KillDisk Wiping Process

Article ID: KB0026541
Created: 2023-07-19 20:21:00
Updated: 2023-07-19 20:22:40
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/234709da6fb2464070404a950d3ee44b', 'value': '234709da6fb2464070404a950d3ee44b'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/bf870a491bd7a51426ddeb16624bcb6d', 'value': 'bf870a491bd7a51426ddeb16624bcb6d'}

Title

KillDisk Wiping Process

Purpose:

Follow this procedure when a user requests KillDisk on a computer or laptop and needs to have information removed. This process needs to be completed before any pc is removed from a location.

Required Information to be documented in each Incident:

Contact NameContact NumberClinic / Facility NumberComputer Service Tag (one computer per incident)Detailed Description of the issue.Screen shot of the Error

Troubleshooting Process

1.

Confirm with user that the issue matches the issue reported.

2.

Please document required information and troubleshooting details in the incident.

3.

Please attach any referenced knowledge articles to the Incident.

4.

Provide the user with the incident number and refer the incident to the appropriate Field System Support Assignment Group per Operating Group. FSS Team will complete the remainder of the process.

5.

Confirm the Legal hold Check process has been performed and all legal hold data has been saved.

If not, please update the work notes and complete the Legal Hold Check process.

Legal Hold Status Check - Fresenius Medical Care (service-now.com)

6.

If the device is not encrypted and/or cannot be encrypted, the KillDisk application will need to be run on the device prior to removing it from the site. Copy KillDisk executable from FSS App share to down to the unencrypted computer.

7.

Double click the KillDisk icon to begin preparing the computer. Then setup files will be extracted.

8.

At the prompt, input 1 and enter to continue the process or 2 to exit the application.

9.

A prompt will appear asking for total amount of partitions found on Disk 0. Enter the count and press Enter to

continue.

10.

Auto play and SEP will see the new partition, close both popups and then you will be prompted to reboot the

computer now type Y/N and press enter.

11.

If Y is entered, a Windows notification will popup stating the computer will shut down. If N is entered the

application will close. ***Please NOTE: even if N is selected, the computer is ready for the next stage. The difference

is only an automatic reboot vs. a manual reboot***

12.

After reboot, the WinPE image will begin to load off the new partition and then a selection screen will appear.

This screen allows the customer to change the default time zone then click OK. If left alone the time zone will

default to Central and continue after 30 seconds.

13.

Once the Desktop loads, a network check will take place. If the computer is not on the network, a prompt will

appear notifying the customer to check cables and test again. This test will not close until a valid IP Address is

available.

14.

A VNC server will be enabled, and the following message will appear on the screen. Using a VNC viewer

application, connect to the IP that is provided by the customer. The VNC server password will be provided separately.

15.

Once the session has been established, press any key to continue.

16.

Follow the onscreen prompts and enter the computer user's employee ID and press enter. Next, for auditing

purposes, enter your employee ID and press enter.

17.

Confirm that the Legal Hold list has been checked. Next confirm that the user is not on Legal Hold.

18.

KillDisk will open and scan system for all attached drives, then begin the wiping process. Once the wipe begins

it cannot be stopped.

19.

Depending on the size of the hard drive, the wiping process can take several hours. Please remind the

customer that the computer must stay connected to the network the entire time it is wiping.

20.

Once the wipe is completed, the certificate will be displayed on the screen.

21.

Close the window and the KillDisk application. A prompt for saving the confirmation and logfile to the network

share will be up. Press any key to begin the copy process.

22.

Confirm on a separate computer that a folder with the confirmation certificate and logfile has been saved to the network share. \\corpfs01\businessunits\FSS\KillDisk Confirmations

23.

If the folder was not created, return to the wiped computer. Click on the Active Disk icon and navigate to

Utilities / Explore My Computer.

24.

Using the Boot Disk Explorer, navigate to the RAM disk X drive and copy the contents of the confirmation

folder to a USB drive or if an O: drive is mapped drag and drop the data.

25.

Final Step: A prompt will appear to turn off the computer. Have the customer press Turn Off. If restart is

selected, the computer will boot to a confirmation screen that a wipe was completed.

26.

Once wiping is complete, browse for the Wipe Certificate on the server \\corpfs01\businessunits\FSS \killDisk Confirmations

27.

Confirm the certificate has been saved. If it is not located on the server, upload it to the appropriate location.

28.

Notify the user that the process is complete and send information on returning/disposing of the device.

IT Equipment Returns KB0024543

29.

Please document the following information in a Work Note of the incident.

Legal hold/Killdisk process complete.

Return information provided to user.

30.

Follow the resolution process.

Incident Classification Requirements

Category

Inquiry/Help

Subcategory

Hardware

Resolution Process

Please review/update Classification and provide customer with the Incident number for their reference prior to resolving.

Incident Resolution Categorization

Resolution Code

Solved Remotely (Permanently)

Resolution Category

Inquiry/Help

Resolution Subcategory

Hardware

Resolution Service

KillDisk

Escalation Process

Please review/update Classification and provide customer with the Incident number for their reference prior to escalating

Escalation Group

DTI-EUX-FSS Ticket Allocation

Published by

DTI-EUX-FSS Ticket Allocation