Active Directory Pro

User Unlock Tool

Administrator Guide

DESCRIPTION:

The user unlock tool finds all locked user accounts with a click of a button. You can then unlock the account, reset the password or display additional details like bad password time, count, lockout time and the source computer. This tool makes it easy to troubleshoot account lockouts.

SYSTEM REQUIRMENTS:

- Microsoft .Net 4.7.2
- See below for required permissions.
- Tool can be run from a client computer or on the server.

READ FIRST:

- You need to have rights in Active Directory to unlock and reset accounts. If you are a domain administrator then you are good.
- If you want to allow helpdesk or non domain admins to use this tool, you can do so by delegating them rights in Active Directory
- You must enable auditing to display additional details on locked accounts. This will display the source computer, bad password count, bad password time, domain controller and lockout time. See steps below for enabling this.
- Staff will need rights to view domain controller event logs to view the detailed information. Again, if you are a domain administrator then you already have the required rights.

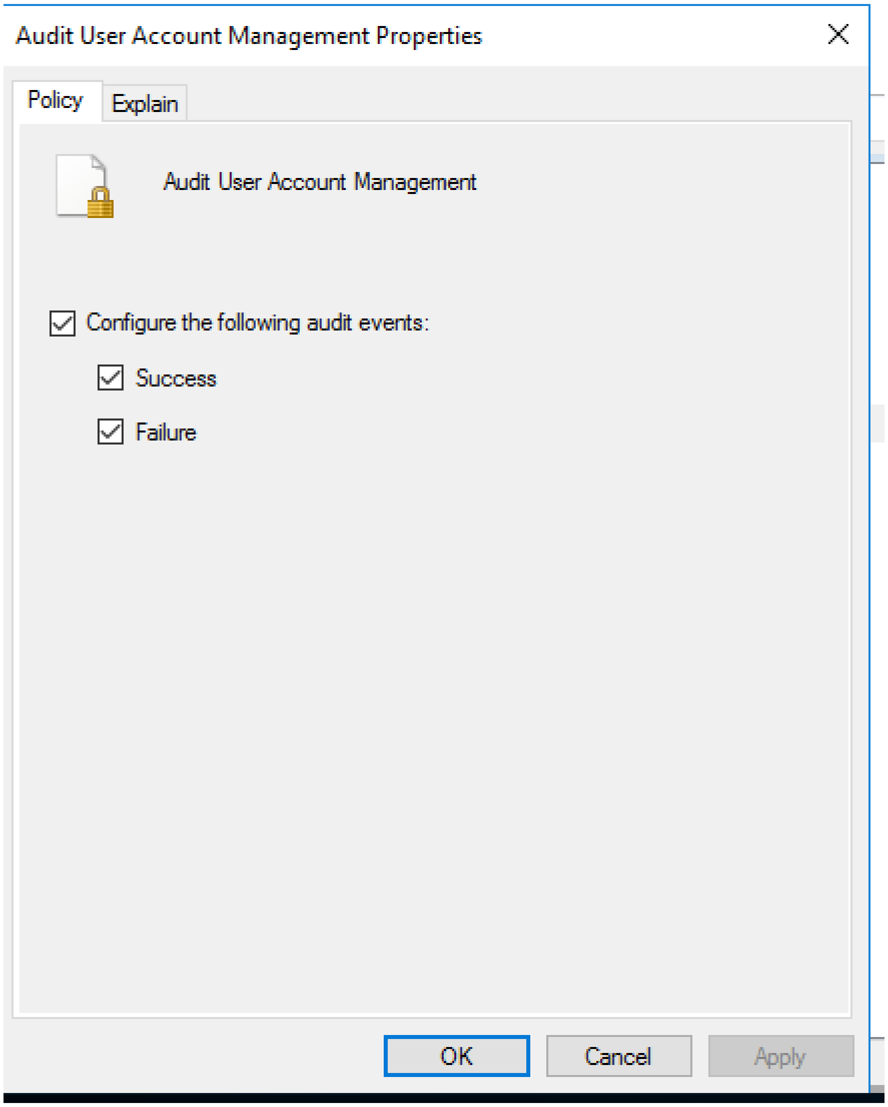
ENABLE AUDITING:

If you want to display additional details on locked accounts like the source computer, you need to make sure auditing is enabled for these events.

