

知 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:

The screenshot displays the 'Authorization Policy' configuration interface. On the left, a list of policies is shown, including 'IDV-Default', 'RD_policy01', 'TS_policy01', 'VDI-Default', and 'VOI-Default'. The 'Details' pane for 'TS_policy01' is open, showing various settings. The 'USB Redirection' section is circled in red, with 'On' selected and 'Disabled' also visible. The 'Advanced' section shows 'Storage Device Read-Only' set to 'Disabled'. Other sections include 'Basic Info', 'Local Resource Mappings', 'Desktop Experience', and 'Security Rules'.

Section	Setting	Value
Basic Info	Name	TS_policy01
Basic Info	Type	VDI
Basic Info	Description	TS default strategy
Local Resource Mappings	Disk	Enabled
Local Resource Mappings	Serial Port	Enabled
Local Resource Mappings	Camera	Enabled
Local Resource Mappings	Mapping Direction	Bidirectional
Local Resource Mappings	VDP Clipboard	Enabled
USB Redirection	On	Selected
USB Redirection	Disabled	Available
Advanced	Storage Device Read-Only	Disabled
Desktop Experience	Allow Desktop to Shut Down	Enabled
Desktop Experience	Allow Desktop to Power Off	Enabled
Desktop Experience	Allow Desktop to Reboot	Enabled
Desktop Experience	Allow Desktop to Disconnect	Enabled
Desktop Experience	Allow Clients to Take Snapshots for Desktop	Enabled
Desktop Experience	Shut Down Thin Clients with Desktop	Disabled
Desktop Experience	Allow Clients to Edit Desktop Names	Disabled
Desktop Experience	Default Video Code Format	H.265
Desktop Experience	Shutdown from OS Start Menu	Enabled
Security Rules	Log Off after Exit	Disabled
Security Rules	Preemptive Login	Enabled
Security Rules	Permit Gateway User Login	Enabled
Security Rules	Disconnect Idle	Not Shut Down
Security Rules	Log Off Idle	Not Shut Down
Security Rules	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

The screenshot shows the 'Details' view of an Authorization Policy named 'TS_policy01'. The 'Local Resource Mappings' section is highlighted with a red circle, and the 'Disk' setting is set to 'Enabled'. A red arrow points from the word 'Disable' to the 'Disk' setting. Other settings in the 'Local Resource Mappings' section include 'Camera' (Enabled) and 'Mapping Direction' (Bidirectional). The 'USB Redirection' section shows 'On' set to 'Disabled'. The 'Advanced' section shows 'Storage Device Read-Only' set to 'Disabled'. The 'Desktop Experience' section includes settings for 'Allow Desktop to Shut Down' (Enabled), 'Allow Desktop to Disconnect' (Enabled), 'Allow Clients to Edit Desktop Names' (Disabled), 'Allow Desktop to Power Off' (Enabled), 'Allow Clients to Take Snapshots for Desktop' (Enabled), 'Default Video Code Format' (H.265), and 'Allow Desktop to Reboot' (Enabled). The 'Security Rules' section includes 'Log Off after Exit' (Disabled), 'Preemptive Login' (Enabled), and 'Permit Gateway User Login' (Enabled). The 'Shut Down Desktop' setting is set to 'Not Shut Down'.

Section	Setting	Value
Local Resource Mappings	Disk	Enabled
	Camera	Enabled
	Mapping Direction	Bidirectional
USB Redirection	On	Disabled
	Storage Device Read-Only	Disabled
Desktop Experience	Allow Desktop to Shut Down	Enabled
	Allow Desktop to Disconnect	Enabled
	Allow Clients to Edit Desktop Names	Disabled
	Allow Desktop to Power Off	Enabled
	Allow Clients to Take Snapshots for Desktop	Enabled
	Default Video Code Format	H.265
	Allow Desktop to Reboot	Enabled
Security Rules	Log Off after Exit	Disabled
	Preemptive Login	Enabled
	Permit Gateway User Login	Enabled
Shut Down Desktop	Not Shut Down	

