



How to Find the Source of Account Lockouts in Active Directory

by Robert Allen

Updated: June 27, 2020

Active Directory Domain Servers

In this post you will learn how to find the source of account lockouts in Active Directory.

I'll show you two methods, the first one uses PowerShell and the second is a GUI tool I created that makes it super easy to unlock user accounts and find the lockout source.

Users locking their accounts is a common problem, its own of the top calls to the helpdesk.

What is frustrating is when you unlock a users account and it keeps randomly locking. The user could be logged into multiple devices (phone, computer, application and so on) and when they change their password it will cause ongoing lock out issues.

This guide will help you to track down the source of those lockouts.

Check it out:

Video Tutorial

Find the Source of Account Lockouts in A...



If you don't like video tutorials or want more details, then continue reading the instructions below.

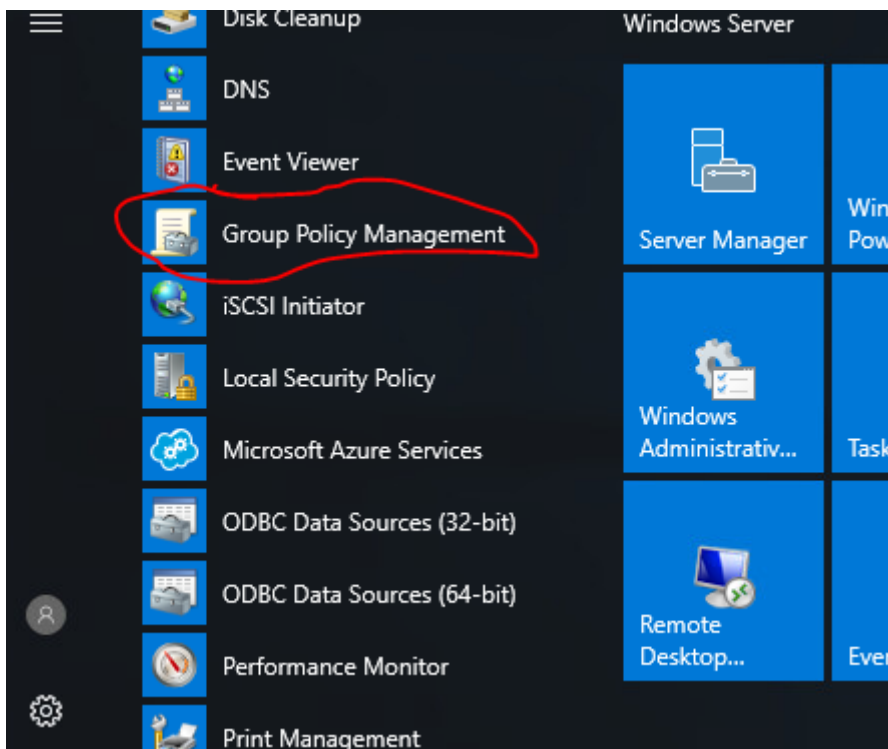
Method 1: Using PowerShell to Find the Source of Account Lockouts

Both the PowerShell and the GUI tool need auditing turned before the domain controllers will log any useful information.

