**标准化实施指南 | 白皮书 | Citrix**



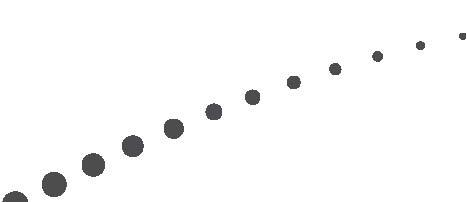
**PoC标准化实施指南**

**Citrix策略管理**

**常见外设和安全策略**

**版本：Draft**

www.citrix.com.cn



[第1章 基本概念 3](#_Toc107432105)

[第2章 HDX图形策略 3](#_Toc107432106)

[第3章 USB磁盘映射 10](#_Toc107432107)

[第4章 USB外设映射 16](#_Toc107432108)

[第5章 场景分类说明USB设备使用 21](#_Toc107432109)

[第6章 复制/粘贴剪贴板策略设置 24](#_Toc107432110)

# 基本概念

策略是设置的集合，这些设置定义如何为一组用户、设备或连接类型管理会话、带宽和安全性。

可以为物理计算机和虚拟机或用户提供策略设置。可以向本地级别或 Active Directory 的安全组中的单个用户应用设置。配置定义具体的条件和规则。如果您未明确分配策略，设置将应用于所有连接。

位于组织单位 GPO 级别的策略设置在网络上具有最高优先级。域 GPO 级别的策略会覆盖站点组策略对象级别的策略。站点组策略对象级别会覆盖 Microsoft 和 Citrix 本地策略级别上存在冲突的所有策略。

所有 Citrix 本地策略都在 Citrix Studio 控制台中创建和管理，并存储在站点数据库中。组策略使用 Microsoft 组策略管理控制台 (GPMC) 创建和管理，并存储在 Active Directory 中。Microsoft 本地策略在 Windows 操作系统中创建，存储在注册表中。

设置根据优先级及其条件合并。任何禁用设置都会覆盖等级较低的启用设置。未配置的策略设置会被忽略，且不会覆盖等级较低的设置。

本地策略也可能会与 Active Directory 中的组策略冲突，在这种情况下，二者可能会根据具体情况相互覆盖。

所有策略按照以下顺序处理：

1. 最终用户使用域凭据登录计算机。
2. 凭据被发送到域控制器。
3. Active Directory 应用所有策略（最终用户、端点、组织单位和域）。
4. 最终用户登录 Citrix Workspace 应用程序并访问应用程序或桌面。
5. 为最终用户和托管资源的计算机处理 Citrix 和 Microsoft 策略。
6. Active Directory 确定策略设置的优先级。之后将其应用于端点设备的注册表和托管资源的计算机。
7. 最终用户从资源注销。最终用户和端点设备的 Citrix 策略不再起作用。
8. 最终用户注销用户设备，从而释放 GPO 用户策略。
9. 最终用户关闭设备，从而释放 GPO 计算机策略。

**注意：不支持在同一个 GPO 中混合使用 Windows 策略和 Citrix 策略。**

# HDX图形策略

HDX 图形模式，一般来说有如下三种模式：

* JPEG
* 屏幕内容使用JPEG编码（文本除外，是RLE ）
* 选择性 H.264 / H.265
* 移动图像使用H.264 / H.265编码
* 其余屏幕内容将使用JPEG编码（文本除外，是RLE ）
* 全屏 H.264 / H.265
* 整个屏幕内容使用H.264 / H.265编码（文本除外，是RLE ）
* 在这种情况下， “针对3D图形工作负载优化”启用，这样文本也是用H.264 / H.265编码

Thinwire 在配置“使用视频编解码器进行压缩”策略不同值时使用了不同的技术，如下所示：

策略为**不使用视频编解码器(Do not use the video codec)**

* 文字：RLE
* 简单的图像和纯色：RLE
* 静态图像：JPEG
* 动态图像：自适应 JPEG

策略为**视频编解码器针对主动变化的区域(For actively changing regions)**

* 文字：RLE
* 简单的图像和纯色：RLE
* 静态图像：JPEG
* 动态图像：H.264 / H.265

策略为**针对整个屏幕(For the entire screen)**

* 文本：RLE（或 H.264 / H.265，如果已启用优化 3D 图形工作负载）
* 简单图像和纯色：H.264 / H.265
* 静态图像：H.264 / H.265
* 动态图像：H.264 / H.265

