

ARM 系列

常见问题的解决方案

目录	
1. RDP 系列	5
1.1 RDP 主机部署	5
1) 部署的一般步骤	5
部署方法 1:手动部署	5
部署方法 2:快速部署	5
2) 用户被提示登录到主机,需要等待用户退出?	6
3) 终端无法连接到主机,表明主机不存在?	6
 主机只能连接两个终端? 	7
5) 哪些版本的 Windows 可以用作远程桌面主机?	7
6) 安装 RDPWrap 后,发现服务没有安装?	7
 更新 Windows10 后终端无法连接主机? 	7
8) 无法支持最新的 Windows10 系统?	7
1.1.1 部署问题: 部署软件或是多用户补丁软件无法打开?	8
1.2 显示的问题	
1)HDMI显示,显示屏幕不能完全覆盖显示区域?	11
2) 连接 VGA 显示器,显示器屏幕不能完全覆盖显示器的显示区域吗?	
3)连接到远程主机后无法更改分辨率?	
4)分辨率修改后,不生效?	13
1.3 声音的问题	13
1) 耳机里没有声音?	13
2)不能录音?	13
3)录音后,回放此录音文件发现语速过快?	14
4) HDMI 显示无法输出声音?	14
1.4 网络问题	14
1)两台或更多的机器经常掉线?有时 A 端断开,有时 B 端断开	14
2)终端网络设置为自动获取 IP,但经过一段时间后,是否存在 IP 冲突?	14
3)无线信号太弱	14
4)无线网络不稳定?	14
1.5 终端系统升级问题	15
1)针对不同终端升级固件的方法是什么?	15
2)什么时候需要升级终端固件?	15
1.6 外设支持问题	15
1) 无法使用 u 盘?	
2)不能使用打印机?	19
3)不能使用相机?	21
4) 不能使用扫描枪?	21
1.7 管理工具的问题	21
1) 管理工具无法唤醒终端?	21
2)管理工具不能监控终端?	22
1.8 崩溃和掉线问题	23
1) 崩溃的问题	23
2) 掉线的问题	23
3)不能退出一个问题,黑屏,有鼠标箭头可以移动吗?	24
4)终端卡死:鼠标可以动,但是桌面无法点击?	24

1.9 多用户使用问题	24
1)有些软件不能多个用户同时打开?	24
2)如何将软件快捷方式发送到所有用户的桌面?	25
3)连接 win10 主机,终端可以直接关闭主机?	25
1.10 像谷歌浏览器这样的软件不能运行	25
1.11 终端屏幕缓慢刷新,像幻灯片一样	26
1.12 如何禁止使用 U 盘,禁止修改终端设置	
1.13 忘记终端密码	42
1.14 恢复出厂设置	42
1.15 终端可以关闭主机?	45
1.16 其他问题	46
1.16.1 NSIS 错误:启动安装程序错误?	
1.16.2 安装 VDPlayer 报错?	47
1.16.3 终端连接到主机后,无法播放视频?	
1.16.4 登陆界面不显示账户列表?	48
1.16.5 远程桌面服务启动报错误 2 或错误 126?	
1.17 域用户名问题	50
1.18 Remote Desktop Services 停止或 Remote Desktop Services 丢失	50
2. 四个协议系列	53
2.1 不同的协议	53
2.2 Vmware 连接问题	53
1) 连接提示 SSL 问题?	53
2)登录后,无法修改分辨率?	53
3)不能记录?	53
4)使用 u 盘?	53
2.3 Citrix 连接问题	53
1) 输入的服务器 IP 地址无法连接到服务器?	53
2)连接后,Windows 系统界面上没有 Citrix 工具栏?	54
3)登录后,无法修改分辨率?	54
4)无法记录,登录到虚拟机接口后,记录设备不存在?	54
5) ARM 终端是否可以直接输入服务器登录地址(不是网页登录方式)?	54
6)使用 U 盘	54
2.4 Spice 连接问题	54
2.5 终端系统设置问题	54
1)连接到主机后无法更改分辨率?	54
2) 在扩展模式下,双屏幕连接如何显示不同的协议?	55
2.6 其他连接问题	55
1) 有支持华为虚拟化平台的终端吗?	55
2) 是否有办法支持其他客户?	55
3. 定制系统系列	55
3.1 所有的机型都支持 android 和 ubuntu	55
3.2 Ubuntu 系列	55
1) 哪些型号支持 ubuntu?	55
2) 提供 ubuntu 固件的目的?	55
3)ubuntu 如何支持它?	56

3.3 Android 系列	56
1) 哪些型号支持 android?	56
2) 提供 android 固件的目的?	56
3) 如何支持 android ?	56
4) android 支持 USB 摄像头吗?	56
4. 各机型特性	56
4.1 每种终端支持的软件列表	56
4.2 每种类型的硬件和软件信息	
说明:	

1. RDP 系列

RDP 系列是指终端只有 RDP 协议,没有其他协议。RDP 连接可能不会显示在终端上。此外,该 RDP 版本不允许 客户修改终端系统的内部代码或添加软件。



Log in to an account of the host

终端是通过 RDP 协议登录一个主机账号,使用该主机;多台终端意味着多人同时使用一台主机;

1.1 RDP 主机部署

- RDP 主机部署的常见问题以及如何处理它们
- 1) 部署的一般步骤 以下都是在主机上操作的 r

部署方法 1:手动部署

项目	需要	效果
1. 创建账户	是的	创建终端登录用户, 主机不支持无帐号登录
2. 启用远程桌面功能	是的	远程桌面连接的核心功能
3. 将用户添加到远程桌面用户组	是的	只有添加到远程桌面用户组的帐户才能远程登录
3. 关闭防火墙	是的	防火墙会阻塞到远程桌面的连接
4. 设置静态 IP		设置静态 IP 可以防止主机 IP 更改
5. 安装多用户连接服务	是的	默认情况下, Windows 主机在同一时间只能登录一个用户,
		其他用户将被锁定;通过安装多用户连接服务,多个用户可
4		以同时连接到登录主机。
6. 安装 RDP 加速包	是的	在您的主机上启用 RemoteFX 以改善远程桌面体验(客户端
		上的 RDP 版本高于 8.0)
7. 网络级别身份验证		有时需要关闭 NLA 并调整协议层,以便在主机上的组策略
		(gpei.msc)中进行协商;

部署方法 2:快速部署

使用 "RDP 桌面部署"软件进行快速部署,部署软件将自动执行上述步骤;

项目	需要	效果
1. 点击"部署"	是的	一系列操作的一个关键;
2. 创造用户	是的	在部署软件上为终端登录创建帐户;
3. 重新启动计算机	是的	某些设置需要修改才能生效;

附录:NLA

有时 有时需要关闭 NLA 并调整协议层,以便在主机上的组策略(gpedit.msc)中进行协商;

KDP桌面部者v1.6.20						– 🗆 X
	一键	部署(音	署完成后	5,重启电脑才能使配置	置生效)	
快速部署	⊙其ī	它型号	北太	5		本机IP:
批量创建账户	O FL3	300	1/\/C	<u>,, 123</u>	<u>4 ⊇</u> 部署≥	192.168.56.1
其它工具	☑ 更新	新补丁		5.RDP加速包未安装!		
教程						
English	近柱 账户列	登陆信息 咦:(点	灵 上可洗取)			
	序号	账户名	密码	登陆IP	账户名:	6
	1	1	未获取	192.168.56.1	密码:	6
	2	2	未获取	192.168.56.1	类型:	
	5	5	~3742	192.100.30.1	 ● 标准账户 	0 管理员账户
					☑ 账户永不过期	
注意: 界面上加下划线的					☑ 用户不能修改密码	
文字都是可点击的		除>	修改密码>			创建>
	账户:(6; 密码是:	6			^
						¥
? RDP桌面部署v1.6.20						– 🗆 X
	一键	部署(音	『署完成后	;,重启电脑才能使配 计	置生效)	– 🗆 X
	一键 ◎ 其ī	部署 (部 ^{] 211} 号	『署完成后 状态	i, 重启电脑才能使配置	置生效)	- □ × <u>本机IP:</u>
♀ RDP桌面部署v1.6.20 快速部署 批量创建账户	—键 ◎ 其ī	部署(部 ^{3型号}	『署完成后 <u>状态</u>	i,重启电脑才能使配置 <u>: 1 2 3</u>	置生效) <u>4</u> 5 _{部署≥}	- □ × 本机IP:_ 192.168.56.1
₽ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具	—键 ⊙其ī O FL3 ☑ 更新	部署(音 ^{22型号} 300 新补丁	W署完成后 <u>状态</u>	5.RDP加速包未安装!	置生效) <u>4 5</u> <u>部署≥</u>	-
✔ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程	—键 ⊙ 其ī O FL3 ☑ 更新	部署(音 ^{这型号} 300 新补丁	W署完成后 状态	5.RDP加速包未安装!	置生效) <u>4 5</u> <u>部署</u> ≥	-
ℜ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	键 ◎ 其T ◎ FL3 ◎ 更 远程 账户列	部署(音 ^{3型号} 300 新下丁 登陆信息 J表: (点者	都署完成后 <u>状态</u> 同选取)	5.RDP加速包未安装!	置生效) <u> 4</u> 5 <u> 部署</u> ≥	- □ × <u>本机IP:</u> 192.168.56.1
✔ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	 一键 ○ 其前 ○ FL3 ○ 更新 □ 正 □ 正 □ 正 □ 示 □ 示 	部署(音 ^{这型号} 300 新补丁 登陆信息 康:(点司 账户名	形署完成后 状态 「「満取) 密码	5.RDP加速包未安装! 登陆IP	置生效) 4 5 部署≥ 账户名:	-
ℜ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	 一键 ○ 其1 ○ FL3 ○ 更新 ○ 正式 <l< td=""><td>部署(音 ^{2型号} 300 新补丁 受陆信息 限:(点目 账户名 1</td><td>「著完成后 大衣 「「「法取」 「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一</td><td> 重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 </td><td>査生效) <u> 4</u> 5 部署> 部署> 部署> 部署→</td><td> × <u>本机IP:</u> 192.168.56.1 6 6</td></l<>	部署(音 ^{2型号} 300 新补丁 受陆信息 限:(点目 账户名 1	「著完成后 大衣 「「「法取」 「一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一	 重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 	査生效) <u> 4</u> 5 部署> 部署> 部署> 部署→	× <u>本机IP:</u> 192.168.56.1 6 6
ℜ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	 ● 其前 ○ 月1 ○ 月1 ○ 月1 ○ 町 一座 一座 一座 一座 一座 三座 三 三	部署(音 ³⁰⁰ 新补丁 受陆信息 限:(点司 1 2 2		重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1	置生效) 4 5 部署≥ 部署≥ 部署≥ ()	× <u>本机IP:</u> 192.168.56.1 6 6
ℜ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	● 其T ○ 月1 ○ 月1 ○ 月1 ○ 更野 一 一 一 一 一 一 一 一 一 一 一 一 一	部署(音 ³⁰⁰ 新补丁 受陆信息 限:(点词 1 2 3	「 著完成后 状态 「 で の 一 、 、 、 、 、 、 、 、 、 、 、 、 、	 ・重启电脑才能使配置 ・ ・ ・	置生效) 4 5 部署≥ 部署≥ 部署≥ ○ 标准账户	- · · · · · · · · · · · · · · · · · · ·
ℜ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	 一键 ○ 其下 ○ FL3 ○ 更新 一次户列 序号 1 2 3 	部署(音 ³⁰⁰ 新补丁 登陆信息 限广名 1 2 3	「「 で 一 で 一 で の の の の の の の の の の の の の	重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1	置生效) 4 5 部署> 部署> 部署> ○ 标准账户 ○ 标准账户 ☑ 账户永不过期	- · · · · · · · · · · · · · · · · · · ·
♥ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English	● 其T ○ 月1 ○ 月1 ○ 月1 ○ 更野 一 一 一 一 一 一 一 更 「 一 一 一 一 一 一 一 一 一 一 一 一 一	部署(音 ³⁰⁰ 新补丁 受陆信息 限产名 1 2 3	「新書完成に 大之 「「一一」 「「一」 「「一」 「「一」 「「一」 「「一」 「」 「」	重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1	 	- · · · · · · · · · · · · · · · · · · ·
♥ RDP桌面部署v1.6.20 快速部署 批量创建账户 其它工具 教程 English 注意: 界面上加下划线的 文字都是可点击的	● 其T ○ 月1 ○ 月1 ○ 月1 三 更詳 一 一 一 一 一 一 更詳 「 一 一 一 一 一 一 一 一 一 一 一 一 一	部署(音 注型号 300 新补丁 登陆信息 限・ 名 1 2 3 ※ ドク名	水客完成信 火态 「 「 「 「 「 、 、 、 、 、 、 、 、 、 、 、 、 、	重启电脑才能使配置 1 2 3 5.RDP加速包未安装! 登陆IP 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1 192.168.56.1	 	- ○ × 本机IP: 192.168.56.1 6 6 ○ 管理员账户 创建≥

2) 用户被提示登录到主机,需要等待用户退出?