Step 1: Enabling Auditing

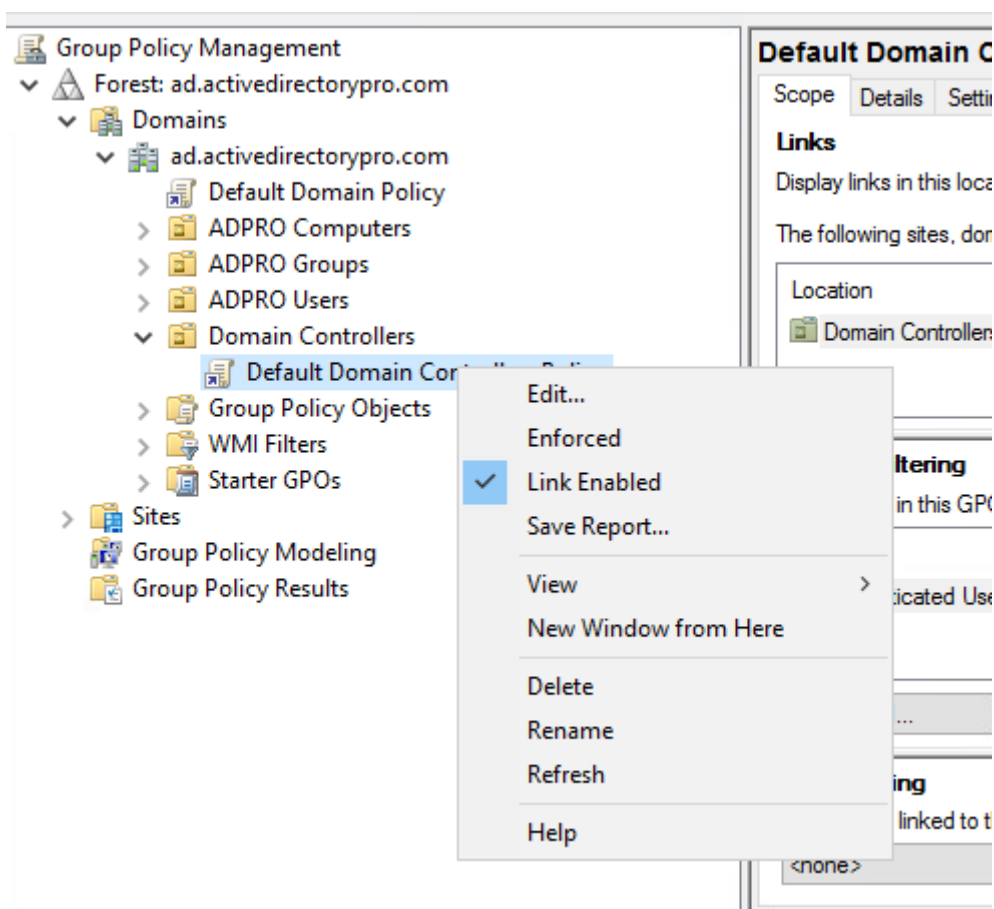
The event ID 4740 needs to be enabled so it gets locked anytime a user is locked out. This event ID will contain the source computer of the lockout.

1. Open the Group Policy Management console. This can be from the domain controller or any computer that has the RSAT tools installed.



2. Modify the Default Domain Controllers Policy

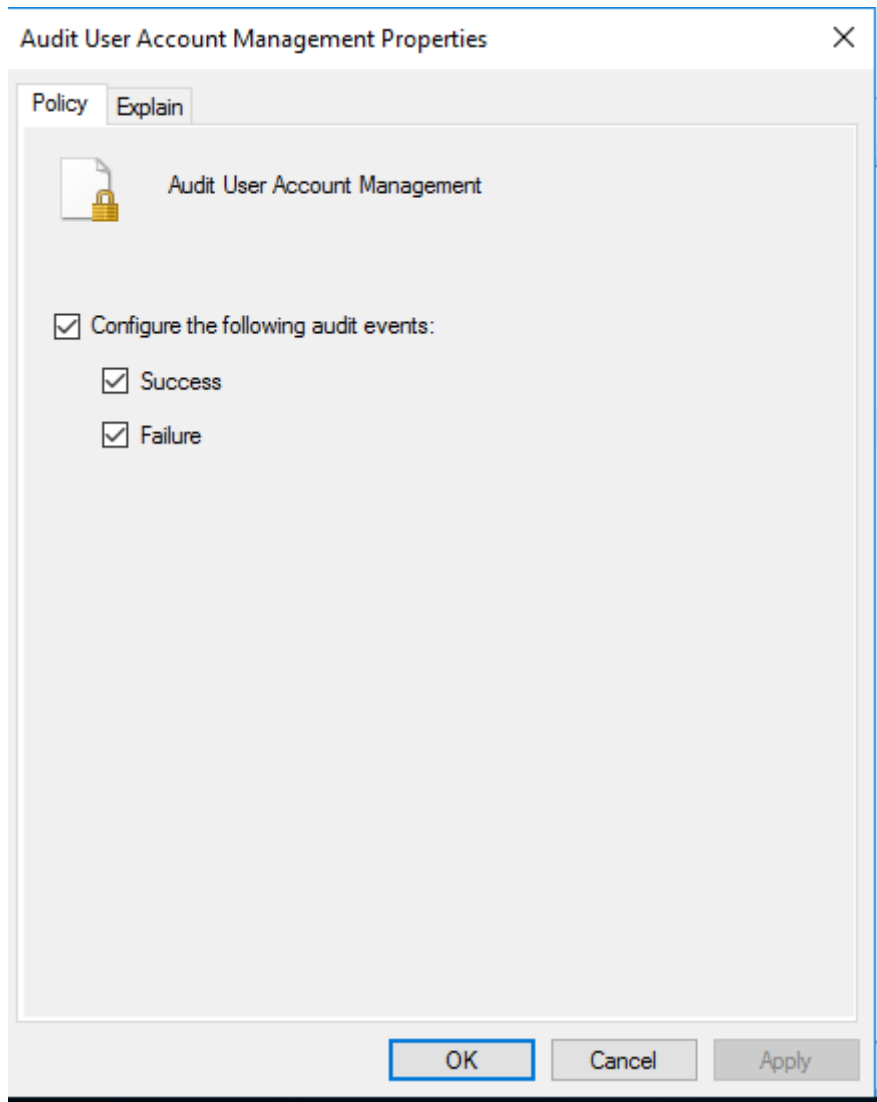
Browse to the Default Domain Controllers Policy, right click and select edit.