“使用视频编解码器进行压缩”策略默认值为**偏好时使用(Use when preferred)**，系统会自动为当前场景选择设置。

图形用户界面, 文本, 应用程序

描述已自动生成

在大多数情况下，“一刀切”的方法不是最好的选择，而应该针对不同场景进行不同的设置。所以，首先要确认的是：“有什么挑战和场景？是否有任何密集图形的工作，需要满足的多媒体要求是什么？用户的网络连接情况如何？”

在大多数情况下，将 Thinwire 配置为使用视频编解码器来针对主动变化的区域是最佳选择。通常，请避免配置使用视频编解码器进行压缩策略为“**偏好时使用**”，因为此设置可能会产生不同的效果，这具体取决于运行的操作系统、硬件和 VDA 版本的类型。还要避免配置任何链接到**旧图形模式**的 Citrix 策略。这些设置仅在 Windows Server 2008 R2 和 Windows 7 上受支持，出于兼容性原因而保留。

我们为以下几个通用场景创建了一些建议的配置。

**场景一：**

|  |  |
| --- | --- |
| **低带宽：**具有严重带宽限制的连接使用场景 | |
| **策略** | **配置** |
| 使用视频编解码器进行压缩  Use Video Codec for Compression | 不使用视频编解码器  Do not use video codec |
| 视觉质量  Visual Quality | 低  Low |
| 简单图形的首选颜色深度  Preferred color depth for simple graphics | 8 位/16 位  8 bit / 16 bit |
| 额外颜色压缩  Extra Color Compression | 启用  Enabled |
| 目标帧速率  Target Frame Rate | 15 |
| 目标最低帧速率  Target minimum frame rate | 10 |
| 移动图像压缩  Moving Image Compression | 启用  Enabled |
| HDX 自适应传输  HDX Adaptive Transport | 首选  Preferred |

说明：即使使用低带宽连接，通常也不会将颜色深度设置为 8 位，而是将其保持在 16 位。虽然 8 位可以显着降低带宽要求，但它也带来了显着降低的用户体验。因此，仅在最极端情况下才建议使用 8 位。

**场景二：**

|  |  |
| --- | --- |
| **呼叫中心/销售网点：**没有特殊多媒体要求的呼叫中心或销售网点场景，目标是在用户体验和用户密度之间找到一个很好的平衡 | |
| **策略** | **配置** |
| 使用视频编解码器进行压缩  Use Video Codec for Compression | 不使用视频编解码器  Do not use video codec |
| 视觉质量  Visual Quality | 中  Medium |
| 简单图形的首选颜色深度  Preferred color depth for simple graphics | 24 位  24 bit |
| 额外颜色压缩  Extra Color Compression | 禁用  Disabled |
| 目标帧速率  Target minimum frame rate | 20 |
| 目标最低帧速率  Target minimum frame rate | 10 |
| 移动图像压缩  Moving Image Compression | 启用  Enabled |
| HDX 自适应传输  HDX Adaptive Transport | 首选  Preferred |

**场景三：**

|  |  |
| --- | --- |
| **任务类型工作：**在任务类型工作的场景中，除了使用基本的办公应用程序外，用户还有一些多媒体需求，例如在线观看视频 | |
| **策略** | **配置** |
| 使用视频编解码器进行压缩  Use Video Codec for Compression | 针对主动变化的区域  For actively changing regions |
| 视觉质量  Visual Quality | 中  Medium |
| 简单图形的首选颜色深度  Preferred color depth for simple graphics | 24 位  24 bit |
| 额外颜色压缩  Extra Color Compression | 禁用  Disabled |
| 目标帧速率  Target minimum frame rate | 30 |
| 目标最低帧速率  Target minimum frame rate | 10 |
| 移动图像压缩  Moving Image Compression | 启用  Enabled |
| HDX 自适应传输  HDX Adaptive Transport | 首选  Preferred |
| 图形硬件加速（此为Citrix Workspace App配置） | 启用 |

在Windows客户端对于Citrix Workspace App配置，参考如下操作步骤：

|  |  |
| --- | --- |
| 步骤 | 操作 |
| 1 | 在Citrix Workspace App安装路径下，复制组策略模板文件CitrixBase.admx和receiver.admx，通常在C:\Program Files (x86)\Citrix\ICA Client\Configuration目录下，拷贝到C:\Windows\PolicyDefinitions目录下。 |
| 2 | 在Citrix Workspace App安装路径下，复制组策略模板文件CitrixBase.admx和receiver.admx，通常在C:\Program Files (x86)\Citrix\ICA Client\Configuration\zh-CN目录下，拷贝到C:\Windows\PolicyDefinitions\zh-CN目录下。 |
| 3 | 运行gpedit.msc打开本地组策略编辑器，选择计算机配置->管理模板->Citrix组件->Citrix Workspace->用户体验。 |
| 4 | 编辑图形硬件加速，配置为已启用。 |

