赵女士，您好！

很高兴收到您的邮件反馈，根据反馈的结果，我将暂时归档此问题。**案例归档后您会收到调查问卷的邮件，希望可以对我们的服务进行评价。**
工单的归档并不会影响我们为您提供技术支持服务，如果您的问题复现，或有新的问题出现，您也可以致电我们的技术支持热线 4008180055。

案例总结：
案例描述：
已安装 30 多台电脑，有 3 台电脑突然出现账号锁定问题

案例分析：
造成计算机锁定的原因是输入用户名密码错误连续 5 次，通过数据分析，发现如下问题：
1）访问机器 IP 地址：146.48.10.120
2）访问方式：NtLmSsp
3）访问失败原因：位置用户名或密码错误

建议操作：
1）在 146.48.10.120 机器上查杀病毒木马；
2）在 146.48.10.120 机器上查看是否有访问被锁定计算机的共享文件或访问共享的三方应用程序，并删除登陆凭据

3）删除本地凭据管理器的过期凭据。键入 Windows 键+R 键，输入 control，打开控制面板，将右上角查看类型选为“类别”，点击“用户账户”-“凭据管理器”-“Windows 凭据”，将被访问造成锁定主机的 IP 或名称的凭据删除，如不确定服务器凭据，删除所有不能确定来源的凭据；

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Nannan <1321587440@qq.com>
发送时间: 2020 年 9 月 1 日 10:10
收件人: Jia Wei <jiawei@cmgos.com>
主题: 回复： 回复： [案例号: CAS-02853-V4B7F1] % 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

你好，邮件已收到。故障已经排除，谢谢！

发自我的 iPhone

---------- 原始邮件 ----------
发件人: Jia Wei <jiawei@cmgos.com>
发送时间: 2020 年 8 月 28 日 09:41
收件人: Nannan <1321587440@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复： 回复： [案例号: CAS-02853-V4B7F1] % 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

赵女士，您好！

电话未能联系到您，您可以按照上封邮件的内容进行问题排查，如果有结果或有问题，可以回复此邮件。我将持续跟踪此案例。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人： Jia Wei
发送时间： 2020 年 8 月 26 日 10:18
收件人： 'Nannan' <1321587440@qq.com>
抄送： CRM Case Email <casemail@cmgos.com>
主题： 回复: 回复： [案例号: CAS-02853-V4B7F1] % 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

赵女士，您好!

收到您反馈的数据。
案例分析：
造成计算机锁定的原因是输入用户名密码错误连续 5 次，通过数据分析，发现如下问题：
1）访问机器 IP 地址：146.48.10.120
2）访问方式：NtLmSsp
3）访问失败原因：位置用户名或密码错误

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。

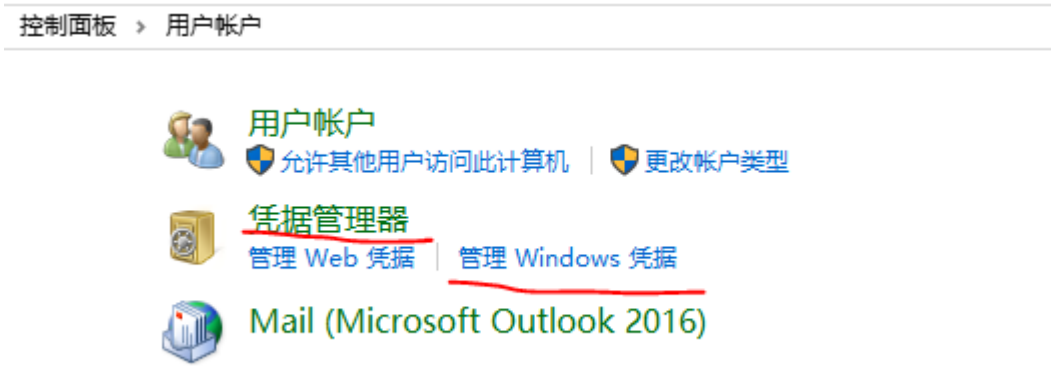
日志名称(M):	安全		
来源(S):	Microsoft Windows secur	记录时间(D):	2020/8/25 17:27:48
事件 ID(E):	4625	任务类别(Y):	Logon
级别(L):	信息	关键字(K):	审核失败
用户(U):	暂缺	计算机(R):	DESKTOP-3TUGG8B

建议操作：

1）在 146.48.10.120 机器上查杀病毒木马；

2）在 146.48.10.120 机器上查看是否有访问被锁定计算机的共享文件或访问共享的三方应用程序，并删除登陆凭据

3）删除本地凭据管理器的过期凭据。键入 Windows 键+R 键，输入 control，打开控制面板，将右上角查看类型选为“类别”，点击“用户账户”-“凭据管理器”-“Windows 凭据”，将被访问造成锁定主机的 IP 或名称的凭据删除，如不确定服务器凭据，删除所有不能确定来源的凭据；