3. Modify the Advanced Audit Policy Configuration

Browse to computer configuration -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policies -> Account Management

Enable success and failure for the "Audit User Account Management" policy.



Auditing is now turned on and event 4740 will be logged in the security events logs when an account is locked out.

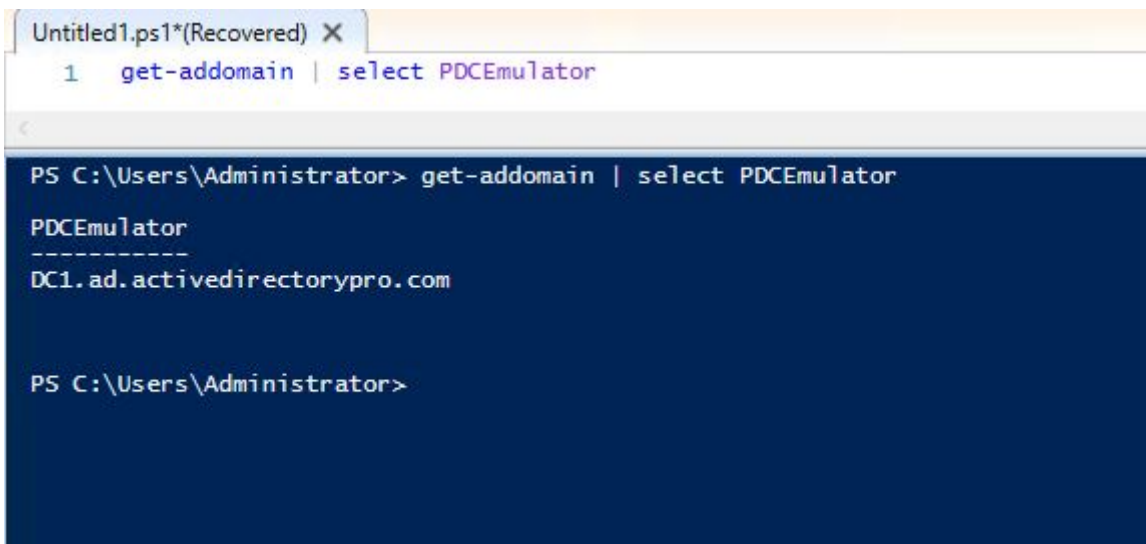
Step 2: Find the Domain Controller with the PDC Emulator Role

If you have a single domain controller (shame on you) then you can skip to the next step...hopefully you have at least two DCs.

The DC with the PDC emulator role will record every account lockout with an event ID of 4740.

To find the DC that has the PDCEmulator role run this PowerShell command

get-addomain | select PDCEmulator



```

Untitled1.ps1*(Recovered) X
1  get-addomain | select PDCEmulator

PS C:\Users\Administrator> get-addomain | select PDCEmulator

PDCEmulator
-----
DC1.ad.activedirectorypro.com

PS C:\Users\Administrator>
  
