

Account Lockout issues

Article ID: KB0024676

Created: 2023-12-29 23:19:34

Updated: 2023-12-29 23:19:55

Author: {'link':

'https://fmcnadev.service-now.com/api/now/table/sys_user/63b5575587723450e3f297d83cbb35b4',

'value': '63b5575587723450e3f297d83cbb35b4'}

Category: {'link':

'https://fmcnadev.service-now.com/api/now/table/kb_category/d48a0fb31be45150aa10dd36bc4bcbf9',

'value': 'd48a0fb31be45150aa10dd36bc4bcbf9'}

Account continuously locks – Network Account Lockouts

Actions for when a customer says they continuously get locked out of the account.

Tools

Active DirectoryAccount Lockout ToolUser Identity Management System (UIDMS)Daily Audit Report

\\adauditpd01\Locked User Reports\CORP.AD.FMCNA.COM

Drill down into the link for the HTML file that says “Recently_Locked_Out_Users.html”

Steps

Turn off the laptop/desktop and keep the device powered offWith the device powered off, unlock the account using the Account Lockout ToolWith the device powered off, refresh the Account Lockout Tool (press F5 to refresh)If the account continues to lockout when the device is still powered off, then there is another source of the locks.Open the Daily Audit Report \\adauditpd01\Locked User Reports\CORP.AD.FMCNA.COMSearch the list in the Audit Report and find the account that is lockingLook for Service Tags that have locked with the account name.If any Service Tag is listed other than the device that is still powered off, then that device listed will also need to be powered off.Use Bomgar if needed to turn off that 2nd device. You can Jump into the device with the service tag or the ip address (if shown) to power off the device or restart the device to log off the account that continues to lock. (typically, that 2nd device will have multiple users logged on)If the Daily Audit Report shows an item that is not a service tag the customer will need to turn off all smart phone or wireless devices.With the laptop/desktop and smart phone/wireless devices ALL powered off, refresh the Account Lockout tool.With all devices power off and after refreshing the account in the Lockout tool the locks should be stopped.If the locks have stopped, you can now turn on the 1st device (laptop/desktop from step 1)Have the customer log in the device and let the desktop icons load. Instruct the customer to wait and do not attempt to open any applications until you have refreshed the Lookout Tool for a few times to confirm the locks have stopped.If the locks have stopped then that will confirm the source was from the 2nd Service Tag or the wireless device.If the source is the wireless device, that device will need to Forget the Wi-Fi passwords for any Fresenius Network found in the Wi-Fi list.Account continuously locks – Network Account Lockouts

Actions for when a customer says they continuously get locked out of the account.

Tools

Active DirectoryAccount Lockout Tool

User Identity Management System (UIDMS)

Daily Audit Report

\\adauditpd01\Locked User Reports\CORP.AD.FMCNA.COM

Drill down into the link for the HTML file that says "Recently_Locked_Out_Users.html"

Steps

Turn off the laptop/desktop and keep the device powered off. With the device powered off, unlock the account using the Account Lockout Tool. With the device powered off, refresh the Account Lockout Tool (press F5 to refresh). If the account continues to lockout when the device is still powered off, then there is another source of the locks. Open the Daily Audit Report \\adauditpd01\Locked User Reports\CORP.AD.FMCNA.COM. Search the list in the Audit Report and find the account that is locking. Look for Service Tags that have locked with the account name. If any Service Tag is listed other than the device that is still powered off, then that device listed will also need to be powered off. Use Bomgar if needed to turn off that 2nd device. You can Jump into the device with the service tag or the ip address (if shown) to power off the device or restart the device to log off the account that continues to lock. (typically, that 2nd device will have multiple users logged on). If the Daily Audit Report shows an item that is not a service tag the customer will need to turn off all smart phone or wireless devices. With the laptop/desktop and smart phone/wireless devices ALL powered off, refresh the Account Lockout tool. With all devices power off and after refreshing the account in the Lockout tool the locks should be stopped. If the locks have stopped, you can now turn on the 1st device (laptop/desktop from step 1). Have the customer log in the device and let the desktop icons load. Instruct the customer to wait and do not attempt to open any applications until you have refreshed the Lookout Tool for a few times to confirm the locks have stopped. If the locks have stopped then that will confirm the source was from the 2nd Service Tag or the wireless device. If the source is the wireless device, that device will need to Forget the Wi-Fi passwords for any Fresenius Network found in the Wi-Fi list.