■ 主机上没有安装多用户连接服务。使用 RDPWrap 或多用户连接安装多用户连接服务.

3) 终端无法连接到主机,表明主机不存在?

■ 将主机本身与自己的远程桌面连接(此时需要填写的主机 IP 为:127.0.0.2);如果连接,调整组策略;

■ 检查主机上的防火墙是否关闭,或者是否允许远程桌面功能通过防火墙;

■ 如果无法连接,请检查远程桌面功能是否打开。如果远程桌面被打开,如果连接仍然不可用,那就是 Windows 系 统本身的问题。尝试更新 Windows 系统、重新安装多用户连接服务或重新安装 Windows 系统。

4) 主机只能连接两个终端?

■ 安装多用户连接服务:RDPWrap 或多用户连接;

- 5) 哪些版本的 Windows 可以用作远程桌面主机?
 - Windows 专业版, 旗舰版, 企业版可以支持作为远程桌面主机;
 - home 版 Windows, home 高级版不能用作远程桌面主机(没有远程桌面功能);

远程桌面	支持	不支持
Windows7	Pro (32bit/64bit SP1)	Start (32bit/64bit SP1)
Windows7	Ultimate (32bit/64bit SP1)	Home (32bit/64bit SP1)
Windows7	Enterprise (32bit/64bit SP1)	Home Premium (32bit/64bit SP1)
Windows8	Pro(32位/ 64位)	Home(32位/64位)
Windows10	Pro(32位/64位)	Home(32位/64位)
Windows10	Enterprise(32位/ 64位)	
Windows10	教育(32位/64位)	
Windows server 2008 R2	标准	
Windows server 2008 R2	数据中心	
Windows server 2012 R2	标准	
Windows server 2012 R2	数据中心	
Windows MultiPoint Server 2012	标准(10个用户)	
Windows MultiPoint Server 2012	保险费(20个用户)	
Windows server 2016	标准	
Windows server 2016	数据中心	
Windows server 2019	标准	
Windows server 2019	数据中心	
企业版是功能最全面的版本,它支持	持作为远程桌面主机。请安装 64 位版本	的系统.

6) 安装 RDPWrap 后,发现服务没有安装?

■ 失压过程中丢失的文件;再次下载和卸载;使用最新版本;

- 7) 更新 Windows10 后终端无法连接主机?
 - 更新 Windows 系统后,远程桌面上的相关系统文件可能会发生变化,导致现有的多用户连接失败;

临时对策	长时间的对抗
卸载最近的更新/运行最新的 RDPWrap	1. 使用 RDPWrap 确保多用户连接是有效的
	2. 使用第三方软件完全禁用 Windows 更新

8) 无法支持最新的 Windows10 系统?

■ 将 Windows 更新到最新的系统后,相关的 RDPWrap 文件无法及时更新,建议使用稍早的版本;当前支持的 Windows 版本是:

Windows10 1511	Windows10 1607
Windows10 1703	Windows10 1709

Windows10 1803	Windows10 1809
Windows10 1903(Only 15 accounts are supported)	Windows10 1909
1909 是最新的版本, RDPWrap 并没有得到完全的支持;	

1.1.1 部署问题: 部署软件或是多用户补丁软件无法打开?

RDP 部署软件或是多用户补丁软件无法运行,或是提示文件找不到?

此现象多是由于 360 杀毒、360 卫士阻止或是删除文件导致;建议按如下方法操作,(将文件保存到 360 杀毒和 360 安全卫士的白名单目录里):

(🕑 360杀毒 - 设置	×	- ×
	 常规设置 146.41 	设置文件及目录白名单 加入白名单的文件及目录在病毒扫描和实时防护时将被跳过。	
	 ① 新報告 ② 多引擎设置 	如果在加入白名単后文件的大小或日期发生改变,该条目将会失效。 文件 状态 状态 添加文件	
	 Q、病毒扫描设置 © 实时防护设置 	添加目录	
	ご 文件白名单	删除	
	□ 免打扰设置□ 异常提醒		
	🗶 系统白名单	带有日名单扩展名的文件在病毒扫描和实时防护时将被跳过。 扩展名 添加	
		删除	
已隔离		✓ 定期扫描白名单中具有极强传播性及感染性的文件。	3
多51筆 程序版:	恢复默认设置	确定 取消	"管家 诗免费?

进入设置界面,点击"文件白名单",

(7) 36	Â	U • X
	360杀毒 - 设置	×
	 ⑦ 常规设置 ① 升级设置 	- 设置文件及目录白名单 加入白名单的文件及目录在病毒扫描和实时防护时将被跳过。 如果在加入白名单后文件的大小或日期发生改变,该条目将会失效。
	 ③ 多引擎设置 Q、病毒扫描设置 	文件 状态 添加文件 □ C:\Users\share\Desktop\123\ 永久有效 添加目录
	◎ 实时防护设置	
	官文件白名单	
	🖸 免打扰设置	全选
	111 异常提醒	
	🗶 系统白名单	
		删除
口隔离。		✔ 定期扫描白名单中具有极强传播性及感染性的文件。
参51手1 程序版:	恢复默认设置	确定 取消 背家 持免费?
添加白	名单目录;	
€ 360 g	2全卫士12 ✦	
		📩 🔀 纪 🗄 🛞 👪 🎮
我的	的电脑 木马查杀	电脑清理 系统修复 优化加速 功能大全 金融•互助宝 软件管家 游戏管家
	1	
		全盤査杀 按位置査杀
	6	查杀木马病毒,拦截可疑行为 ^{您还未进行木马扫描,请立即扫描} 2
	U	快速查杀 ②

点击"木马查杀">"信任区"

➡ 系统急救箱
 ✓ 反勒索服务

😌 360安全卫士	±12 ↑			•	未登录 ① 日	≡ - ×	
	😪 安全操作中心					×	
我的电脑	[] 防护记录	名称	类型	时间	操作	₹.	
	业 下裁记录						
	⊘ 拦截记录					đ	
	① 上报记录					置查杀	Λ
	🗐 优化记录					2	\mathbf{N}
	○— 。权限记录					复区	
	○ 可恢复区					3	
	0 EALE					纪擎	
	ⓒ 已信任区						
	铝 补丁管理						
	🕒 漏洞防护	全洗	添加目录	添加文件	移除		
					13 Mar		

点击"添加目录",选择对应的目录,比如图示选择桌面上的"123"文件夹;

360安全卫;	±12 🕈				
	😪 安全操作中心				© – □ ×
我的电脑	[] 防护记录	名称	类型	时间	操作
	业 下载记录	123	目录	2020-05-29 11:47:27	移除
	⊘ 拦截记录	citizers (share (desktop) i zo			Ē
	⚠ 上报记录				直鱼余
	🗐 优化记录				ਕ
	<u>∽</u> 权限记录				复区
	○ 可恢复区				3
					纪寧
	⊘ 已信任区				
	品 补丁管理				
	二 漏洞防护	全选	添加目录	添加文件	移除

在接收或下载文件时,点击"另存为",将其保存到杀毒软件的白名单目录里,比如上图所示的 C:\us-ers\share\desktop\123目录里;

④ 360恢复区				– ×
被处理的文件都在这里做了安全备份,您可以在此将其彻底删除或恢复到处理前的恢复区占用磁盘空间:472.00 KB	状态。			清空恢复区
名称	处理时间	分类	操作	
▲ ○ 今天处理的项目 1项 占用磁盘空间: 472.00 KB				
HEUR/QVM03.0.8BA1.Malware.Gen c:\users\share\appdata\local\temp\~sfx000ddafb0c\rdp1624.exe	2020-05-29 09:25:27	360杀毒	恢复	删除
♣ 360恢复区		×		
● 將文件恢复到原来所在日录	xe 吗? 法			
《 将文件恢复到床本所在自家				
		浏览		
✓ 恢复后信任此文件,不再查杀	恢复	取消		
全选			恢复所选	删除所选

1.2 显示的问题

1) HDMI 显示,显示屏幕不能完全覆盖显示区域?

- 按下监视器上的"自动"按钮可自动调节;
- 检查显示器是否处于点对点模式,一般选择非点对点模式;
- 调整显示器支持的分辨率;

2) 连接 VGA 显示器,显示器屏幕不能完全覆盖显示器的显示区域吗?

- 按下监视器上的"自动"按钮可自动调节;
- 调整显示器支持的分辨率;
- 提供用于匹配验证的显示器型号;

如果运行的时候阻止,请选择信任可运行文件;

3) 连接到远程主机后无法更改分辨率?

 远程桌面登录到主机后,无法在主机界面修改分辨率;要修改分辨率,需要断开连接。回到终端界面后,可以进入 控制面板或设置面板修改分辨率。(控制面板或设置>分辨率)

显示	声音					
	-显示设置——	颜	分辨率 刷新率 预色深度	1280x720 60HZ 32 bpp	 	COr
						· ·
	MIC音量 win10不支持单通道 静音设置			● 双声道		
			6	保存	返回	
					, Ĵ	
	网络	显示设置				
	し し し し し し し し し し し し し し し し し し し	语言:	简体中	文	~	
		万辨 率 : 颜色:	32	/20	* *	
	诊断					
	信息					
	返回				保存	

Control Centre				
Control Centre	Dia Resolution 800 x 600	splay Properties		
System		Network St	atus: Connected	C

4) 分辨率修改后,不生效?

■ 修改分辨率后, FL200N 或 FL200M 将重新启动。重新启动后,系统会在 15 秒内提示您确定修改后的分辨率。如果在 15 秒内没有点击 "ok",系统将恢复原来的分辨率;

1.3 声音的问题

1) 耳机里没有声音?

- 更换耳机;
- 在终端配置界面,调整音量;
- 调整您登录到的远程桌面的音量;
- 检查正在播放的文件是否有声音;

2) 不能录音?

- 检查插入端子的麦克风拾音器是否正常;
- 检查终端配置屏幕上的记录开关和音量;
- 尝试更换录制软件(win10 系统录制软件无法在远程桌面使用,原因不明)

3) 录音后,回放此录音文件发现语速过快?

这种情况一般出现在连接到 win10 主机的场景中,尝试切换录制通道的方式(单声道录制改为双声道录制或双声 道录制改为单声道录制);

4) HDMI 显示无法输出声音?

■ 目前 ARM 终端的 HDMI 声音输出不是 100%匹配。如果客户购买的终端在某些 HDMI 显示器上有声音输出,请检查无声音输出的显示器是否有内置扬声器,是否正常.

1.4 网络问题

1)两台或更多的机器经常掉线?有时 A 端断开,有时 B 端断开

■ 检查机器的 IP 是否相同,如果是自动获取机器的 IP,检查是否获取到了相同的 IP;

■ 检查机器的 MAC 地址是否相同。如果 FL300 有相同的 MAC 地址,您可以使用 MAC 地址来修改它,并将新的 MAC 地址写在 u 盘上;

2)终端网络设置为自动获取 IP, 但经过一段时间后, 是否存在 IP 冲突?

■ 目前发现的现象如下:IP 网段设置为 10.*.*.*/255.255.255.0。目前, FL600w 20180901 系统包已经解决了本案的 IP 租期问题;

3)无线信号太弱

- 确保外部天线已连接;
- 确保 wifi 热点与机器之间没有墙壁遮挡信号;

4) 无线网络不稳定?

■ 检查 wifi 热点和无线设备的数量。一般来说, wifi 热点和 wifi 终端越多, wifi 干扰越严重, wifi 越不稳定;

1.5 终端系统升级问题

1)针对不同终端升	计级固件的方法是什么?	
型号	升级方法	图片
FL100/FL120	TF+usb 闪存驱动器(非二进制)	
FL300	TF卡或u盘	
	如果机器没有显示,只有 TF 卡	< न]
FL600W	双公头 USB 线+电脑 亚山的 型 A	
	双 USB	
FL600N	USB 线+电脑	
FL200N FL200M	双公头 USB 线+电脑	
FL700(RK3288)	双公头 USB 线+电脑	

2) 什么时候需要升级终端固件?