**场景四：**

|  |  |
| --- | --- |
| **3D 工作负载** | |
| **策略** | **配置** |
| 使用视频编解码器进行压缩  Use Video Codec for Compression | 针对主动变化的区域  For actively changing regions |
| 使用视频编解码器的硬件编码  Use hardware encoding for video codec | 启用  Enabled |
| 视觉质量  Visual Quality | 无损构建  Build to lossless |
| 目标帧速率  Target minimum frame rate | 30/60 |
| 目标最低帧速率  Target minimum frame rate | 10 |
| 移动图像压缩  Moving Image Compression | 启用  Enabled |
| HDX 自适应传输  HDX Adaptive Transport | 首选  Preferred |
| 图形硬件加速（此为Citrix Workspace App配置） | 启用 |
| 图形的H265解码（此为Citrix Workspace App配置） | 启用 |

在Windows客户端对于Citrix Workspace App配置，参考如下操作步骤：

|  |  |
| --- | --- |
| 步骤 | 操作 |
| 1 | 在Citrix Workspace App安装路径下，复制组策略模板文件CitrixBase.admx和receiver.admx，通常在C:\Program Files (x86)\Citrix\ICA Client\Configuration目录下，拷贝到C:\Windows\PolicyDefinitions目录下。 |
| 2 | 在Citrix Workspace App安装路径下，复制组策略模板文件CitrixBase.admx和receiver.admx，通常在C:\Program Files (x86)\Citrix\ICA Client\Configuration\zh-CN目录下，拷贝到C:\Windows\PolicyDefinitions\zh-CN目录下。 |
| 3 | 运行gpedit.msc打开本地组策略编辑器，选择计算机配置->管理模板->Citrix组件->Citrix Workspace->用户体验。  图形用户界面, 表格  描述已自动生成 |
| 4 | 编辑图形硬件加速，配置为已启用。  图形用户界面, 文本, 应用程序  描述已自动生成 |
| 5 | 编辑图形的H265解码，配置为已启用。 |

基于上述四种场景，还有两条可选策略，可根据实际情况选择配置。

1. 拖动时查看窗口内容  
   图形用户界面, 文本

   描述已自动生成
2. 菜单动画  
   图形用户界面, 文本, 应用程序

   描述已自动生成

这两个策略默认都是允许，通常情况下选择配置为禁止。

# USB磁盘映射

对于USB磁盘映射，有两种方式，默认使用HDX优化模式，USB磁盘上的数据会以优化模式实现更好的传输性能。当然，也可以切换到通用USB设备映射模式。这个模式通常为了解决大于4GB的文件传输和USB磁盘使用加密信息的问题，例如某些加密USB磁盘在使用时会检查USB设备上的加密信息，而该信息必须通过USB总线通信完成。

要进行USB磁盘映射，可以参考如下步骤。

|  |  |
| --- | --- |
| 步骤 | 操作 |
| 1 | 启用可移动驱动器重定向策略  默认情况下，该策略是允许客户端访问可移动驱动器的。用户连接到VDA时，会提示是否允许访问客户端本地的驱动器，是只读还是可写。  首先，打开“Citrix Studio”，在左边控制台树，点击“策略”。在右边点击“创建策略”，创建一条新的策略。    要启用USB磁盘重定向，需要首先启用“客户端驱动器重定向”策略。该策略是USB磁盘，也就是移动驱动器的依存策略。只有允许该策略，才能够允许移动驱动器重定向策略。    点击“选择”链接，确认允许客户端驱动器重定向。    接下来需要配置客户端移动驱动器重定向。    点击“选择”链接，编辑设置。    系统默认允许客户端移动驱动器重定向，检查确认即可。  为了让终端用户每次登录时自动连接客户端移动驱动器，可以配置“自动连接客户端驱动器”策略。    默认为允许，检查配置。和客户端驱动器重定向策略一样，该策略除了移动驱动器之外，也对客户端软盘驱动器、客户端光驱、客户端硬盘、客户端移动磁盘、客户端网络盘生效。 |
| 2 | 指定策略应用对象。  除了类似AD活动目录组策略，Citrix的策略在支持组织单元（OU）为应用对象之外，还支持很多其他类型的用户和计算机对象区分。 |
| 3 | 如果想实现数据单向传输（数据只允许上传不允许下载）,可开启如下策略：  找到“只读客户端驱动器访问模式”,该策略默认为禁用，我们需要设置为启用。点击选择，编辑设置    应用了该策略的对象，可以实现数据只能上传不能下载。 |
| ~~4~~ | 特殊USB驱动器重定向。  如前所述，有时需要把USB磁盘映射成一个USB设备，以实现特殊的目的。这时可以选择设置“客户端USB设备优化规则”    这里以特定U盘为例，使得连接时使用通用USB设备方式重定向该U盘。 |