贾伟 Jia Wei
神州网信技术有限公司
服务电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人：Nannan <1321587440@qq.com>
发送时间：2020 年 8 月 26 日 9:38
收件人：Jia Wei <jiawei@cmgos.com>
主题：回复：［案例号：CAS-02853-V4B7F1 ］% 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

你好，文件已上传至平台。这台电脑是 25 号下午五点左右发现账号被锁定的，电脑是没有设置密码的。

另，前两个电话因为刚好手头有事没接到，回拨时是机器答复，实在不好意思！

发自我的 iPhone

------------------ 原始邮件 ------------------
发件人：Jia Wei <jiawei@cmgos.com>
发送时间：2020 年 8 月 26 日 09:26
收件人：赵女士 <1321587440@qq.com>
抄送：CRM Case Email <casemail@cmgos.com>
主题：回复：［案例号：CAS-02853-V4B7F1 ］% 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

赵女士，您好！

电话未能联系到您，如果您对于数据收集有问题可以回复此邮件，我可以与您取得电话沟通。

贾伟 Jia Wei

神州网信技术有限公司

服务电话： 400-818-0055

电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.

11F, Block C North Building, Raycom InfoTech Park, Beijing

mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人: Jia Wei
发送时间: 2020 年 8 月 25 日 16:38
收件人: 赵女士 <1321587440@qq.com>
抄送: CRM Case Email <casemail@cmgos.com>
主题: 回复:[案例号: CAS-02853-V4B7F1] % 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

赵女士，您好!