On your Default Domain Controller policy navigate to the following GPO settings:

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

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



Audit User Account Management Properties

Policy | Explain

Audit User Account Management

☑ Configure the following audit events:

☑ Success

☑ Failure

The required auditing is now turned on and event ID 4740 will be logged in the security event logs when an account is locked out. The user unlock tool will query the domain controller event logs for this event ID to display additional lockout details.

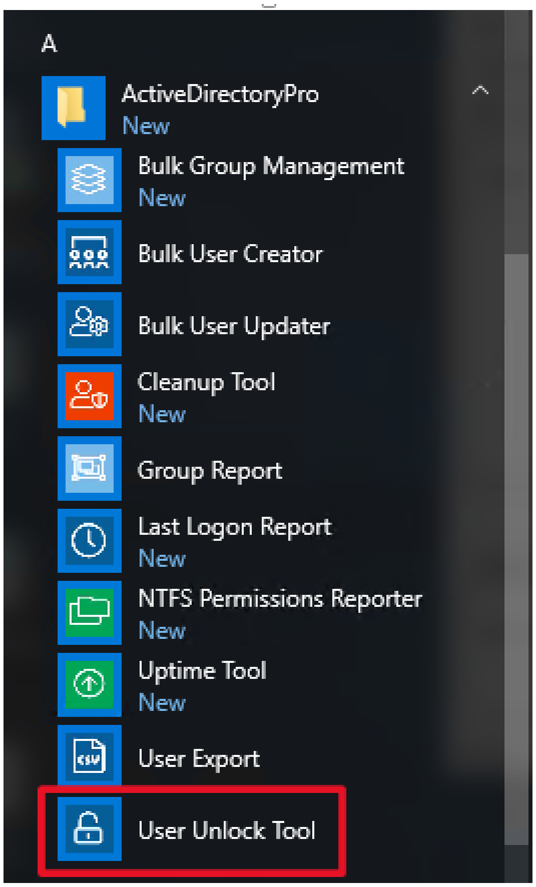
HOW TO:

The following section includes the following examples:

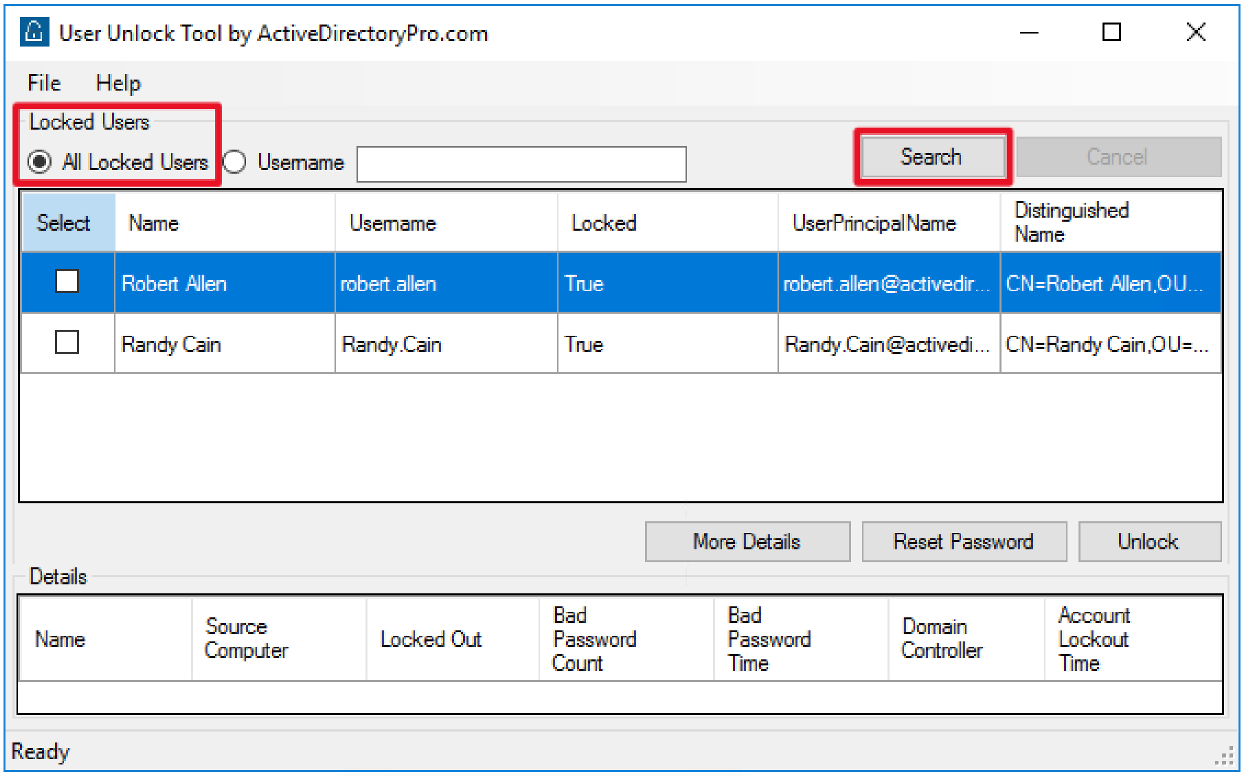
Example 1: Find All Locked User Accounts
Example 2: Unlocking accounts
Example 3: Resetting Passwords
Example 4: Check Status on a single account
Example 5: Display additional lockout details

Example 1: Find All Locked User Accounts

All tools are added to the start menu under the folder ActiveDirectoryPro



To find all locked user accounts select “all Locked Users” and click search.



Locked Users

● All Locked Users ○ Username

Select	Name	Username	Locked	UserPrincipalName	Distinguished Name
□	Robert Allen	robert.allen	True	robert.allen@activedir...	CN=Robert Allen,OU...
□	Randy Cain	Randy.Cain	True	Randy.Cain@activedi...	CN=Randy Cain,OU=...