```

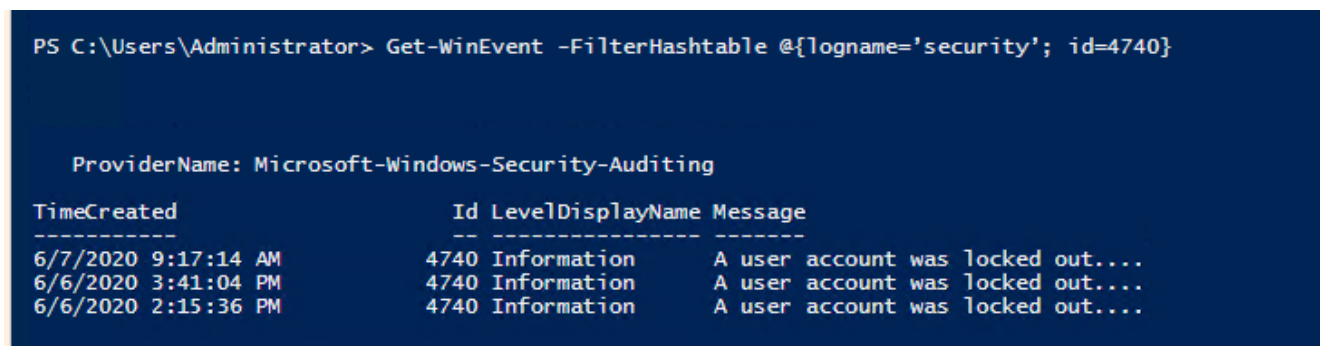
Step 3: Finding event ID 4740 using PowerShell

All of the details you need is in event 4740. Now that you know which DC holds the pdcemulator role you can filter the logs for this event.

On the DC holding the PDCEmulator role open PowerShell and run this command

```
Get-WinEvent -FilterHashtable @{logname='security'; id=4740}
```

This will search the security event logs for event ID 4740. If you have any account lockouts you should a list like below.



```

PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @{logname='security'; id=4740}

ProviderName: Microsoft-Windows-Security-Auditing

TimeCreated              Id LevelDisplayName Message
-----
6/7/2020 9:17:14 AM      4740 Information A user account was locked out....
6/6/2020 3:41:04 PM      4740 Information A user account was locked out....
6/6/2020 2:15:36 PM      4740 Information A user account was locked out....
  
```

To display the details of these events and get the source of the lockout use this command.

```
Get-WinEvent -FilterHashtable @{logname='security'; id=4740} | fl
```

```
PS C:\Users\Administrator> Get-WinEvent -FilterHashtable @{logname='security'; id=4740} | fl

TimeCreated      : 6/7/2020 9:17:14 AM
ProviderName     : Microsoft-Windows-Security-Auditing
Id               : 4740
Message          : A user account was locked out.

                Subject:
                Security ID:      S-1-5-18
                Account Name:     DC1$
                Account Domain:   adpro
                Logon ID:         0x3E7

                Account That Was Locked Out:
                Security ID:      S-1-5-21-1536893199-618012757-1031678021-1104
                Account Name:     test.user001

                Additional Information:
                Caller Computer Name:  PC1

TimeCreated      : 6/6/2020 3:41:04 PM
```

This will display the caller computer name of the lockout. This is the source of the user account lockout.

You can also open the event log and filter the events for 4740

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose ☐ Error ☐ Information

☒ By log Event logs: Security

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4740

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

That is it for method 1.

Although this method works it takes a few manual steps and can be time consuming. You may also have staff that is not familiar with PowerShell and need to perform other functions like unlock or reset the users account.

That is why I created the [Active Directory User Unlock GUI tool](#). This tool makes it super easy for staff to find all locked users and the source of account lockouts.

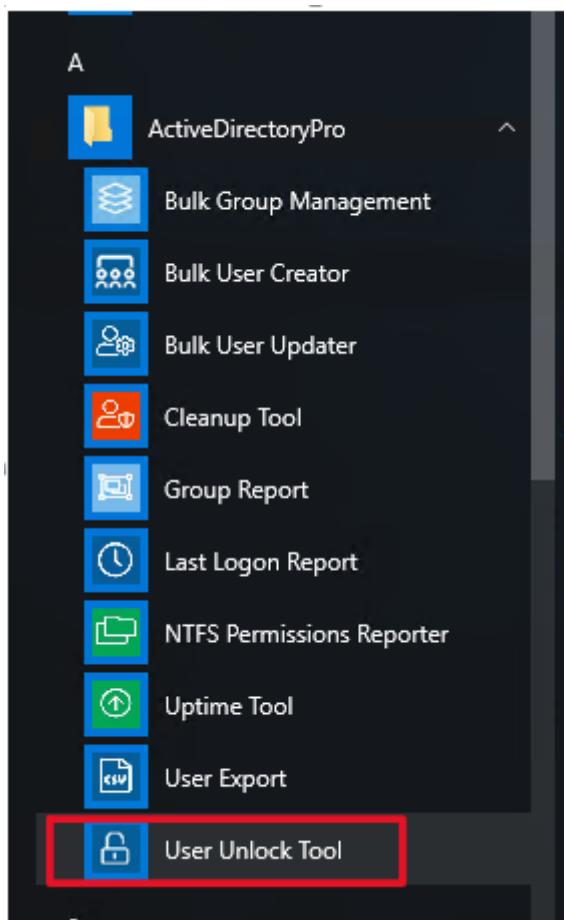
Check out the steps below for using the unlock gui tool.

