WorkSpace configures the desktop authorization policy to disable the USB function, but the terminal desktop can still use USB

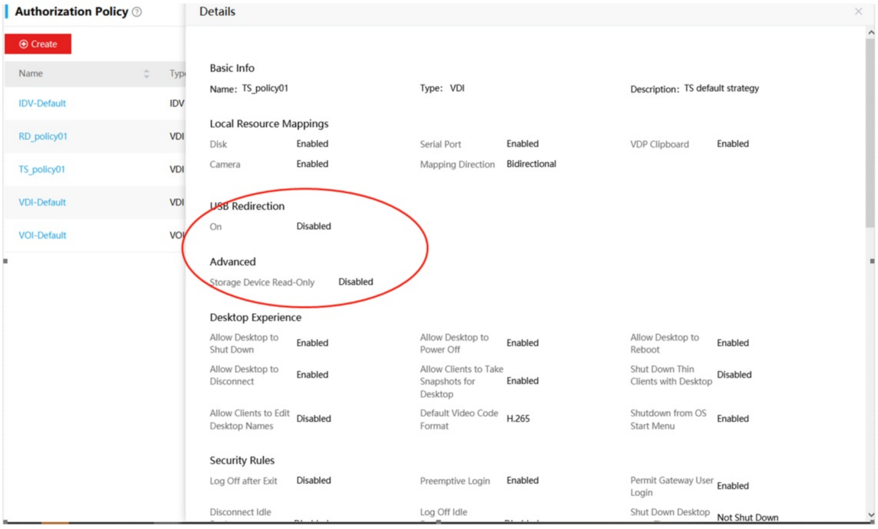
Cloud Computing 徐帅 2021-05-25 Published

Network Topology

none

Problem Description

WorkSpace needs to disable the USB function of the terminal desktop and set an authorization policy to disable USB redirection, but the terminal can still use the U disk to copy files after logging in to the desktop. As shown below:



Name	Type
IDV-Default	IDV
RD_policy01	VDI
TS_policy01	VDI
VDI-Default	VDI
VOI-Default	VOI

Basic Info

Name: TS_policy01 Type: VDI Description: TS default strategy

Local Resource Mappings

Disk	Enabled	Serial Port	Enabled	VDP Clipboard	Enabled
Camera	Enabled	Mapping Direction	Bidirectional		

USB Redirection

On	Disabled

Advanced

Storage Device Read-Only	Disabled

Desktop Experience

Allow Desktop to Shut Down	Enabled	Allow Desktop to Power Off	Enabled	Allow Desktop to Reboot	Enabled
Allow Desktop to Disconnect	Enabled	Allow Clients to Take Snapshots for Desktop	Enabled	Shut Down Thin Clients with Desktop	Disabled
Allow Clients to Edit Desktop Names	Disabled	Default Video Code Format	H.265	Shutdown from OS Start Menu	Enabled

Security Rules

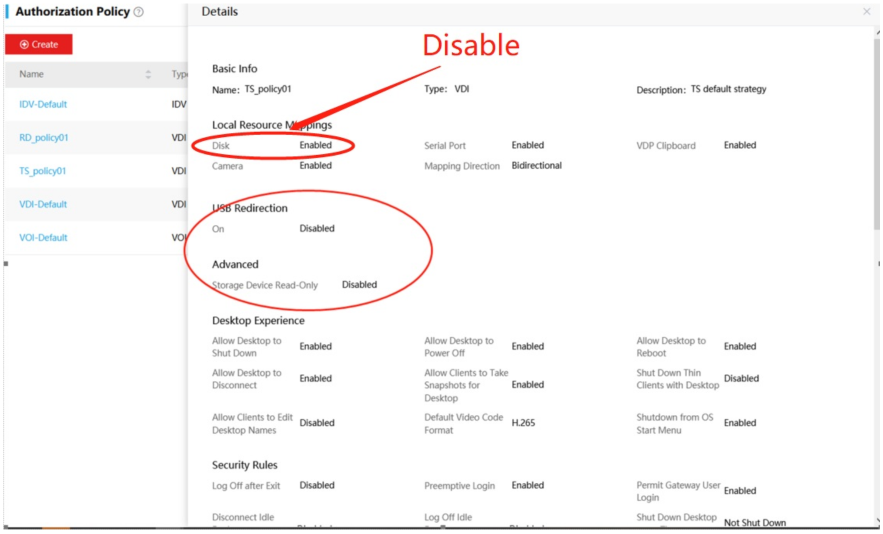
Log Off after Exit	Disabled	Preemptive Login	Enabled	Permit Gateway User Login	Enabled
Disconnect Idle		Log Off Idle		Shut Down Desktop	Not Shut Down

Process Analysis

In addition to USB, the terminal transferring files to the desktop can also support local resource mapping to transfer files. When the USB redirection function is turned off, the U disk can still be mapped to the desktop by local resource mapping. Therefore, if you want to disable the USB function of the terminal desktop, you need to disable the disk in the local resource mapping, so that the U disk will not be mapped to the virtual machine desktop.

Solution

Disable the disk in the local resource mappings



Disable

Authorization Policy

⊕ Create

Name	Type
IDV-Default	IDV
RD_policy01	VDI
TS_policy01	VDI
VDI-Default	VDI
VOI-Default	VOI

Details

Basic Info

Name: TS_policy01 Type: VDI Description: TS default strategy

Local Resource Mappings

Disk	Enabled	Serial Port	Enabled	VDP Clipboard	Enabled
Camera	Enabled	Mapping Direction	Bidirectional		

USB Redirection

On	Disabled

Advanced

Storage Device Read-Only	Disabled

Desktop Experience

Allow Desktop to Shut Down	Enabled	Allow Desktop to Power Off	Enabled	Allow Desktop to Reboot	Enabled
Allow Desktop to Disconnect	Enabled	Allow Clients to Take Snapshots for Desktop	Enabled	Shut Down Thin Clients with Desktop	Disabled
Allow Clients to Edit Desktop Names	Disabled	Default Video Code Format	H.265	Shutdown from OS Start Menu	Enabled

Security Rules

Log Off after Exit	Disabled	Preemptive Login	Enabled	Permit Gateway User Login	Enabled
Disconnect Idle		Log Off Idle		Shut Down Desktop	Not Shut Down