# USB外设映射

前文介绍了USB映射有两种方式，通用USB设备和具有单独逻辑通道的USB设备。除了USB磁盘，在“基本概念”一节我们介绍过还有很多其他使用USB接口和总线，但是能够使用ICA特定逻辑通道重定向的设备，例如摄像头、扫描仪（TWAIN）、智能卡、打印机、USB声卡等等，因此，对于这些设备通常使用对应的ICA通道策略进行配置：





而对于非单独逻辑通道设备，往往需要使用通用USB设备重定向。使用通用USB设备重定向时，如果设备类型未能自动映射，则需要进行手动配置USB重定向策略。

|  |  |
| --- | --- |
| 序号 | 步骤 |
| 1 | 获取设备的VID、PID等信息。  按照“基本概念”一章描述，在接入USB设备的PC或终端上，查看设备管理器中对应的设备属性，记录其VID、PID等信息。  获取USB设备的驱动程序，确认USB设备在PC或终端上能够正常使用。 |
| 2 | 为了启用通用USB设备的重定向，需要配置“USB设备”策略。    为了重定向USB设备，首先需要配置允许“客户端USB设备重定向”    如果是摄像头等即插即用设备，可启用“客户端USB即插即用设备重定向”。  如前一章介绍，可以使用“客户端USB设备优化规则”策略，设置USB设备是否使用设备优化规则。 |
| 3 | 出于设备类型考虑，有些设备默认是不进行重定向的。同理，也有一些设备我们需要禁止通过ICA协议映射到虚拟桌面或虚拟应用，因此，可以对重定向规则进行配置，指定允许和禁止的USB设备。  默认的允许禁止策略为：  DENY: class=09 # Hub devices  DENY: class=03 subclass=01 # HID Boot device (keyboards and mice)  DENY: class=0b # Smartcard  DENY: class=e0 # Wireless Controllers  DENY: class=02 # Communications and CDC Control  DENY: class=0a # CDC Data  ALLOW: # Ultimate fallback: allow everything else  策略逐条进行比对匹配，要禁用所有USB设备，可使用未附带任何其他标记的”DENY:”。  1、可使用策略配置规则：    点击“添加”，填入类似以下内容：  Allow: VID=XXXX PID=XXXX # XXXX是ID，这里写注释  2、也可直接修改注册表  HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\<userID>\User\VCPolicies  修改注册表可能导致系统异常，同时也不如组策略灵活 |
| 4 | 配置Receiver端USB允许禁止规则  可修改Receiver端注册表来调整USB允许禁止策略  HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB\DeviceRules  或  HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\DeviceRules    按照前节格式，编辑注册表键值即可。 |
| 5 | 如果未启用优化规则策略，特定设备重定向可能需要将其切换到通用模式。  对于很多USB Key类外设，其VID/PID往往显示为HID设备，默认是不会进行重定向的，需要启用USB重定向允许策略，强制其进行重定向。    USB Key如果被识别为智能卡，但又不想按照默认智能卡方式进行映射，除了使用通用USB重定向策略之外，还需禁止智能卡的自动系统挂钩。修改如下注册表项：  32-bit and 64-bit systems:  HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\AppInit\_Dlls\Smart Card Hook  64-bit systems:  HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\AppInit\_Dlls\Smart Card Hook |
| 6 | 设备自动重定向  用户可以自行勾选自动映射选项    Receiver端的配置可以使用icaclient\_usb.adm(.ADMX/.ADML)组策略模板。如果客户端支持组策略，可以使用模板配置自动映射策略    如果设备使用虚拟通道，可以修改注册表：  HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB\Devices  或  HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB\Devices  直接制定特定类型的设备进行重定向 |
| 7. | 如果想实现数据单向传输（数据只允许上传不允许下载）,可开启如下策略：  找到“只读客户端驱动器访问模式”,该策略默认为禁用，我们需要设置为启用。点击选择，编辑设置    应用了该策略的对象，可以实现数据只能上传不能下载。 |