- 终端经常崩溃;
- 有一个新版本的终端固件(新版本将修复问题并添加功能,客户可以选择更新);

1.6 外设支持问题

外设设备使用三种模式和特性

	的特点	周边可见状态	支持此模式的模型
模式 1:RDP 模式	终端识别并驱动设备并将	只有这个最终用户是可见	支持所有 ARM 模型
	其映射到服务器	的	
模式 2:局域网共享模式	共享模式,所有用户可见,	所有用户可见	FL120、FL600W FL600N
	但不固定设备号,适用于		
	不同型号的外设		(需要在服务器上安装 USB
			重定向软件)
模式 3:USB 独占模式	USB 独占模式,此终端设	只有这个最终用户是可见	FL200M
	备,只有此终端用户可见,	的	
	适用于同一类型的外设		

	驱动装置	主机(服务器)安装设备驱动程序
模式 1:RDP 模式	需要	不需要
模式 2:局域网共享模式	不需要	需要
模式 3:USB 独占模式	不需要	需要

型号	是否支持	开启方式
	模式 1:支持	在终端选项中启用 USB 目录重定向(仅 USB 存储)
FL120	模式 2:支持	在终端选项中启用 USB 设备重定向(支持大多数 USB 设备)
	模式 3:不支持	不支持
	模式 1:支持	检查[启用打印机映射]和[本地磁盘映射]。不要检查[启用 USB 设备重定向]。
FL200M	模式 2:不支持	不支持
	模式 3:支持	启用[启用 USB 设备重定向],不检查[启用打印机映射]和[本地磁盘映射]
	模式 1:支持	在终端选项中启用 USB 目录重定向(仅 USB 存储)
FL600W	模式 2:支持	在终端选项中启用 USB 设备重定向(支持大多数 USB 设备)
	模式 3:不支持	不支持
	模式 1:支持	在终端选项中启用 USB 目录重定向(仅 USB 存储)
FL600N	模式 2:支持	在终端选项中启用 USB 设备重定向(支持大多数 USB 设备)
	模式 3:不支持	不支持

使用场景:

场景	建议型号及模式
单个终端使用 usb 闪存驱动器	所有型号,选择模式一
单个终端使用打印机	选择模式1。如果模式1不可用,请使用模式3
	模式 2 用于其他型号(同一型号的外设不能固定设备名称)
多个终端使用 usb 驱动器	所有型号,选择模式一
多个终端使用打印机	FL200M-RDP 模式,如果不支持此模式,请选择模式 3
多个终端使用 USB 设备, 而不是 USB	FL200M 选择模式
驱动器和打印机	模式 2 用于其他型号(同一型号的外设不能固定设备名称)

下面是每种模式的设置关系图:

Contro	ol Center Add Microsoft RDP Connection		×	
Conne Displ Network	General Options action Settings Personalization Image: Construction Settings Image: Construction Settings ay Properties Sound mapping work Settings Enable multi touch Sound mapping Image: Construction Settings ork Diagnosis Enable Printer mapping System Start a program System Start the program on construction o	Experience Gateway	Action	
2020/0	3/06 02:09:20 Ok	Cancel	ork Status: Connected	
▲FL200M 模型 1:选择[本地码		7		

▲FL200M 模型 1:选择[本地磁盘映射]

+		返回
连接名称	协议类型 服务器地址 自	动登录 操作
testvmware	、新建Microsoft RDP连接	编辑删除
	连接名称(RDP	
	服务器地址 (192.168.1.10	
	■ 记住用户名	
	用户 (1	
	密码(*	
	域	
	□ 设备重定向 保存 Ⅰ	取消
	密码 * 域	〕 〕 取消

▲ FL600N 四协议界面:选择【设备重定向】,然后模式三,不选择【设备重定向】模式

Windows 将根据你所输入的名称,为你打开相应的程序、 文件夹、文档或 Internet 资源。
打开(<u>O</u>): gpedit.msc ~
确定 取消 浏览(B) 一;默认是模式一
外设
┌ 外设配置
■ USB设备重定向
 ● U盘目录重定向 ● USB设备重定向
说明: -
1.USB目录重定向只能支持目录访问的方式重定向U盘到虚拟 桌面;
2.USB设备重定向可以以虚拟设备的形式重定向USB接口类 _ 型的打印机,扫描仪,USB转串口,摄像头,U盘等兼容的设 _
保存返回

▲FL600N 和 FL600w:型号 1 选择[U 盘目录重定向]



1)无法使用 u 盘?

■ 目前, FL200N 和 FL200M 只支持 FAT32 文件系统 u 盘,不支持 NTFS 文件系统 u 盘;

2) 不能使用打印机?

■ 打开终端设置界面的 USB 重定向功能,在主机上安装相应的 USB 重定向驱动程序;

型号	操作方法
FL120	1. 打开终端:USB 设备重定向;2. 在主机上安装 USB 重定向软件;
FL300	打印机不支持
FL600	1. 打开终端:USB 设备重定向;2. 在主机上安装 USB 重定向软件;
FL200M/FL200N	先尝试模式1。如果模式1不可用,请尝试模式3
FL700N	1. 打开终端:USB 设备重定向;2. 在主机上安装 USB 重定向软件;

Control Center	Add Microsoft RDP Connection	×	
Connection Settings Connection Settings Display Properties Conserve Settings Network Settings Network Diagnosis Contemport	General Options Experience Gateway Personalization	Action	
2020/03/06 02:54:02	Ok Cancel	work Status: Connected	

▲FL200M 型号 1:勾选【启用打印机映射】,不勾选【启用 USB 设备重定向】

Control Center	Add Microsoft RDP Connection	×
Connection Settings Connection Settings Display Properties Conserve Settings Network Settings Network Diagnosis Contemport	General Options Experience Gateway Personalization	Action
2020/03/06 02:55:34	Ok Cancel	work Status: Connected

▲FL200M 型号 1:选择【启用 USB 设备重定向】,不选择【启用打印机映射】,连接到主机后,安装打印机驱动程序;

3) 不能使用相机?

■ 目前, ARM 终端不支持摄像头;

4) 不能使用扫描枪?

- 有些扫描枪是不兼容的;
- 终端固件版本太低;

1.7 管理工具的问题

1) 管理工具无法唤醒终端?

■ 目前,只有 FL600N、FL600M、FL200N 和 FL200M ARM 机器支持远程唤醒;

2) 管理工具不能监控终端?

■ 版本 4.3 或 5.0 的管理工具, 您需要在设置中启用监控;

如果远程控制窗口出现数字 5900 或 5901,但终端无法控制,请尝试修改此数字并重新连接控制终端。如果原来是 5900,请改成 5901 如果是 5901,试着把它改成 5900;默认值是 5900;

■ FL200N(FL200M)需要使用 TCM 2.5.1 启用终端上的 VNC 功能;

day have been the												
冬病管埋	系统										_	
	终端管理			任务管理	里	TCM	正书					
- 1 2												
195	NUL (2010) 000		网络近星	·		m - to be m						
设立	连接设立	显示设置	MARIA	业书设置	云朝室間直	日志官理						
WiFi	开	~ SSID)	WiFi密码								
802.	1x 开	~ 用户:	名	密码								
VNC	п	✓ ∞□										
	т	- 留明			┛╵							
桑作	_											
行任务												
列表一												
	全部		~			今进 10%	SHA 日中利主	тсмітні	~	当前TCM证书·		
	全部		~		Q	全选取消	^{新选择 导出列表}	TCM证书	~	当前TCM证书:		
: 彩号	全部	ž		IPt	Q 也址	全选 取》 MAC地址	前选择 导出列表 镜像发布时	ТСМ证书	~	当前TCM证书: 硬件版本	任务初	术态

💻 Thin Cl	lient Management Syster General	m Ta	ısk	TCM Certificate	3				
Task Se System W VI Task Op Start T Thin Clife	lection n Setting Display Settin AFFI On ▼ SSI NC On ▼ erations asks ant List ΔII	ng Network Setting	Certificate Setting		Event Lint TOM Cart	feate	Current TCM Certificate		
ID	Type De	evice Name IF	Address	MAC Address	Image Release Time	TCM Certificate	Hardware Version	Task Status	
1	FL200M TC	22691001 19	2.168.18.107	4A:59:67:F3:88:42	20190701131847E	None TCM Certifica	te S00001		

其他型号的 VNC 远程控制终端功能默认开启;它不能被关闭;

1.8 崩溃和掉线问题

1) 崩溃的问题

- 在使用这台机器超过三到五年之后,尝试重刷终端固件;
- 这台机器是在温度过高的环境中使用的。建议环境温度低于 30 度;
- 终端系统出现问题,可以通过恢复系统默认设置或重新升级终端系统;

2) 掉线的问题

■ IP 或 MAC 冲突导致一台机器与另一台机器轮流掉线;

网络不稳定,连接电缆或网络设备(交换机等)本身不稳定(远程桌面连接需要稳定的网络环境,因为整个桌面表示 是实时交换数据);

- 这台机器是在温度过高的环境中使用的。建议环境温度低于 30 度;
- 在使用这台机器超过三到五年之后,它的硬件已经老化了;
- 子系统出现问题,可以通过恢复系统默认设置或重新升级终端系统;

3)不能退出一个问题,黑屏,有鼠标箭头可以移动吗?

■ IP 冲突,导致不完全断开连接;

4)终端卡死:鼠标可以动,但是桌面无法点击?

现象:终端假死,只有鼠标能动,但是桌面无法点击,通过拔掉网线,会自动退回终端界面;(恢复了与服务器的正常连接后,也会退回终端界面或是恢复正常的桌面)

出现这种现象,有几种可能:

◆ 终端硬件问题

通过采用一台终端连接一台服务器的方式(网络环境也和其它机器隔离开来),进行超过 12 小时的测试(播放 视频),如果无异常,基本可以判断为终端无故障;如果异常,那就是硬件问题,请寄回厂家或尝试重刷终端固 件后再测试;

◆ 网络故障

网络故障包括物理网络设备(比如网线、交换机等异常)故障和 IP 冲突、MAC 地址冲突;通过检查所有设备的 IP 和 MAC 来排除设置问题;通过更换网线或交换机来排查物理网络设备问题;

◆ 服务器资源问题

服务器资源不足,导致终端获取不到桌面数据而出现这种类似网络不佳的现象;

其原因是: 服务器无法及时发送桌面数据给终端,导致终端无法实时获取桌面画面,从而导致终端只有鼠标能动,画面卡住的情况;

(此种情况建议排查方法是:减少所带终端的数量,比如原来带 10 台的情况,现在只开两台终端,然后进行相同的操作,检查是否有故障现象出现,如果没有故障现象出现,基本上就是服务器资源不足导致;)

1.9 多用户使用问题

1) 有些软件不能多个用户同时打开?

可能的几种原因:

可能的几种原因		
可能的原因	说明	可尝试的方法
软件安装路径错误	部分软件默认安装在当前用户目录下,比	更改安装文件的路径,创建启动程序的快
	如谷歌浏览器(参考 1.10 节的方法)	捷方式,并发到所有用户的桌面上
软件不兼容	部分软件不兼容新版本 Windows 系统	在软件的快捷方式上以兼容模式运行
软件不支持多用户模式	部分软件设计的时候就是单 windows 单用	尝试用 VDI 的方式部署桌面
	户运行模式	
软件只支持管理员用户	部分软件,需要最高权限	创建管理员权限的账户给所有终端使用

■ 软件本身不支持多用户运行模式,这是软件本身的限制,除非软件开发者进行修改,否则无法实现多用户运行模式;(请尝试使用此软件的其它版本,或是使用具体相同功能的同类软件);

■ 将软件安装在 D 盘或其他盘上(不是系统盘,系统盘通常是 C 盘);部分软件会将软件安装在当前用户目录;比如 谷歌浏览器;

2) 如何将软件快捷方式发送到所有用户的桌面?

■ 复制快捷方式向公众用户的桌面(路径:C:\Users\Public\桌面);

3) 连接 win10 主机,终端可以直接关闭主机?

■ 此问题为用户权限问题,需要在组策略中进行修改;首先,输入 gpedit.msc 在运行框中打开组策略编辑器。将该位 设置为计算机配置、Windows 配置、安全设置、本地策略的用户权限分配目录。然后,找到关闭系统或计算机的选项.