问题定义：已安装 30 多台电脑，今天有 3 台电脑突然账号就被锁定了

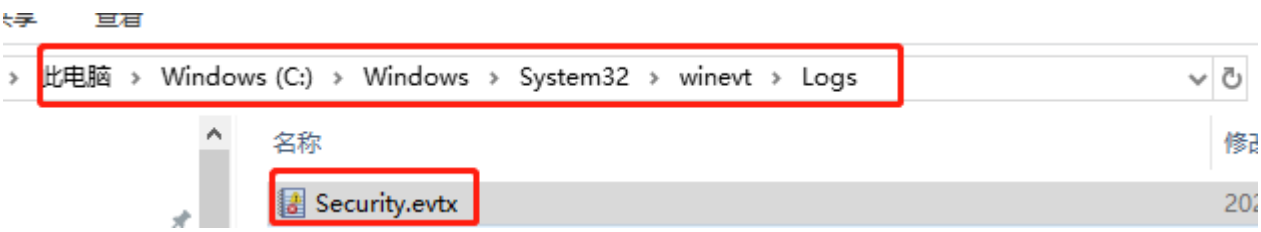
问题范围：协助您分析并处理上述问题。

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。

为了进一步定位问题原因，还需您进行如下数据反馈。

数据收集：

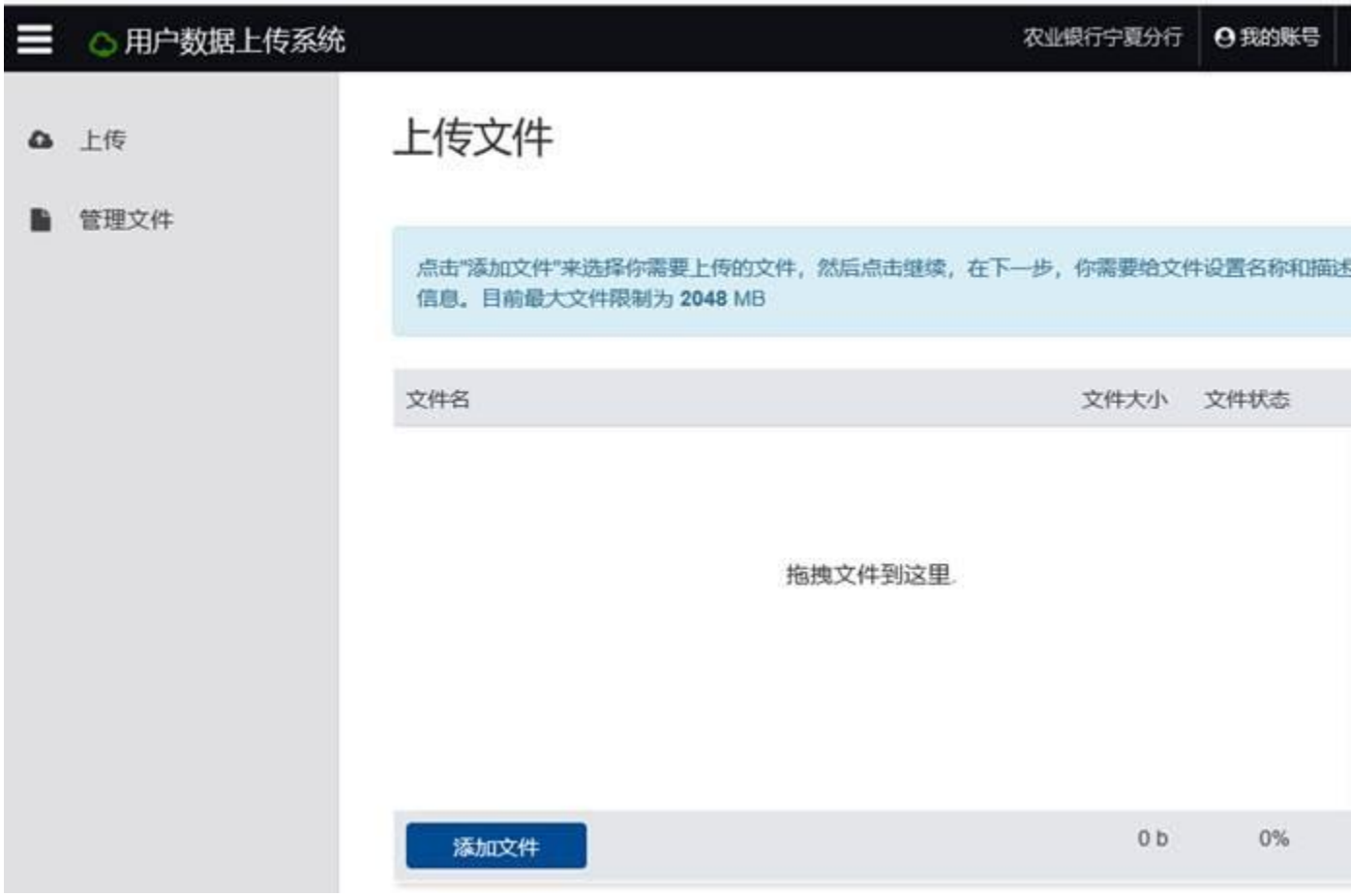
1. 等到问题复现后，进入系统，将 C:\Windows\System32\winevt\Logs 地址下的 Security.evtx，**压缩后**通过数据上传网站上传。



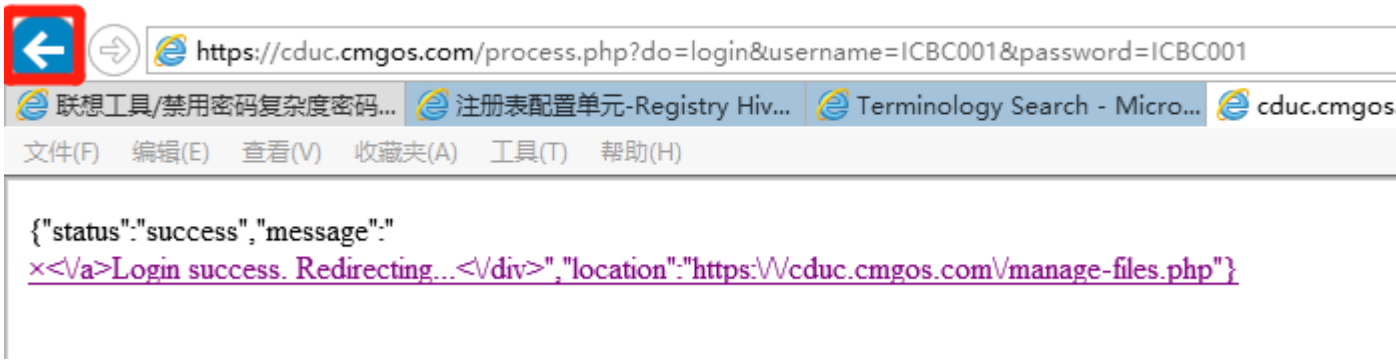
数据上传：

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：GDYJGGW
密码：GDYJGGW

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



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。

贾伟 Jia Wei
神州网信技术有限公司
服务电话： 400-818-0055
电子邮箱： jiawei@cmgos.com

C&M Information Technologies Co., Ltd.
11F, Block C North Building, Raycom InfoTech Park, Beijing
mail: Jiawei@cmgos.com | visit: www.cmgos.com

发件人： Jia Wei <jiawei@cmgos.com>
发送时间： 2020 年 8 月 25 日 16:15
收件人： 赵女士 <1321587440@qq.com>
抄送： Jia Wei <jiawei@cmgos.com>
主题：[案例号: CAS-02853-V4B7F1] % 汕头市龙湖区人民法院账户被锁定希望排查被锁定原因 % 初次响应 CMIT:0001826

赵女士 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 贾伟 。 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-02853-V4B7F1 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

以上内容是一封有关向神州网信技术有限公司提交技术支持事件的邮件。

如果您希望本次回复能够被自动加入技术支持事件中，您可以选择“全部回复”。