

FMC VDI Policies / Disabled Features

Article ID: KB0026570

Created: 2023-12-29 23:07:20

Updated: 2023-12-29 23:07:47

Author: {'link':

'https://fmcnaddev.service-now.com/api/now/table/sys_user/31a85ef41bb989501d67db1dcd4bcb92',

'value': '31a85ef41bb989501d67db1dcd4bcb92'}

Category: {'link':

'https://fmcnaddev.service-now.com/api/now/table/kb_category/e68729471bdbf9d0cfb6a756624bcb48',

'value': 'e68729471bdbf9d0cfb6a756624bcb48'}

Purpose:

Follow this to know more about the FMC VDI Policies

Details/Scenarios/Notes

The below mentioned are some FMC VDI Policies.

FMC VDI Policies

1.

Disabled Features

Access to USB devices (except mouse and keyboard)Audio/Video capability (ie. Teams, Zoom, etc.)Printing to local deviceAccess to user's local and network drives, for off-network/remote users

To join online meetings users should use their local workstation or phone.

2.

Retention Policy

Effective 11 April 2018

ECS Virtualization regularly monitors usage of VDI desktops, and we have observed many VDI desktops going unused. To efficiently manage resources, Virtualization will enact the following retention policy based on AD account status and the user's last VDI logon.

Account Status

Last Logon

Action

Enabled

Never

Delete VDI desktop* if user does not log into their

VDI desktop within 30 days from assignment

Enabled

>90 days

Delete VDI desktop*

Disabled

>30 days

Delete VDI desktop*

NOTE: This is a reminder that ECS Virtualization is NOT responsible for managing, or recovering, data on VDI desktops. As with physical laptops/desktops, it is the user's responsibility to ensure important data is routinely stored elsewhere, such as OneDrive or on a network folder.