# 场景分类说明USB设备使用

在“USB 普通重定向”策略启用的情况下，我们可以通过“客户端 USB 设备重定向规则” 策略来控制允许或者禁止某些\某类设备走普通 USB 重定向通道。“客户端 USB 设备重定 向规则”只会控制 USB 通道设备的行为，不影响其他优化通道（音频等）工作。

**场景一：**

例如，用户有很多种类的 USB 耳机，品牌也不一致，同时又需要使用 U 盘等大容量存储。

对于耳机希望走音频优化通道，U 盘类大容量存储希望走 普通USB 通道，那么一个个去禁止耳机的 VID 工作量会很大。

由于一般大容量存储的 class 都是 08，所以我们可以借助“客户端 USB 设备重定向规则” 策略，只允许 class 08 走普通 USB 通道，那么其余的 USB 耳机则会去走优化通道。

图形用户界面, 文本, 应用程序

描述已自动生成

**场景二：**

用户有很多不同种类的 USB 设备，大部分都希望走普通 USB 重定向通道，偶尔会去使用一两个需要走其他优化通道的设备（如 USB 耳机），那么建议有针对性的设置禁止 VID 的规则。这样只有被禁止的设备，VDA 才不允许其走普通 USB 重定向通道。

图形用户界面, 文本, 应用程序

描述已自动生成

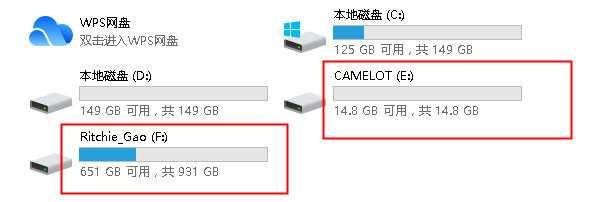
**场景三：**

从用户需求角度出发，当用户希望U盘可以在本地计算机和虚拟桌面中共享使用时，则需要该U盘设备走CDM磁盘优化通道。反之，则配置走普通USB重定向通道。

如果 U 盘显示位于 xxx，说明 U 盘这时走的是 CDM 磁盘优化通道，而不是 USB 重定向。

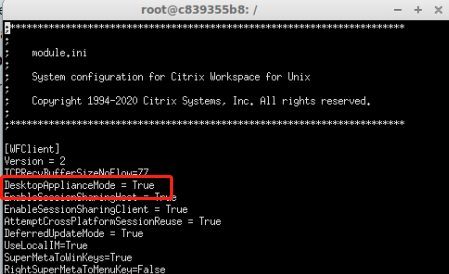


如果 U 盘直接显示名字，说明 USB 重定向成功，此时设备管理器可以看到此 U 盘设备。



对于一些瘦客户机来说，如果希望U盘这类 USB 设备从客户端接入之后就走默认的USB 重定向通道，那么需要客户端额外配置如下键值：

/opt/Citrix/ICAClient/config/module.ini --> WfClient --> DesktopApplianceMode = true



# 复制/粘贴剪贴板策略设置

用户连接Citrix桌面后，可以调用本地的剪贴板，快速完成文本内容的复制粘贴。

要进行剪贴板映射，可以参考如下步骤。

|  |  |
| --- | --- |
| 步骤 | 操作 |
| 1 | 启用剪贴板重定向策略  默认情况下，该策略是允许客户端使用剪贴板的。用户连接到VDA时，可在本地客户端和虚拟桌面之间互相剪贴文本内容。  首先，打开“Citrix Studio”，在左边控制台树，点击“策略”。在右边点击“创建策略”，创建一条新的策略。找到“客户端剪贴板重定向”，点击“选择”链接，编辑设置。    点击“选择”链接，编辑设置。    系统默认允许剪贴板重定向，检查确认即可。 |
| 3 | 如果想实现数据单向传输（数据只能从本地剪切至虚拟桌面）,在开启剪贴板重定向基础上，还需要开启“限制客户端剪贴板写入”策略：  找到“限制客户端剪贴板写入”,该策略默认为禁用，我们需要设置为启用  点击选择，编辑设置    设置为启用    应用了该策略的对象，可以实现剪贴板内容只能上传不能下载。 |