1.10 像谷歌浏览器这样的软件不能运行

软件无法打开,有三种可能:软件不支持多用户模式,软件安装路径错误,软件不兼容;

可能的原因	对策
软件安装路径错误	软件应该安装在程序文件或程序文件(X86)文件下的 C 盘上;
软件不兼容	请检查运行在兼容模式
本软件不支持多用户模式	用其他同类软件代替,如 Microsoft office 软件代替 WPS

) 以谷歌浏览器为例说明具体的操作方法:

将安装文件夹"谷歌"复制到程序文件或程序文件(X86)文件夹,如下所示:

>	此电脑 > 2	本地磁	盘 (C:) > Program Files >				
		名	称	修改日期	类型	大小	
			7-Zip	2019/7/27 15:39	文件夹		
			360	2019/7/26 21:05	文件夹		
	7		Bonjour	2019/10/8 16:49	文件夹		
			Cloudpoint	2019/8/28 17:30	文件夹		
			Common Files	2019/10/8 16:49	文件夹		
rd			DIFX	2019/7/27 17:04	文件夹		
		_	FileZilla FTP Client	2019/10/17 10:30	文件夹		
			Google	2019/12/24 15:45	文件夹		
			internet explorer	2019/10/9 20:13	文件夹		
			Microsoft Office	2019/12/14 15:13	文件夹		
			Microsoft Office 15	2019/7/26 20:22	文件夹		
			MSBuild	2019/8/30 11:04	文件李		

● 启用兼容模式,通过尝试不同的兼容模式来确保软件可用;

fp Google Chrome 属性 X	
常规 快捷方式 兼容性 安全 详细信息 以前的版本	
如果此程序不能在这个版本的 Windows 上正常工作,请尝试运行兼 容性疑难解答。	
运行兼容性疑难解答	S Google Chrome Properties
如何手动选择兼容性设置?	Security Details Previous Versions General Shortcut Compatibility
兼容模式 I 以兼容模式运行这个程序: Windows Vista (Service Pack 1) v	If you have problems with this program and it worked correctly on an earlier version of Windows, select the compatibility mode that matches that earlier version. <u>Help me choose the settings</u> Compatibility mode
设置 □ 简化的颜色模式	 Run this program in compatibility mode for: Windows XP (Service Pack 3)
8 位(256)色 ~	Settings
□用 640 x 480 屏幕分辨率运行	Run in 640 x 480 screen resolution
□ 禁用全屏优化	Disable visual themes
□ 以管理员身份运行此程序	 Disable desktop composition Disable display scaling on high DPI settings
更改高 DPI 设置	Privilege Level
●更改所有用户的设置	Change settings for all users
确定 取消 应用(A)	OK Cancel Apply

替换其他同类浏览器软件

谷歌浏览器-用 firefox 代替(注意:firefox 使用的资源比谷歌少)

如果进行了如上操作后,终端还是无法使用谷歌浏览器,请尝试卸载显卡驱动后再打开;如果卸载显卡驱动后可以 打开谷歌浏览器,那问题是显卡驱动异常或是不兼容导致;

1.11 终端屏幕缓慢刷新,像幻灯片一样

- 老版本的 FL120 和 FL300 可能有这个问题,因为 7.1 RDP 版本;
- 如果除了老的 FL120 和 FL300 版本外,其他终端仍然是这种情况,请检查 RDP 加速包:RDP accelerator_v1.7.0.0.exe 是否安装在主机上,并检查组策略配置;组策略配置如下:

输入 "gpedit。在运行框中,进入组策略配置窗口,点击"计算机配置"、"管理配置"、"Windows 组件"、"远程桌面服务"和 "远程桌面会话主机"。

按键盘上的"Window +R",输入"gpedit.msc",

/ 运行		×	
Windows 将根据你所 文件夹、文档或 Intern	输入的名称,为你打开相应的 net 资源。	程序、	
打开(<u>O</u>): gpedit.msc		~	
确定	取消浏	ව <u>්(B</u>)	
点击"计算机配置→管理员模	板→windows 组件→远档	桌面会话主机"	
Local Group Policy Editor		_	
File Action View Help			
V P Computer Configuration	Windows Components	Setting	^
> Software Settings	Select an item to view its description.	Contractive X Installer Service	
Windows Settings Administrative Templates		Add features to Windows 10	
> Control Panel		📔 App Package Deployment	
> 🦳 Network		App Privacy	
Printers		App runtime	
Start Menu and Taskhar		Application Compatibility AutoPlay Paliaian	
> Start Wend and Taskbar		Biometrics	
Vindows Components		BitLocker Drive Encryption	
ActiveX Installer Service		Camera	
Add features to Windov		🧮 Cloud Content	
App Package Deployme		🚞 Connect	
App Privacy		Credential User Interface	
Application Compatibil		Data Collection and Preview Builds	
AutoPlay Policies		Desktop Gadgets	
> 📔 Biometrics		Desktop Window Manager	
> 📔 BitLocker Drive Encrypti		Device and Driver Compatibility	<u> </u>

¥

5

Local Group Policy Editor

<

📔 Camera

1.0

>

Extended Standard /

File Action View Help MDM Microsoft Secondary Authentication Factor RemoteFX for Windows Server 2008 R2 Configure RemoteFX Setting State Comment > Microsoft User Experience Virtualization Configure RemoteFX Configure RemoteFX Optimize visual experience when using RemoteFX Optimize visual experience for Remote Desktop Service Sessi... NetMeeting OneDrive Online Assistance Edit policy setting ~ Not configured Not configured No No Requirements: Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only Online Assistance Online Assistance Presentation Settings Remote Desktop Services Remote Desktop Connection Client Remote Desktop Session Host Remote Desktop Session Host Device and Resource Redirection Device and Resource Redirection Device and Resource Redirection Description: This policy setting allows you to control the availability of RemoteFX on both a Remote Desktop Virtualization Host (RD Virtualization Host) server and a Remote Desktop Session Host (RD Session Host) server. Device and Resource Redirection Licensing Printer Redirection Profiles RD Connection Broker Remote Session Environment Remote FX for Windows Server 2008 Security Session Time Limits Temporary folders Resource Session Functions When deployed on an RD Virtualization Host server, RemoteFX delivers a rich user experience by rendering content on the server by using graphics processing units (GPUs). By default, RemoteFX for RD Virtualization Host uses server-side GPUs to deliver a rich user 有四个项目:

Contraction

连接,授权,远程桌面环境,安全;

连接

Local Group Policy Editor File Action View Help

- 0 ×

Microsoft User Experience Virtualization	^	Connections				
OneDrive		Select an item to view its description.	Setting	State	Comment	
Online Assistance			E Automatic reconnection	Not configured	No	
Portable Operating System			E Allow users to connect remotely by using Remote Desktop S	Not configured	No	
Presentation Settings			E Deny logoff of an administrator logged in to the console ses	Not configured	No	
Remote Desktop Services			E Configure keep-alive connection interval	Not configured	No	
RD Licensing			E Limit number of connections	Not configured	No	
Remote Desktop Connection Client			Suspend user sign-in to complete app registration	Not configured	No	
Remote Desktop Session Host			Set rules for remote control of Remote Desktop Services use	Not configured	No	
Application Compatibility			Select network detection on the server	Not configured	No	
Connections			Select RDP transport protocols	Enabled	No	
Device and Resource Redirection			Restrict Remote Desktop Services users to a single Remote D	Not configured	No	
Licensing			Allow remote start of unlisted programs	Not configured	No	
Printer Redirection			Turn off Fair Share CPU Scheduling	Not configured	No	
Profiles				-		
RD Connection Broker						
Remote Session Environment						
Security						
Session Time Limits						
PSC Foods						
Search						
Security Center						
Shutdown Ontions						
Smart Card						
Software Protection Platform						
Sound Recorder						
Store						
Sync your settings						
Tablet PC						
Task Scheduler						
Windows Calendar						
Windows Color System	~					
>		Extended (Standard /				
setting(s)						
	合"	,如下所示:				

启用"选择 RDP 传输",如下所示:

Select RDP transport protocols Previous Setting Next Setting Not Configured Comment: Enabled Image: Comment: Disabled Image: Comment: Disabled Supported on: At least Windows Server 2012, Windows 8 or Windows RT Select Transport Type Use both UDP and TCP His policy setting allows you to specify which protocols can be like RDP to use UDP. Vou can select one of the following options: Vau can select one of the following options: We use both UDP and TCP You can select one of the following options: Use both UDP and TCP You can select one of the following options: Wuse able this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: We double of the RDP traffic will use UDP. If you select "Use either UDP or TCP" and the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use UDP. (K Cancel Apply)										<u> </u>	
Select RDP transport protocols Previous Setting Next Setting Not Configured Comment: Image: Comment: Image: Comment: Disabled Disabled Image: Comment: Image: Comment: Image: Comment: Options: At least Windows Server 2012, Windows 8 or Windows RT Image: Comment: Image: Comment: Image: Comment: Select Transport Type Image: Comment: Image: Comment:	Select RDP transp	ort protocols									\times
Not Configured Comment: Enabled Disabled Supported on: At least Windows Server 2012, Windows 8 or Windows RT Options: Help: Select Transport Type Inis policy setting allows you to specify which protocols can be used for Remote Desktop Protocol (RDP) access to this server. If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use UDP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. Will choose the optimal protocols for delivering the best user	Select RDP transp	ort protocols			Previous Sett	ting	Next	Setting]		
Enabled Disabled Supported on: At least Windows Server 2012, Windows 8 or Windows RT At least Windows Server 2012, Windows 8 or Windows RT At least Windows Server 2012, Windows 8 or Windows RT Determine the server of the server of the server. If spolicy setting allows you to specify which protocols can be used for Remote Desktop Protocol (RDP) access to this server. If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP (default)" If you select "Use either UDP or TCP." and the UDP connection is successful, most of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use TCP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel Apply	O Not Configured	Comment:									^
O Disabled At least Windows Server 2012, Windows 8 or Windows RT Options: Help: Select Transport Type This policy setting allows you to specify which protocols can be used for Remote Desktop Protocol (RDP) access to this server. If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel	Enabled										
Options: Help: Select Transport Type This policy setting allows you to specify which protocols can be used for Remote Desktop Protocol (RDP) access to this server. If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel	O Disabled	Constant									~
Options: Help: Select Transport Type This policy setting allows you to specify which protocols can be used for Remote Desktop Protocol (RDP) access to this server. If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use TCP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel		Supported on:	At least Window	vs Server 2012	2, Windows 8 o	or Windo	ws RT				^
Options: Help: Select Transport Type Use both UDP and TCP Use both UDP and TCP If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP," all of the RDP traffic will use TCP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel											~
Select Transport Type Use both UDP and TCP If you enable this policy setting, you must specify if you would like RDP to use UDP. You can select one of the following options: "Use both UDP and TCP", "Use only TCP" or "Use either UDP or TCP (default)" If you select "Use either UDP or TCP" and the UDP connection is successful, most of the RDP traffic will use UDP. If the UDP connection is not successful or if you select "Use only TCP", all of the RDP traffic will use TCP. If you disable or do not configure this policy setting, RDP will choose the optimal protocols for delivering the best user experience. OK Cancel	Options:			Help:							
OK Cancel Appiy	Select Transport Type	; ₽ ✓		This policy used for Re If you enab like RDP to You can sel TCP", "Use If you selec successful, If the UDP (TCP," all of If you disab choose the experience.	setting allows mote Desktop le this policy si use UDP. ect one of the only TCP" or "I t "Use either U most of the RI connection is n the RDP traffic ole or do not cc optimal proto	you to sp Protocol etting, you followini Use eithe DP or TC DP traffic not succe c will use onfigure to cools for co	pecify v (RDP) ou mus ⁱⁿ g optio r UDP o r UDP o P" and will us essful ou TCP. this pol beliverir	which prot access to 1 t specify if ns: "Use b or TCP (de the UDP c e UDP. r if you sel licy setting ng the bes	ocols this s f you oth L fault conne dect "l g, RDi t use	can b erver, would DP an ction i use on P will r	e ^ disis
					L	OK		Cancel		Арр	ly

许可

Local Group Policy Editor					-	٥	\times
File Action View Help							
🗢 🄿 🙍 💼 🗟 🖬 🝸							
Microsoft User Experience Virtualization	📑 Licensing						
NetMeeting	Catala Barrata Daditar Karadan	Catting	Chate	Comment			
OneDrive	Set the Remote Desktop licensing	Setting	State	Comment			
Online Assistance	linde	Use the specified Remote Desktop license servers	Not configured	No			
Portable Operating System	Edit policy setting	📰 Hide notifications about RD Licensing problems that affect t	Not configured	No			
Presentation Settings		Set the Remote Desktop licensing mode	Enabled	No			
Remote Desktop Services	Requirements:						
RD Licensing	At least Windows Server 2003 with						
> Connection Client	Service Pack 1						
🛩 🚞 Remote Desktop Session Host	Description:						
Application Compatibility	This policy setting allows you to						
Connections	specify the type of Remote Desktop						
Device and Resource Redirection	Services client access license (RDS						
Licensing	CAL) that is required to connect to						
Printer Redirection	this KD Session Host server.						
Profiles	You can use this policy setting to						
RD Connection Broker	select one of two licensing modes:						
> 📔 Remote Session Environment	Per User or Per Device.						
Security							
Session Time Limits	Per User licensing mode requires that						
Temporary folders	RD Session Host server have an RDS						
RSS Feeds	Per User CAL.						
Search							
Security Center	Per Device licensing mode requires						
Shutdown Options	that each device connecting to this						
Smart Card	Per Device CAL						
Software Protection Platform							
Sound Recorder	If you enable this policy setting, the						
Store	Remote Desktop licensing mode that						
Svnc vour settings	you specify is honored by the Remote						
Tablet PC	Desktop license server.						
Task Scheduler	If you disable or do not configure this						
Windows Calendar	policy setting, the licensing mode is						
Windows Color System	not specified at the Group Policy level.						
< >	Extended Standard						
3 setting(s)							

启用"设置远程桌面授权模式",如下所示:

 自用"设置)	远程桌面	授权模式	、",如下所示:				
Set the Remote De	esktop licensing n	node		_		×	
Set the Remote De	esktop licensing n	node	Previous Setting	Next Setting			
O Not Configured	Comment:					~	
Enabled							
 Disabled 						~	
	Supported on:	At least Windo	ows Server 2003 with Service Pack 1			^	
						~	
Options:			Help:				
Specify the licensing i server. Per User	mode for the RD S	ession Host	I his policy setting allows you to sp Desktop Services client access licer to connect to this RD Session Host You can use this policy setting to s modes: Per User or Per Device. Per User licensing mode requires th connecting to this RD Session Host CAL. Per Device licensing mode requires to this RD Session Host server have If you enable this policy setting, th mode that you specify is honored I server. If you disable or do not configure t licensing mode is not specified at the	secrity the type of R isse (RDS CAL) that server. elect one of two lic hat each user accou t server have an RD is that each device of an RDS Per Device e Remote Desktop by the Remote Desi this policy setting, 1 the Group Policy le	emote is required unt S Per Used connectin CAL. licensing ktop licen	d r g sse	
			OK	Cancel	Арр	ly	

远程会话环境



配置"RemoteFX for Windows Server 2008 R2",然后启用"限制最大颜色深度,使用硬件~, Prionitize H.264/AVC~,配置 H.264/AVC~,配置压缩~,配置图像质量~,启用 RemoteFX 编码~,配置 RemoteFX 自适应~";

a. 为 windows server 2008 R2 配置"RemoteFX"

Configure RemoteFX — — X Configure RemoteFX Previous Setting Next Setting Not Configured Comment: Next Setting V Enabled Supported on: Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only V Options: Help: V								
Configure RemoteFX Previous Setting Next Setting O Not Configured Comment: Image: Comment image: Commen	Configure Remote	x						×
O Not Configured Comment: Enabled Disabled Supported on: Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only Options: Help: 	Configure RemoteF>	х		Previous Setting	Next Settin	g		
Enabled Disabled Supported on: Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only Options: Help:	O Not Configured	Comment:						^
O Disabled Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only Options: Help:	Enabled							
Supported on: Windows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only Options: Help:	O Disabled							\sim
Options: Help:	S	Supported on:	Windows 7 or Windows Sen	ver 2008 R2 (and their	subsequent Se	vice Pa	acks) only	^
Options: Help:								~
	Options:		Help:					
This policy setting allows you to control the availability of RemoteFX on both a Remote Desktop Virtualization Host (RD Virtualization Host) server and a Remote Desktop Session Host (RD Session Host) server. When deployed on an RD Virtualization Host server, RemoteFX delivers a rich user experience by rendering content on the server by using graphics processing units (GPUs). By default, RemoteFX for RD Virtualization Host uses server-side GPUs to deliver a rich user experience over LAN connections and RDP 7.1. When deployed on an RD Session Host server, RemoteFX delivers a rich user experience by using a hardware-accelerated compression scheme. If you enable this policy setting, RemoteFX will be used to deliver a rich user experience over LAN connections and RDP 7.1. If you disable this policy setting, RemoteFX will be disabled. If you do not configure this policy setting, the default behavior			This policy RemoteFX Virtualizati (RD Sessio When dep delivers a I by using g for RD Virt user exper When dep a rich user compressi If you enal a rich user If you disa If you do r	v setting allows you to on both a Remote De ion Host) server and a n Host) server. loyed on an RD Virtuaric incluser experience by raphics processing un ualization Host uses so ience over LAN conne loyed on an RD Sessio experience by using a on scheme. ble this policy setting, experience over LAN ble this policy setting, not configure this polici	control the av sktop Virtualizi Remote Deskti lization Host set y rendering cor its (GPUs). By i erver-side GPU ctions and RDF n Host server, hardware-acc RemoteFX will connections ar RemoteFX will cy setting, the	ailabilit stion H pp Sess erver, Riv ttent or default, s to del 2 7.1. Remote elerated default be use d RDP l be disa	y of ost (RD ion Host moteFX n the serv RemoteF iver a rich FX delive d to deliv 7.1. abled. behavior	er X rs er
OK Cancel Apply				OK	Can	cel	Арр	y

Optimize visual experience when using Ren	noteFX — 🗆 X	
Optimize visual experience when using Ren	noteFX Previous Setting Next Setting	
O Not Configured Comment:	^	
Enabled		
O Disabled	×	
Windo	ws 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only	
Options:	Help:	
Screen capture rate (frames per second): Highest (best quality) ~ Screen Image Quality:	This policy setting allows you to specify the visual experience that remote users will have in Remote Desktop Connection (RDC) connections that use RemoteFX. You can use this policy to balance the network bandwidth usage with the type of graphics experience that is delivered.	
Lowest ~	Depending on the requirements of your users, you can reduce network bandwidth usage by reducing the screen capture rate. You can also reduce network bandwidth usage by reducing the image quality (increasing the amount of image compression that is performed).	
	If you have a higher than average bandwidth network, you can maximize the utilization of bandwidth by selecting the highest setting for screen capture rate and the highest setting for image quality.	
	By default, Remote Desktop Connection sessions that use RemoteFX are optimized for a balanced experience over LAN conditions. If you disable or do not configure this policy setting, Remote Desktop Connection sessions that use RemoteFX will be	$c \rightarrow$
	OK Cancel Apply	
💭 Optimize visual experience for Remote De	esktop Service Sessions — 🗌	×
Optimize visual experience for Remote D	esktop Service Sessions Previous Setting Next Setting	
O Not Configured Comment:		
Enabled		
		~
Supported on: Win	dows 7 or Windows Server 2008 R2 (and their subsequent Service Packs) only	
Options:	Help:	
Visual experience: Rich multimedia	This policy setting allows you to specify the visual experience that remote users receive in Remote Desktop Services sessions. Remote sessions on the remote computer are then optimized to support this visual experience.	
	By default, Remote Desktop Services sessions are optimized for rich multimedia, such as applications that use Silverlight or Windows Presentation Foundation. If you enable this policy setting, you must select the visual	
	experience for which you want to optimize Remote Desktop Services sessions. You can select either Rich multimedia or Text. If you disable or do not configure this policy setting, Remote	
	Desktop Services sessions are optimized for rich multimedia.	
		~
	OK Cancel Apply	

b. 配置其它, 启用"限制最大颜色深度, 使用硬件~, Prionitize H.264/AVC~, 配置 H.264/AVC~, 配置压缩~, 配置图像质量~, 启用 RemoteFX 编码~, 配置 RemoteFX 自适应~"

Limit maximum color depth	– 🗆 X	
Limit maximum color depth	Previous Setting Next Setting	
O Not Configured Comment:	<u>^</u>	
Enabled		
O Disabled	v	
Supported on.	Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows XP	
Options:	Help:	
Color Depth Client Compatible	 This policy setting allows you to specify the maximum color resolution (color depth) for Remote Desktop Services connections. 	
	You can use this policy setting to set a limit on the color depth of any connection that uses RDP. Limiting the color depth can improve connection performance, particularly over slow links, and reduce server load.	
	If you enable this policy setting, the color depth that you specify is the maximum color depth allowed for a user's RDP connection. The actual color depth for the connection is determined by the color support available on the client computer. If you select Client Compatible, the highest color depth supported by the client will be used.	
	If you disable or do not configure this policy setting, the color depth for connections is not specified at the Group Policy level.	· ·
	Note: 1. Setting the color depth to 24 bits is only supported on	
L	OK Cancel Apply	
Use the hardware default graphics a	dapter for all Remote Desktop Services sessions — 🗆 🗙	
Use the hardware default graphics	adapter for all Remote Desktop Services sessions	
Previous Setting Next Setting		
O Not Configured Comment:		
Enabled		
O Disabled	×	
Supported on.	At least Windows Server 2012, Windows 8 or Windows RT	
Options:	Help:	
	This policy setting enables system administrators to change the graphics rendering for all Remote Desktop Services sessions.	
	If you enable this policy setting, all Remote Desktop Services sessions use the hardware graphics renderer instead of the Microsoft Basic Render Driver as the default adapter.	
	If you disable this policy setting, all Remote Desktop Services sessions use the Microsoft Basic Render Driver as the default adapter.	
	If you do not configure this policy setting, Remote Desktop Services sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. In all other cases, Remote Desktop Services sessions use the hardware graphics renderer by default.	
	NOTE: The policy setting affects only the default graphics processing unit (GPU) on a computer with more than one GPU	
	OK Cancel Apply	

Prioritize H.264/A	AVC 444 graphics n	node for Remote	Desktop Connections		— D	Х	
Prioritize H.264/	AVC 444 graphics	mode for Remote	e Desktop Connections	Previous Setting	Next Setting		
○ Not Configured	Comment:					^	
 Enabled 							
 Disabled 						\sim	
	Supported on:	At least Window	ws Server 2016, Windows	10		$\hat{}$	
Options:			Help:				
			This policy setting prio for non-RemoteFX vGP the RDP server, the sen an RDP 10 connection H.264/AVC 444.	ritizes the H.264/AVC U scenarios. When y rer will use H.264/AV where both the client	444 graphics mod ou use this setting C 444 as the codec t and server can use	e ^ on in e	
				OK (Cancel App	ly V	
💭 Configure H.264/	/AVC hardware en	coding for Remo	te Desktop Connections		— 🗆	×	
Configure H.264	AVC hardware en	coding for Remo	ote Desktop Connections	Previous Setting	Next Setting	9	
O Not Configured	Comment:					~	
Enabled							
O Disabled						\sim	
	Supported on:	At least Windo	ws Server 2016, Windows	10		< >	
Options:			Help:				
Prefer AVC hardware	encoding:		This policy setting lets	you enable H.264/A	VC hardware encod	ding ^	
Always attempt			hardware encoding, if	an error occurs, we v	vill attempt to use	icu	
			we will always use soft	ware encoding.	configure this por	icy,	
			If you set the encoding Desktop will always try when available, be awa Hyper-V with Remotef on the Hyper-V host m	g option to "Always A to use H.264/AVC h are that, for Window: FX vGPU enabled, the nachine.	Attempt", Remote ardware encoding s Server running e policy has to be s	et	
			If you set the encoding vGPU virtual machines running Hyper-V with be set on the Hyper-V	g option to "Attempt 5" be aware that, for \ RemoteFX vGPU ena host machine.	only for RemoteF Windows Server bled, the policy ha	(s to	
<		>	If you set the encoding RemoteFX vGPU scena hardware encoding for	g option to "Attempt arios", Remote Deskto r all scenarios except	only for non- op attempts to use RemoteFX vGPU.	~	
				ОК	Cancel Ap	ply	

Configure compression for RemoteFX Configure compression for RemoteFX		
📆 Configure compression for RemoteFX	, data	×
	data Previous Setting Next Setting	
Not Configured Comment: Enabled		
O Disabled Supported on:	At least Windows Vista with Service Pack 1	
Ontions	Halo	
	This policy setting allows you to specify which Remote Desktop	
Optimized to use less memory	Protocol (RDP) compression algorithm to use. By default, servers use an RDP compression algorithm that is	
	If you enable this policy setting, you can specify which RDP compression algorithm to use. If you select the algorithm that is optimized to use less memory, this option is less memory- intensive, but uses more network bandwidth. If you select the algorithm that is optimized to use less network bandwidth, this option uses less network bandwidth, but is more memory- intensive. Additionally, a third option is available that balances memory usage and network bandwidth. In Windows 8 only the compression algorithm that balances memory usage and bandwidth is used.	
	You can also choose not to use an RDP compression algorithm. Choosing not to use an RDP compression algorithm will use more network bandwidth and is only recommended if you are using a hardware device that is designed to optimize network	
Configure image quality for RemoteFX Configure image quality for RemoteFX Only Configure image quality for RemoteFX	Adaptive Graphics – – X Adaptive Graphics Previous Setting Next Setting	
Not Configured Comment		
C LINDICU	^	
O Disabled Supported on: At	t least Windows Server 2012, Windows 8 or Windows RT	
O Disabled Supported on:	t least Windows Server 2012, Windows 8 or Windows RT	
O Disabled Supported on: Ar Options: Image quality: Medium V	t least Windows Server 2012, Windows 8 or Windows RT Help: This policy setting allows you to specify the visual quality for remote users when connecting to this computer by using Remote Desktop Connection. You can use this policy setting to balance the network bandwidth usage with the visual quality that is delivered. If you enable this policy setting and set quality to Low, RemoteFX Adaptive Graphics uses an encoding mechanism that results in nedium quality images. This mode consumes the lowest amount of network bandwidth of the quality modes. If you enable this policy setting and set quality to Medium, RemoteFX Adaptive Graphics uses an encoding mechanism that results in medium quality images. This mode provides better graphics quality than low quality and uses less bandwidth than high quality. If you enable this policy setting and set quality to High, RemoteFX Adaptive Graphics uses an encoding mechanism that results in high quality images and consumes moderate network bandwidth. If you enable this policy setting and set quality to Lossless, RemoteFX Adaptive Graphics uses lossless encoding, In this mode, the color integrity of the graphics data is not impacted.	
O Disabled Supported on:	t least Windows Server 2012, Windows 8 or Windows RT Help: This policy setting allows you to specify the visual quality for remote users when connecting to this computer by using Remote Desktop Connection. You can use this policy setting to balance the network bandwidth usage with the visual quality that is delivered. If you enable this policy setting and set quality to Low, RemoteFX Adaptive Graphics uses an encoding mechanism that results in low quality images. This mode consumes the lowest amount of network bandwidth of the quality modes. If you enable this policy setting and set quality to Medium, RemoteFX Adaptive Graphics uses an encoding mechanism that results in medium quality images. This mode provides better graphics quality than low quality and uses less bandwidth than high quality. If you enable this policy setting and set quality to High, RemoteFX Adaptive Graphics uses an encoding mechanism that results in high quality images and consumes moderate network bandwidth. If you enable this policy setting and set quality to Lossless, RemoteFX Adaptive Graphics uses lossless encoding. In this mode, the color integrity of the graphics data is not impacted. OK Cancel Additive Cancel	