Method 2: Using the User Unlock GUI Tool to Find the Source of Account Lockouts

I created this tool to make it super easy for any staff member to unlock accounts, reset passwords and find the source of account lockouts.

Just like PowerShell this tool requires the auditing be turned on for Account Management. See steps above for enabling these audit logs.

1. Open the User Unlock Tool



2. Click the Search Button, then click more details

That is all there is to it.

You will now see a list of times the account was locked out and the source computer.

In addition you can unlock the account and reset the password all from one tool. The tool will display all locked accounts, you can select a single account or multiple accounts to unlock.

The user unlock tool is included in my [AD Pro Toolkit bundle](#), this is a bundle of 10 tools to help simplify and automate routine AD tasks.

I hope you found this article useful. If you have questions or comments let me know by posting a comment below.

Recommended Tool: SolarWinds Server & Application Monitor

This utility was designed to [Monitor Active Directory](#) and other critical services like Azure, DNS, and DHCP. It will quickly spot domain controller issues, replication, performance issues with cloud services, failed logon attempts, and much more.

What I like best about this tool is it's easy to use interface and instant alerting features.

[Download your 30-day free trial](#)

8 thoughts on “How to Find the Source of Account Lockouts in Active Directory”

Jorge

December 1, 2020 at 10:52 am

Hi,

What about the events with an empty Caller machine and no IP information?
How could you track that issue?

Thank you.

[Reply](#)

Sean

January 18, 2021 at 2:22 pm

Yeah, I have an account with no caller computer name, how does that get tracked?

[Reply](#)

Amit

April 10, 2021 at 6:17 am

It could be non-windows device such as mobile device as AD can't read non-windows devices so need to ask user to clear cached credentials on his personal devices if he is using office/skype/email application on it

[Reply](#)

Mark

April 19, 2021 at 9:35 am

In real terms it is not unusual in some environments to see the event viewer on the dc contain an event with no originating source information, perhaps just saying "WORKSTATION". The best auditing tool in the world can't report on what is not logged. Leaves you with two choices, work with customer to consider any and all devices they could have cached profiles / creds on and eliminate one by one. (Also consider whether any of your services could have basic auth enabled as the cause could be a brute force password attempt from a malicious party, which is simpler with basic auth). OR go nuclear and enable netlogon debug logging. Not to be taken lightly and in the strongest possible terms DO NOT leave this on and walk away. As per MS guidance use at your own risk. "<https://docs.microsoft.com/en-us/troubleshoot/windows-client/windows-security/enable-debug-logging-netlogon-service>"

[Reply](#)

Robert Allen

April 24, 2021 at 1:41 pm

Good information. Thanks Mark

[Reply](#)

Muchtall

May 6, 2021 at 3:18 pm

Smartquotes: The bane of Sysadmins everywhere. Totally put a monkeywrench in the commands shown here. Thanks for the tips though! Very helpful!

[Reply](#)**Matthew McDonald**[July 9, 2021 at 7:14 pm](#)

I'm trying your GUI tool now... does it not just connect to the PDC? I'm showing it query every DC in my environment when I click More Details.

[Reply](#)**Robert Allen**[September 6, 2021 at 11:01 am](#)

Some information it pulls from the user account so it needs to connect to all domain controllers.

[Reply](#)

Leave a Comment

Tools

[AD Cleanup Tool](#)[Bulk import new users](#)[Export all users to CSV](#)[Get AD Users Last Logon Time](#)

Popular Articles

[PowerShell: Export Active Directory Group Members](#)[How To Configure a Domain Password Policy](#)[Create Bulk Users in Active Directory \(Step-By-Step Guide\)](#)[Top 25 Active Directory Security Best Practices](#)[5 Best SSH Clients for Windows](#)[Dcdiag: How to Check Domain Controller Health](#)[How to Clear Windows DNS Cache \(Server & Workstations\)](#)

Search

Search

© 2021 Active Directory Pro, All rights reserved
[About](#) | [contact](#) | [EULA](#) | [Privacy Policy](#) | [YouTube](#)