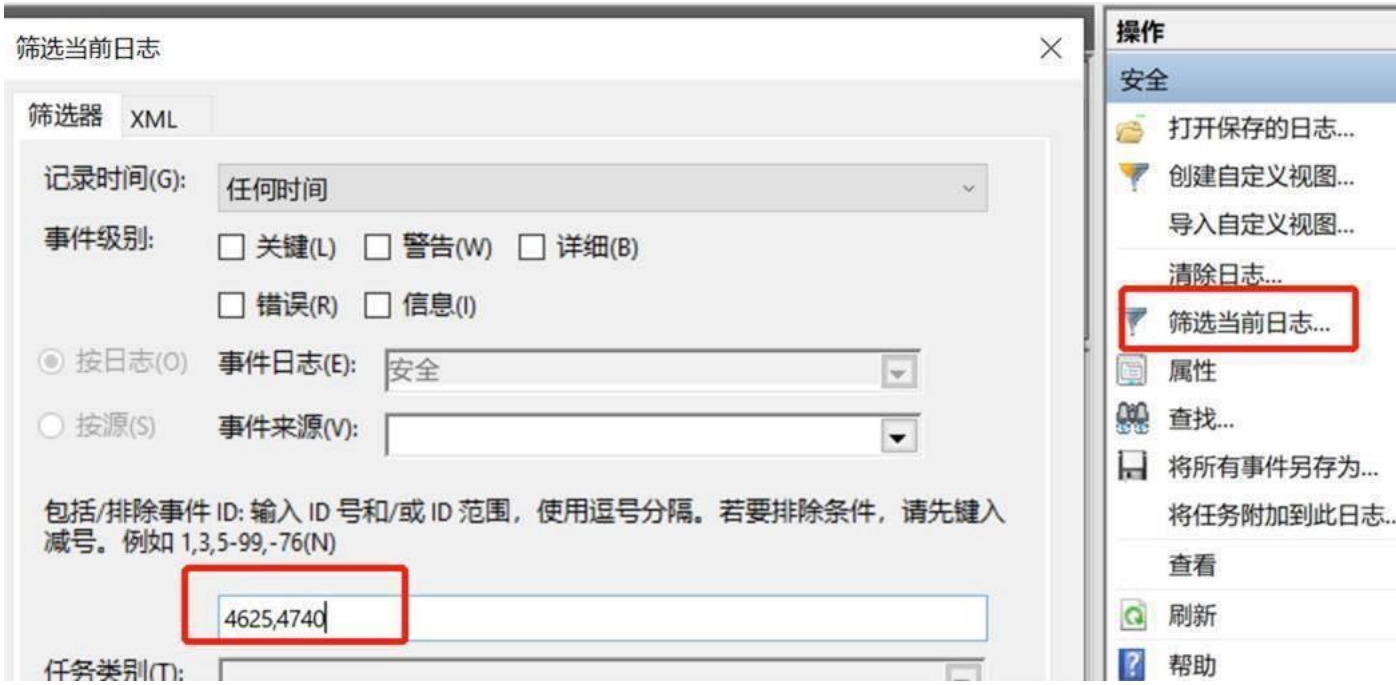
任先生 您好：

根据刚才的电话沟通，我谨在此阐述您所述问题涉及的范围定义：
问题定义：CMGE 系统在使用过程中出现帐户锁定情况。
问题范围：协助用户分析、处理此问题。
如您对以上问题范围定义有任何疑问请直接与我联系。

排查方法：
1、右键左下角 Windows 图标，选择打开操作系统的事件查看器，定位到“事件查看器—Windows 日志—安全”，选中“安全”，查看系统审核日志。



2、选择“筛选当前日志”，在弹出的窗口中“所有事件 ID”那输入 4625,4740 ，筛选这两个事件 ID，选中某个事件，查看详细的事件信息，看能否查看到尝试使用错误的用户名或密码登录的 IP 来源。



危亮 Wei Liang
神州网信技术有限公司
C&M Information Technologies Co.,Ltd.
服务电话：400-818-0055
电子邮箱 Email: weiliang@cmgos.com

发件人: Wei Liang <weiliang@cmgos.com>
发送时间: 2020 年 10 月 16 日 15:27
收件人: 任先生 <115891892@qq.com>
抄送: Wei Liang <weiliang@cmgos.com>
主题: [案例号: CAS-03109-T1M4W7]% 联想 OEM 用户-四川省通信管理局用户反馈账户锁定问题 %初次响应 CMIT:0001510

任先生 先生/女士，您好!

感谢您联系神州网信技术支持中心。 我是技术支持工程师 危亮 。 很高兴能有机会协助您解决该问题。 您可随时通过邮件回复以及该问题事件号码 CAS-03109-T1M4W7 与我联系。

如果您有任何其他疑问，请随时与我联系。

此致,

敬礼