Enable RemoteFX	(encoding for Ren	noteFX clients de	signed for Windows Server 2008 R2 SP1 — 🛛 🗙	
Enable RemoteFX	(encoding for Ren	noteFX clients de	esigned for Windows Server 2008 R2 SP1	
Previous Setting	Next Setting]		
O Not Configured	Comment:		~	
Enabled				
 Disabled 	C		~	
	Supported on:	At least Windo	ws Server 2012, Windows 8 or Windows RT	
Options:			Help:	
			This policy setting allows you to configure graphics encoding to use the RemoteFX Codec on the Remote Desktop Session Host server so that the sessions are compatible with non-Windows thin client devices designed for Windows Server 2008 R2 SP1. These clients only support the Windows Server 2008 R2 SP1 RemoteFX Codec.If you enable this policy setting, users' sessions on this server will only use the Windows Server 2008 R2 SP1 RemoteFX Codec for encoding. This mode is compatible with thin client devices that only support the Windows Server 2008 R2 SP1 RemoteFX Codec.If you disable or do not configure this policy setting, non-Windows thin clients that only support the Windows Server 2008 R2 SP1 RemoteFX Code will not be able to connect to this server. This policy setting applies only to clients that are using Remote Desktop Protocol (RDP) 7.1, and does not affect clients that are using other RDP versions.	
			OK Cancel Apply	
Configure Remot	eFX Adaptive Grap	hics	- D X	1 🗡
Configure Remot	eFX Adaptive Grap	hics	Previous Setting Next Setting	
O Not Configured	Comment:		^	
Enabled				
O Disabled	Supported on		~	
	Supported on.	At least Windo	ws Server 2012, Windows 8 or Windows RT	
Options:			Help:	
RDP experience:			This policy setting allows the administrator to configure the	
Optimize for server s	calability		Remote Desktop Virtualization Host servers. By default, the system will choose the best experience based on available	
			system will choose the best experience based on available nework bandwidth. If you enable this policy setting, the RemoteFX experience could be set to one of the following options: 1. Let the system choose the experience for the network condition 2. Optimize for server scalability 3. Optimize for server scalability 3. Optimize for minimum bandwidth usage If you disable or do not configure this policy setting, the RemoteFX experience will change dynamically based on the network condition."	
<		>		
			OK Cancel Apply	
	-			_

■ 安全

A control to the second sec	P Land Carry Dalias Editor								
Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian Work Varian	File Action View Help								- 6 /
Monto Alexander Strander Over de Strander <	🔶 🤿 🙋 📷 🗟 🖬	1 7							
Market State Market State <td>Microsoft User Experience Virt</td> <td>ualization 🔺 📔</td> <td>Security</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Microsoft User Experience Virt	ualization 🔺 📔	Security						
Seven aller all constrained with the seven all cons	NetMeeting	Select	an item to view its description.	Setting			State	Comment	
Require uses automatical connections by using Network Level Automatications of the Experiment Parameter and Par	OneDrive Online Assistance			E Server authentication ce	rtificate template		Not configured	No	
Personalization Provide standard P	Portable Operating System			E Set client connection en	cryption level		Not configured	No	
Import of the section of	Presentation Settings			Always prompt for pass	word upon connection		Not configured	No	
Particular Particular Particular Particular <td>Remote Desktop Services</td> <td></td> <td></td> <td>E Require secure RPC con</td> <td>munication</td> <td></td> <td>Not configured</td> <td>No</td> <td></td>	Remote Desktop Services			E Require secure RPC con	munication		Not configured	No	
<pre>in the second seco</pre>	RD Licensing	an Client		Require use of specific s	ecurity layer for remot	e (RDP) conn	Not configured	No	
Image: Section Comparison of the secti	Remote Desktop Connection Remote Desktop Session +	lost		Require user authentical	tion for remote connec	tions by usin	Disabled	No	
terrenter terenter terenter terenter terenter terenter	🔲 Application Compatibi	lity		I. Require user addrenates		actions by domini	bibabica		
■ control framework for the formation of the formation	Connections								
Provide Control from the contrel from the contrel from the contrel from the contrel	Device and Resource R	edirection							
Province the state of th	Printer Redirection								
tower / Care in the constant from the constant	Profiles								
Image: State in the	RD Connection Broker								
The second s	> Remote Session Enviro	nment							
	Security Session Time Limits								
If strate Subsets Offices Subsets Of	Temporary folders								
Bach Services Se	RSS Feeds								
were dear Some to dear Som	Search								
where because Subtrace Decisions Holms Subtrace Decisions Holms Med Sections Previous Sections P	Security Center								
Setting Protection Reference were were detection Reference Set Rescards and Rescards were authentication for remote connections by using Network Level Authentication Previous Setting Verd Setting Note Configured Comment Disabled Supported on: At least Windows Vista Comment Disabled This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host set in the remote connection process. Options: Help: This policy setting allows you to specify whether to require user authentication for remote connection process. Up you called the solicy setting allows to the RD Session Host set in the remote connection process. Up you called the logicity setting allows to the RD Session Host set in the remote connection process. Up you called the logicity setting allows to the RD Session Host set in the remote connection process. Up you called the logicity setting allows the vector the RD Session Host set in the remote connection process.	Smart Card								
is de le	Software Protection Platform								
Note of the service	Sound Recorder								
terement terem	Store								
Wedward Cold Statest Control Statest In the data Nervork & Statest / States	a sync your settings Tablet PC								
whether def views windows def views Require user authentication for remote connections by using Network Level Authentication Require user authentication for remote connections by using Network Level Authentication Require user authentication for remote connections by using Network Level Authentication Previous Setting Net Configured Disabled Supported on: Help: Cotions: Cotions: Cotio	Task Scheduler								
Webset Cols Setting Control & Standard (Standard / Standard / S	Windows Calendar								
*************************************	Windows Color System	× Fiter	ided (Standard /						
株用 "使用 Network 级别的身份验证来要求远程连接的用户身份验证",如下所示: ● require user authentication for remote connections by using Network Level Authentication Previous Setting Netro Setting	7 setting(s)	- Chief							
Require user authentication for remote connections by using Network Level Authentication Require user authentication for remote connections by using Network Level Authentication Previous Setting Net Configured Comment: Enabled Obtabled Supported on: At least Windows Vista This policy setting allows you to specify whether to require user authentication for remote connections by using Network Level Authentication The policy setting allows you to specify whether to require user authentication for remote connections by using Network Level Authentication. This policy setting allows you to specify whether to require user authentication for remote connections by using Network Level Authentication. This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server. Options: Help:	林田"庙田 Na	work 奶 剧	的自从必证本	西	的田白自	公应证,	, 70下前	f≓.	
Require user authentication for remote connections by using Network Level Authentication Previous Setting Next Setting Not Configured Comment: Disabled Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Sesion Host support Network Level Authentication. This policy setting enhances security by requiring that user authentication or the client support Network Level Authentication. This policy setting, only client computers that support Network Level Authentication in the upper refer connect to the RD Sesion Host secure. To determine whether a client computer supports Network Level Authentication for server bestop Connection on the client Desktop Connection on the client Computer supports Network Level Authentication is in the required for user authentication is not required for user authentication before allowing remote Work Rever Authentication Defore allowing remote	示用 使用 Ne	IWUK 级加	的名仍巡凪不	安不起性建步	(1)用/ 为	仍驰阻	, <u>9</u> 4 [17]	121.	
	Require user auth	entication for ren	note connections by u	sing Network Level /	Authentication			×	
Require user authentication for remote connections by using Network Level Authentication Previous Setting NextSetting Net Configured Comment: Enabled Image: Comment: Disabled At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication or remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication on course and then close to connect to the RD Session Host support Network Level Authentication on connect to the RD Session Host support Network Level Authentication on connect to the RD Session Host support Network Level Authentication on the clear connect on process. If you enable this policy setting, only client computer supports Network Level Authentication is not required for user authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote	OF Require user auti	entreation for fer	iote connections by a	sing recivery cerery	adhendeadon			\sim	
Reguine user authentication for remote connections by using Network Level Authentication Previous Setting NetdSetting Not Configured Comment: Enabled Image: Comment: Disabled Image: Comment: Options: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that Support Network Level Authentication and connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication of the RD Session Host server. To determine whether a client computer supports Network Level Authentication is not nequired, click thereo Desktop Connection and the policy for the Phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not nequired for user authentication before allowing remote		10 10 A			A 41 12 12				
Previous Setting Next Setting O Not Configured Comment: © Enabled Image: Comment: @ Disabled Supported on: At least Windows Vista Image: Comment: Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication below setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication on the client computer support Network Level Authentication on the client computer, click the icon in the upper-left comer of the Remote Desktop Connection dialog box, look for the phrase Network Level Authentication is protected. If you disable this policy setting network Level Authentication is in the remote connection for allog box, look for the phrase Network Level Authentication is upported. If you disable this policy setting, network Level Authentication is not required for user authentication supported. If you disable this policy setting network Level Authentication is not required for user authentication before allowing remote	Require user autr	nentication for rer	note connections by u	ising Network Level	Authentication				
Previous setting Previous setting Not Configured Comment: Enabled Image: Comment: Disabled Supported on: At least Windows Vista Image: Comment: Options: Help: This policy setting allows you to specify whether to require user suthentication for remote connections to the RD Session Host server by using Network Level Authentication cure artier in the remote connection process. If you enable this policy setting, only client computer sthat support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication dialog box, and then click About. In the phrase Network Level Authentication dialog box, and then click About. In the phrase Network Level Authentication dialog box, and then click About. In the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is propreted. If you disable this policy setting. Network Level Authentication is not required for user authentication before allowing remote	Desuisus Catting	Maria Castina							
Not Configured Comment: Image: Comment: Image: Comment: Image: Comment: At least Windows Vista Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication occur earlier in the remote connection to the RD Session Host server by using Network Level Authentication concur earlier in the remote connection to the RD Session Host Session Host server. Image: The transmission of the transmission of the transmission occur earlier in the remote connection to the RD Session Host Session Host server. Image: The transmission occur earlier in the remote connection to the RD Session Host server. Image: The transmission occur earlier in the remote connection on the client on the RD Session Host server. Image: The transmission occur earlier in the remote connection on the Client on the Client on the User Authentication and the State Security by requiring that user authentication occur earlier in the remote connection dialog box, and then click About. In the About Hemote Desktop Connection allog box, and then click About. In the About Hemote Desktop Connection and the Click About. In the About Hemote Desktop Connection dialog box, and then click About. In the About Hemote Desktop Connection allog box, and then click About. In the About Hemote Desktop Connection allog box, and then click About. In the About Hemote Desktop Connection allog box, and then click About. In the About Hemote Desktop Connection allog box, and then click About. In the About Hemote Desktop Co	Previous Setting								
Okt Configured Comment: Enabled Image: Comment: Bisabled At least Windows Vista Options: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialg box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote		- ·							
Chabled Disabled Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication on the client Authentication and connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. If you enable this policy setting, only client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication server. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote Work Cancel Authentication server.	O Not Configured	Comment:						~	
Obsabled Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that supports Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication or not client computer, click the icon in the upper-left conner of the Remote Desktop Connection dialog box, and then dick About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you clisable this policy setting, Network Level Authentication is not required for user authentication before allowing remote V OK Cancel	-								
Original Supported on: At least Windows Vista At least Vist	 Enabled 								
Obisabled Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote V	0.00							U	
Supported on: At least Windows Vista Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host computer, stath server by using Network verel Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication server. To determine whether a client computer supports Network Level Authentication, stat Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then Click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote ~	Disabled							×	
Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host enhances security by requiring that user authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote		Supported on:	At least Windows Vi	sta				~	
Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote									
Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote								\sim	
Options: Help: This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote	_ .								
This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote	Options:		He	p:					
This policy setting allows you to specify whether to require user authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote									
authentication for remote connections to the RD Session Host server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote ¥			Th	is policy setting allo	ws you to specif	v whether t	o require user	1~	
server by using Network Level Authentication. This policy setting enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			au	thentication for rem	ote connections	to the RD S	ession Host		
enhances security by requiring that user authentication occur earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			ser	ver by using Netwo	k Level Authent	ication. Thi	s policy setting		
earlier in the remote connection process. If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote V OK Cancel Apply			en	hances security by re	equiring that us	er authentic	ation occur		
If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			ea	rlier in the remote co	nnection proce	ss.			
If you enable this policy setting, only client computers that support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote									
support Network Level Authentication can connect to the RD Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			If v	ou enable this polic	y settina, only c	lient comp	iters that		
Session Host server. To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			su	pport Network Level	Authentication	can connec	t to the RD		
To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			Se	ssion Host server.					
To determine whether a client computer supports Network Level Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote									
Authentication, start Remote Desktop Connection on the client computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			To	determine whether	a client comput	er supports	Network Level		
computer, click the icon in the upper-left corner of the Remote Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote OK Cancel			Au	thentication. start R	emote Desktop	Connection	on the client		
Desktop Connection dialog box, and then click About. In the About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			co	mputer, click the ico	n in the upper-	left corner o	f the Remote		
About Remote Desktop Connection dialog box, look for the phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			De	sktop Connection di	alog box, and th	hen click Ab	out. In the		
phrase Network Level Authentication supported. If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			Ab	out Remote Desktor	Connection di	alog box, lo	ok for the		
If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote			ph	rase Network Level	Authentication s	upported.			
If you disable this policy setting, Network Level Authentication is not required for user authentication before allowing remote OK Cancel									
OK Cancel Apply			lf v	ou disable this polic	y setting, Netw	ork Level Au	thentication is		
OK Cancel Apply			no	t required for user a	thentication be	fore allowin	ng remote		
OK Cancel Apply				-				×	
OK Cancel Apply							_		
					OK	Cancel	VlagA		

更改之后,单击"Apply"生效.

1.12 如何禁止使用 U 盘,禁止修改终端设置

- 不使用 usb 闪存驱动器,在两个步骤:
- 1) 通过修改终端设置,禁用 U 盘功能

Control Center	Add Microsoft RDP Connection	×	
Connection Settings Display Properties Consection Settings Network Settings Network Diagnosis System	General Options Experience Gateway Personalization Ilocal disk mapping Ilocal disk mapping Pacconnect if connection is dropped Enable multi touch Sound mapping Play on remote computer WLAN compressing Enable RemoteFX graphic feature Redefined the RDP port 3389 Enable Network Level Authentication(NLA) Enable multimedia redirection Enable serial port mapping Enable serial port mapping Start a program Start the program on connection Full path name: Runtime folder:	Action	
2020/03/06 02:10:55	Ok Cancel	twork Status: Connected	

▲FL200M,【本地磁盘映射】和【启用 USB 设备重定向】选项,不要勾选

外设配置 ——		
■ USB设备	重定向	
● U盘目	录重定向	
O USB-	设备重定向	
说明:		<u> </u>
1.USB目: 桌面;	录重定向只能支持目录访问的方式重定向Ua	盘到虚拟
2.USB设 型的打印框	备重定向可以以虚拟设备的形式重定向USB L,扫描仪,USB转串口,摄像头,U盘等差	接口类 _
	保存	返回
Ŋ 和 FL600w:	取消【USB 设备重定向】	



2) 通过设置终端密码,防止用户修改终端配置(设置密码后,每次进入终端设置界面,都需要输入密码;)

Cor	trol Center					
			System			
	Info	rmation Voice	Advance Operation	Time		
Co	nnection Settings	ction				
				(manufacture)		
D	splay Properties	Restart	Upgrade	Export Log	_	
		Password	Change Password			
1	etwork Settings C	ther Settings	New Password:			
		Always Connect.	New Password.			
N	etwork Diagnosis	Delay Time of Auto	Password Confirm:			
	A					
			Confirm	Cancel		
	Jystem					

▲FL200M: 密码设置界面,注意:如果你忘记了你的密码,通过恢复出厂设置清除它;

密码	
新密码	
_ 再功忽码	
旧密码	
新密码	
┃	
±1100 (X	
	保存 返回

▲FL600N 和 FL600w 密码设置界面

■ 不允许修改终端设置:

通过设置终端密码,用户无法修改终端配置(设置密码后,每次进入终端设置界面,都需要输入密码);

Control Center			×	
		System		
<u>es</u>	Information Voice	Advance Operation Time		
Connection Settings	Action			
	Battart	Unarrada		
Display Properties	Restart	opgrade Export Log		
	Password	Change Password		
Network Settings	Other Settings	New Password:		
	Always Connect			
Network Diagnosis	Delay Time of Auto	Password Confirm:		
System		Confirm Cancel		
2020/03/06 02:10:11		Netwo	rk Status: Connected	

▲FL200M 密码设置界面;

密码	
_设置新密码	
新密码	
重输一次	
旧密码	
新密码	
重输一次	
L	
	保存 返回

▲FL600N 和 FL600w 密码设置界面

1.13 忘记终端密码

下面是每个终端的超级密码和密码重置方法

型号	超级密码	密码重置的方法
N380	Updateme	重新刷终端固件
FL120	sharefl120 或 fladmin	重新刷终端固件
FL200N、FL200M	没有	将系统恢复到工厂状态
FL300	cloudcomputer300	重新刷终端固件
FL600w	fladmin	重新刷终端固件
FL600N	fladmin	重新刷终端固件

FL200M:恢复出厂复位

如果无法启动终端系统,在关机情况下,长时间按电源键可弹出恢复菜单,选择:Factory reset



注:目前只有终端固件版本超过 20190515 才支持此功能。

1.14 恢复出厂设置

- FL120 恢复到出厂复位 重新刷终端固件
- FL200M 恢复出厂复位

如果无法启动终端系统,在关机情况下,长时间按电源键可弹出恢复菜单,选择:Factory reset



注:目前只有终端固件版本超过 20190515 才支持此功能。

■ FL600w恢复到出厂复位

在界面上点击恢复按钮;如果无法显示,则只能重新刷入终端固件;

欢迎使用!			
查找主机			
SHARE-PC(192.168	3. 18. 103)		连接
			刷新
			控制面板
本机IP:	192. 168. 18. 108		、大机
■ 一直自动连接			
主机1	主机2	主机3	配置
控制面板			
P			
网络	显示与声音	外设与启动	日期与时间
di tel	14日上午有		
±14-)		山昌应拜	_{示切信} 志
升级与恢复			
A.	四史初	M≯€	7史利
┌恢复设置			
	恢复回默认		
保有	字设置	加载设置	
<u>.</u>			返回



■ FL600N 恢复出厂复位

在界面上点击恢复按钮;如果无法显示,则只能重新刷入终端固件;





1.15 终端可以关闭主机?

需要修改组策略配置,以 win7 为例,操作方法如下:



Local Group Policy Editor		-	
File Action View Help			
🗢 🔿 🙍 📰 💥 🖹 😖 🛛 🖬			
Local Computer Policy	Policy	Security Setting	
a 👰 Computer Configuration	Allow log on through Remote Deskton Services	Administrators Remote	
Software Settings	Back un files and directories	Administrators Backup	
a 🚞 Windows Settings	Bypass traverse checking	Evenyone LOCAL SERVIC	
Name Resolution Policy	Change the system time	LOCAL SERVICE Admini	
Scripts (Startup/Shutdown)	Change the time zone	LOCAL SERVICE Admini	
Deployed Printers	Create a pagefile	Administrators	Shut down the system Properties 8
Security Settings	Create a token object	Administrators	
Account Policies	Create a lokel object	LOCAL SERVICE NETWO	Local Security Setting Explain
Local Policies	Create global objects	EOCAL SERVICE, NETWO	
Audit Policy	Create permanent shared objects	Administrators	Shut down the system
Security Options	B Debug programs	Administrators	
Security Options	Debug programs	Administrators	
Windows Firewall with Advanced Security	Deny access to this computer from the network	Guest	
Dublic Key Delicies	Long Deny log on as a batch Job		Administrators
Software Restriction Policies	Deny log on as a service	C	Backup Operators
Software Restriction Policies	Beny log on locally	Guest	Users
IP Security Policies on Local Computer	leg Deny log on through Remote Desktop Services		
Advanced Audit Policy Configuration	in Enable computer and user accounts to be trusted for delega		
Policy-based OoS	log Force shutdown from a remote system	Administrators	
Administrative Templates	log Generate security audits	LOCAL SERVICE, NETWO	
a 🕵 User Configuration	impersonate a client after authentication	LOCAL SERVICE, NETWO	
Software Settings	increase a process working set	Users	
Windows Settings	increase scheduling priority	Administrators	Add Lleas or Group Remove
Administrative Templates	Load and unload device drivers	Administrators	Add User of Caloup
	lock pages in memory	AL 111 A. B. I	
	log Log on as a batch job	Administrators, Backup	
	log Log on as a service	NT SERVICE ALL SERVIC	
	ling Manage auditing and security log	Administrators	
	leg Modify an object label		
	ling liviodity firmware environment values	Administrators	
	lig Perform volume maintenance tasks	Administrators	
	in Profile single process	Administrators	Carica Appy
	Profile system performance	Administrators, NT SERVI	
	We Kemove computer from docking station	Administrators, Users	
	Replace a process level token	LOCAL SERVICE, NETWO	
	i Restore files and directories	Administrators, Backup	
	🔤 Shut down the system	Administrators, Users, Ba	
	Synchronize directory service data		
	Take ownership of files or other objects	Administrators	

去(电脑配置 Windows >设置>安全设置>本地策略>用户权限分配),修改力从远程系统关闭,关闭系统,删除用户不允许 关闭的力量从远程系统关闭窗口和关闭系统窗口,并重新启动计算机才能生效。

<mark>注:</mark>用户表示标准用户组,管理员表示管理员用户组,管理员表示管理员用户。标准用户在用户组中,管理员类型 在管理员用户组中。

1.16 其他问题

1.16.1 NSIS 错误:启动安装程序错误?

可能有三个原因:

1) 在英文系统中,软件所在的路径中有中文字符,也就是说,软件所在的文件夹或上面文件夹的名称中有中文;或 复制文件在桌面下运行(注意:文件名不能有中文字符)

2)下载或传送此档案时发生损坏或部分资料遗失;再次下载或传输此文件;

3) 被杀毒软件误杀;关闭或完全退出杀毒软件, 然后下载软件重新运行;

1.16.2 安装 VDPlayer 报错?

此问题是系统导致,请尝试重新安装系统;

1.16.3 终端连接到主机后,无法播放视频?

目前发现此问题出现在小部分机子上,系显卡驱动异常导致,请尝试更换不同版本的显卡驱动;

1.16.4 登陆界面不显示账户列表?

Windows 默认不会在登陆界面显示所有账户列表,如果需要显示所有账户,请在部署工具上修改为 RDP 模式,如下图:

RDP桌面部署v1.6.21 wv	ww.thinstation.cn			
快速部署	模式切换 ◎ RDP模式		系统信息 系统: Microsoft Windows 7 旗舰版	64-bit 6.1.7601
加量回建版戸	O SSL模式		RDP版本: 6.1.7601.17514	RDP状态: Listening
具它工具	O 协商模式			
教程			<u>桌面测试></u>	多用户状态>
English	远程控制终端		软	件安装
	终端IP:	192.168.1.108	安装	RDP加速包>
	端口号:	5900 💌	Ē	<u> </u>
	<u>连接终端</u> ;	<u>></u>	系	统设置
			开启队	5火墙服务>
注音 男面上加下划线的			系统	<u>更新开关></u>
文字都是可点击的				<u>重启></u>
	口尔族为生中的样子			
	D 经19 IX / J K D P 模式			Ť

1.16.5 远程桌面服务启动的时候,报错误 2、错误 126

打开 regedit, 找到路径 HKLM\System\CurrentControlSet\Services\TermService\Parameters, 发现少了一个二制文件 serviceDLL。

手动创建,右键新建-->可扩充字符段值,设置名称为 serviceDLL,值 %SystemRoot%\System32\termsrv.dll 如图:

创建好了之后如图:

♪注册表编辑器 ☆供(D) 検想(D) 表示の 体帯さ(A) 帮助(A)				
又(中(F) 明耀(E) 豊智(V) 収蔵夫(A) 報助(H Parameters) _	夕称	厳思	教課
Performance			PEG 67	(動道士:()票)
TFsFlt		Ware in DU	REG EXDAND CZ	(Kurters Beetf() Surters 22) termine all
Themes		serviceDLL	REG_EXPAND_52	%SystemRoot%(System32\termsrv.dil
		ServiceDIIUnio	REG_DWORD	0x0000001(1)
- TrkWks				
TrustedInstaller				
STRATE				
TSDefenseBt				
⊳ - 🏭 tsnethlpx64				
tssecsrv				
🛛 - 🏭 TSSysKit				
> - 🏭 tunnel				
⊳-]]i uagp35	E.			
🛛 - 🏭 UGatherer				
UGTHRSVC				
—🍌 uliagpkx	-			
库机\HKEY_LOCAL_MACHINE\SYSTEM\Curre	ntC	ontrolSet\services\Te	rmService\Paramete	ers

创建好之后,再次启动 Remote Desktop Services 服务,无报错。服务器远程访问恢复正常。 注意:如果是 termsrv.dll 库文件缺失或损坏,可以从同版本其他操作系统中拷贝一个文件进行快速修复

1.17 域用户名问题

域用户名的输入方式有三种,如下

域用户名输入的三种方式						
比如用户名是 user1, 域名是 share.cc	om in the second s					
方法一:直接输入方式	方法二: @方式	方法三: /方式				
用户名栏输入用户名,	用户名输入 : <u>user1@share.com</u>	用户名栏输入: share.com/user1				
域名栏输入域名	域名栏不用输入	域名栏不用输入				

捷径配置							
自动 主机1	IP 地址	用户名	密码	端口	域		
\odot		user1	*****	3389	share. co		
■ 记住用户	白名和密码						
主机2 〇	白名和密码			3389			
主机3 〇	白名和密码			3389			
自启动时间 3	(单位/秒):		保存		返回		
▲方法-	_						

捷径配置	<u> 뮌</u> 크.				
自动 主机1	IP 地址	用户名	密码	端口	域
•		user1	*****	3389	share. co
 记住用户名 主机2 〇 〇 □ 记住用户名 	3和密码 3和密码			3389	
主机3 ○ □ 记住用户名 自己动时间(名和密码]	3389	
3	110/初7 :		保存		返回
▲方法二					

捷径配置					
自动 主机1	IP 地址	用户名	密码	端口	域
 ① □ 记住用户名和 	密码	user1@shar	*****	3389	
主机2 ○ ■ 记住用户名和	密码			3389	
主机3 〇 回 に住用户名和	密码			3389	
自启动时间(单位 3	立/秒):		保存		返回

▲方法三

1.18 终端连接后, Remote Desktop Services 停止或 Remote Desktop Services

丢失?

出现此问题,请按如下方法进行修复(修复时间比较长,耐心等待):

- 1)下载当前系统的微软原版 ISO 文件;
- 2) 解压此文件;
- 3)运行解压出来的"Setup.exe"程序;
- 4) 按提示操作,出现安装类型的提示时,请选择"升级"(如果弹出是否保留文件、设置和程序,请点击"是");

升级(U) 升级到较新版本的 Windows 并保留文件、设置和程序。升级选项仅在运行现有版本 的 Windows 时才可用。建议您先备份文件然后再继续执行操作。
自定义(高级)(C) 安装 Windows 的新副本。此选项不会保留您的文件、设置和程序。此选项对磁盘和 分区所做的更改在您使用安装光盘启动计算机时可用。建议您先备份文件然后再继续 执行操作。

此过程耗时较长,请耐心等待;

5)安装完成后,如果依然无法连接,请使用部署工具重新进行部署;

2. 四个协议系列

2.1 不同的协议

RDP, Vmware, Citrix, Spice

型号	具体信息	协议
RDP	微软远程桌面协议,非虚拟化,终端登录后,是共享服务器(主机)的硬件和软件	RDP
Vmware	Vmware 的远程连接模式,虚拟化架构,终端登录后,获得独立的虚拟机;	PCOIP 或 RDP
Citrix	Citrix 公司的远程连接,虚拟化架构,终端登录后,得到一个单独的虚拟机;	ICA/HDX
Spice	视频效果比较好是远程连接,虚拟化架构,终端登录后,得到一个独立的虚拟机;	Spice

2.2 Vmware 连接问题

1) 连接提示 SSL 问题?

■ 服务器上没有启用 SSL 安全身份验证,并且在终端 vmware 客户端设置上关闭了 SSL 身份验证;

2) 登录后,无法修改分辨率?

■ 分辨率修改需要在终端本身的设置界面进行调整;

3) 不能记录?

■ Vmware 的 ARM 客户端目前不支持录制设备,所以录制是不可能的;

4) 使用 u 盘?

- u 盘和其他 USB 外设由服务器控制。终端连接到虚拟机后,可以选择需要重定向的 USB 设备;
- 如果需要限制使用 U 盘,请参考如下方法:

2.3 Citrix 连接问题

1) 输入的服务器 IP 地址无法连接到服务器?

■ 目前,所有的客户端都是通过浏览器地址登录的。常见的格式是:http:// server IP/Citrix/StoreWeb,这需 要咨询 Citrix 服务器的部署工程师;

■ 用户名需要是一个域名,而不是一个普通的名字。例如,如果 shareuser1 用户的域名是 share.com,那么登录 用户名是:shareuser1@share.com

2) 连接后, Windows 系统界面上没有 Citrix 工具栏?

■ 目前, FL600N的 citrix 客户端还没有 citrix 工具栏。FL200N的 citrix 客户端有一个 citrix 工具栏;

3) 登录后,无法修改分辨率?

■ 分辨率修改需要在终端本身的设置界面进行调整

4) 无法记录, 登录到虚拟机接口后, 记录设备不存在?

■ 此问题首先由客户端在 Windows 下登录,以查看是否存在相同的问题。如果是这样,您需要咨询 citrix 的部署 工程师。如果 Windows 下的客户端没有这个问题,检查 ARM 的声音设置,确保终端不是静音的;

5) ARM 终端是否可以直接输入服务器登录地址(不是网页登录方式)?

■ 目前 ARM 终端不支持客户端直接登录,需要先使用浏览器登录;

6) 使用 U 盘

- u 盘和其他 USB 外设由服务器控制;
- 如果需要限制使用 U 盘,请参考如下方法:

2.4 Spice 连接问题

- 1) 服务器无法连接?
- 检查 IP 设置,通过 ping 功能判断网络是否正常;
- 目前 ARM 端 spice 客户端只支持"IP+端口号"的连接方式

2.5 终端系统设置问题

1) 连接到主机后无法更改分辨率?

■ 分辨率修改需要修改终端本身的设置界面,连接到主机后无法修改,或者只能修改到终端自己设置的分辨率;

某些版本的 FL600N 可能是系统未集成的分辨率修改补丁。您可以咨询制造商获得分辨率修改后的补丁文件。更新补丁后,可以通过终端设置界面修改分辨率;

2) 在扩展模式下,双屏幕连接如何显示不同的协议?

■ 首先,将显示模式更改为扩展模式。然后更改需要连接到不同显示接口的两个协议(一个设置为 VGA 显示,另一 个设置为 HDMI 显示)。

确定主显示器当前处于哪个显示接口。如果是在 VGA 上,首先连接 HDMI 显示协议,反之亦然;

2.6 其他连接问题

1) 有支持华为虚拟化平台的终端吗?

■ 目前, ARM 终端还没有集成华为的虚拟化客户端;

2) 是否有办法支持其他客户?

■ 如果有其他客户端软件 ARM 架构的源代码,可以提供给我们尝试集成到 ARM 终端;

3. 定制系统系列

自定义系统是指客户对我们提供的底层系统进行自定义。我们完成的系统(RDP 或四协议版本)是我们自己的系统,无法提供给客户修改。我们能提供给客户的是基于 arm 的 android 和 ubuntu;

3.1 所有的机型都支持 android 和 ubuntu

型号	Ubuntu 版本	安卓版本	注
FL120	不支持	不支持	
FL200N	1604	7.1	它需要 2g 的内存和 16g 的硬盘
FL200M	1604	7.1	它需要 2g 的内存和 16g 的硬盘
FL300	不支持	不支持	
FL600W	不支持	不支持	
FL600N	1404	4.4	
FL700N	1604 或 debian9	5.0	安卓系统推荐 2GB 内存
FL800N	1604	7.1	安卓系统推荐 2GB 内存

3.2 Ubuntu 系列

- 1) 哪些型号支持 ubuntu?
- FL600W、FL600N、FL700 (RK3288)、FL200N
- 2) 提供 ubuntu 固件的目的?

■ 提供给客户的 ubuntu 系统用于调试软件。客户利用我们提供的 ubuntu 系统定制系统界面,添加功能(如添加 Spice 客户端、添加 vmware 客户端、添加客户指定的客户端软件等)。

3) ubuntu 如何支持它?

■ ubuntu 系统的软件支持需要没有 SDK 的研发协助。

3.3 Android 系列

1) 哪些型号支持 android?

■ FL600W、FL600N、FL700N (RK3288)

2) 提供 android 固件的目的?

■ 提供给客户的 android 系统用于调试软件。客户使用我们提供的 android 系统定制系统界面,添加功能(如添加 Spice 客户端、添加 vmware 客户端、添加客户指定的客户端软件等)。

3) 如何支持 android ?

■没有 SDK,建议贵司及时与我司技术团队进行技术交流。

4) android 支持 USB 摄像头吗?

■ FL600N 目前有一个支持摄像头的 android 版本:fl600n1_andriod4.4.2_usbcam_20180705;新版本包括对摄像头的支持;

4. 各机型特性

ARM 系列包括 FL100, FL120, FL200N, FL300, FL600W, FL600N, FL600M; FL700N;

4.1 每种终端支持的软件列表

型号	软件1	软件2	软件3	多协议	
FL120	终端管理软			不支持	
	件				
FL200M/FL200N	VDclass 教	VDplayer	TCM 批量组态软件	不支持	
	学软件				
FL300	终端服务器	Shineplayer		不支持	
FL600w	终端管理软			不支持	
	件				
FL600N/FL600M	终端管理软	Shareplayer		Brush	multiple
	件			protocol	firmware
FL700N	N/A			Brush	multiple
				protocol	firmware

FL800N N/A	不支持
软件的名称	效果
终端管理软件	终端管理,用户管理,屏幕播放(FL120, FL600W 不支持屏幕播放)等;
TCM 批量组态软件	修改终端参数,如分辨率、远程控制等功能;
VDclass 教学软件	适用于 RDP 桌面教学软件,可实现学生演示、屏幕静音等功能;
VDP1ayer	FL200M 专用视频播放器, FL200M 可使用该播放器流畅播放 1080P 以下视
	频;
SharePlayer	FL600N 专用视频播放器, FL600N 可使用此播放器流畅播放 1080P 以下的
	视频;
终端服务器	安装在主机上的 FL300 专用服务组件使 FL300 能够找到服务器;
ShinePlayer	FL300 专用视频播放器, FL300 可以使用此播放器顺利播放以下 1080P 视
	频;

4.2 每种类型的硬件和软件信息

型号	CPU	内存/硬盘	网络	RDP 版本	的特点
FL120/FL120N	AllWin A20 双核 1.2GHz	512MB/4GB	100mbps	RDP8.1	支持管理软件管理
FL200M/FL200N	中兴微 A53 四核 2.0GHz	512MB/4GB	1000mbps	RDP8.1	批量配置:批量修改解决方案
					等.;
					特殊播放器:播放本地视频流
					畅;
					教学软件:免费教学软件;
FL300	Amlogic A9 双核 1.5GHz	512MB/4GB	100mbps	RDP7.1	专用的播放器;
FL600w	RK3188 A9 四核 1.6GHz	1GB/8GB	100mbps	RDP8.1	支持管理软件管理;
FL600N	RK3188 A9 四核 1.6GHz	1GB/8GB	100mbps	RDP8.1	管理软件:终端管理、监控等
	20				特殊播放器:播放本地视频流
					畅
					教学软件:免费教学软件;
FL600M	RK3188 A9 四核 1.6GHz	1GB/8GB	100mbps	RDP8.1	管理软件:终端管理、监控等
					特殊播放器:播放本地视频流
					畅
					教学软件:免费教学软件;
FL700N	RK3288 A17 四核 1.8GHz	1GB/8GB	1000mbps	RDP8.1	多协议
FL800N	RK3328 A53 四核 1.5GHz	1GB/8GB	1000mbps	RDP8.1	支持管理软件管理

说明:

1. FL120 管理软件不支持屏幕广播和远程引导,只支持用户管理、终端关机重启、终端监控;

2. RDP8.1 可以提高刷新率,防止幻灯片;

- 3. 特殊播放器采用终端硬件加速,可以播放存储在服务器上的视频;
- 4. VDclass 教学软件:免费教学软件,支持画面播放、学生演示、终端画面静音、远程监控、远程控制、全部或部分终端开放软件、终端断开连接、终端注销、终端重启等;(只适用于 FL200M)
- 5. TCM: ThinClient Manager,免费的终端批量组态软件,支持终端批量修改分辨率,批量开启和关闭 VNC 监控功能, 批量配置 wifi 连接信息,单次或批量重启关机终端等;(只适用于 FL200M)