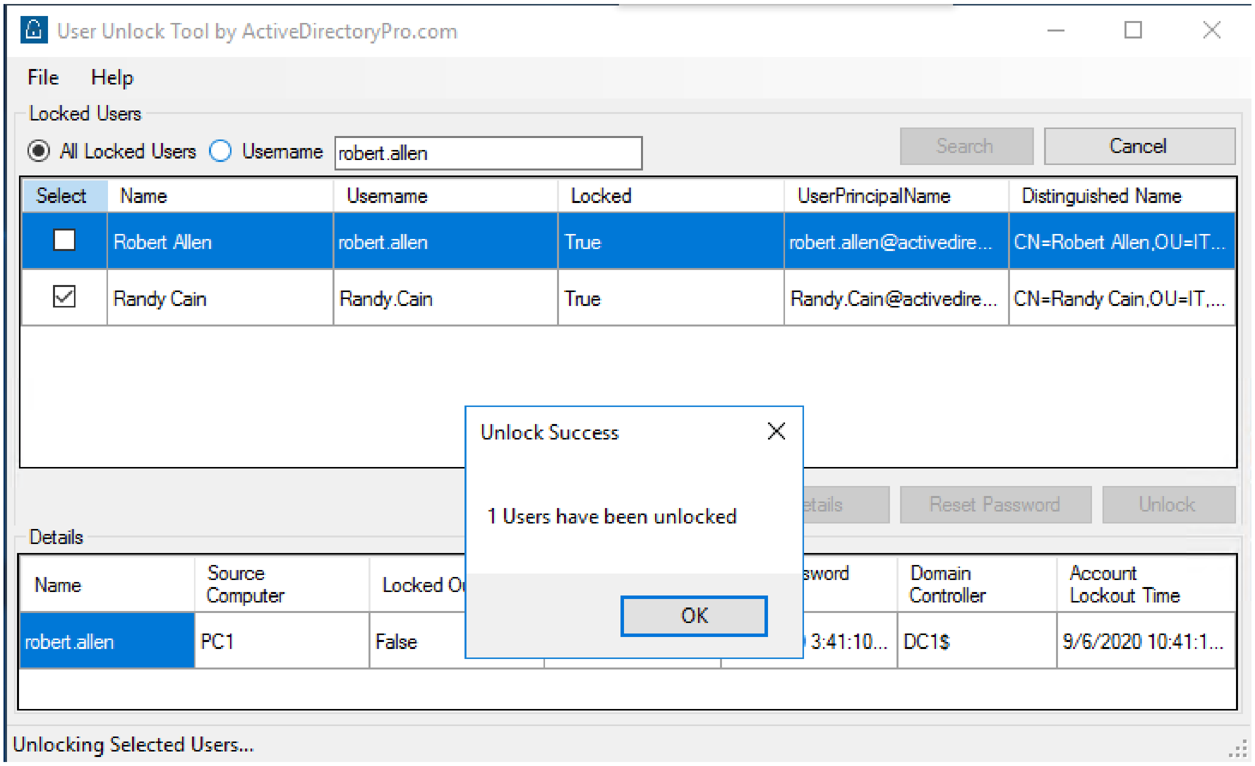
Details

Name	Source Computer	Locked Out	Bad Password Count	Bad Password Time	Domain Controller	Account Lockout Time

On the screenshot above you can see I have two locked user accounts, Robert Allen and Randy Cain.

Example 2: Unlocking accounts

To unlock an account, select one or more accounts then click the unlock button. You will get a popup window letting you know the account has been successfully unlocked.



Locked Users

● All Locked Users ○ Username robert.allen

Select	Name	Username	Locked	UserPrincipalName	Distinguished Name
□	Robert Allen	robert.allen	True	robert.allen@activedire...	CN=Robert Allen,OU=IT...
☑	Randy Cain	Randy.Cain	True	Randy.Cain@activedire...	CN=Randy Cain,OU=IT,...

Unlock Success

1 Users have been unlocked

Details

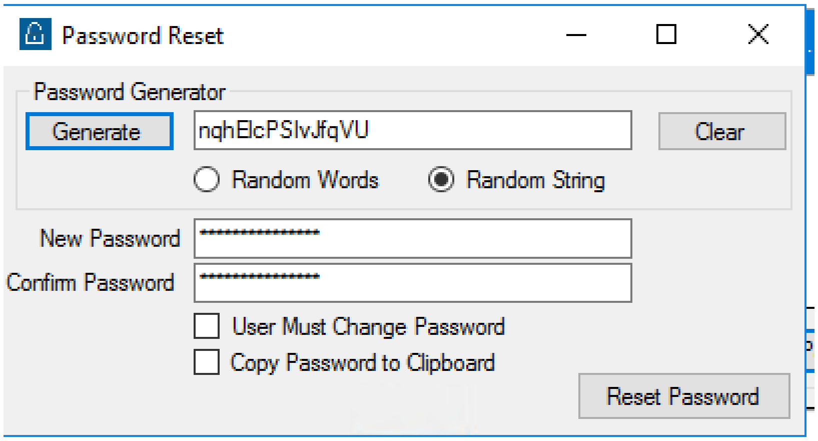
Name	Source Computer	Locked O		sword	Domain Controller	Account Lockout Time
robert.allen	PC1	False		3:41:10...	DC1$	9/6/2020 10:41:1...

Unlocking Selected Users...

Example 3: Resetting Passwords

To reset a users password select the account then click the Reset Password button. You will get a Password Reset box that has several options. You can click the “Generate” button to randomly generate a password.

If you don’t want a random password generated just type the password into the new and confirm password boxes.



Password Generator

nqhElcPSlvJfqVU

○ Random Words ● Random String

New Password ***************

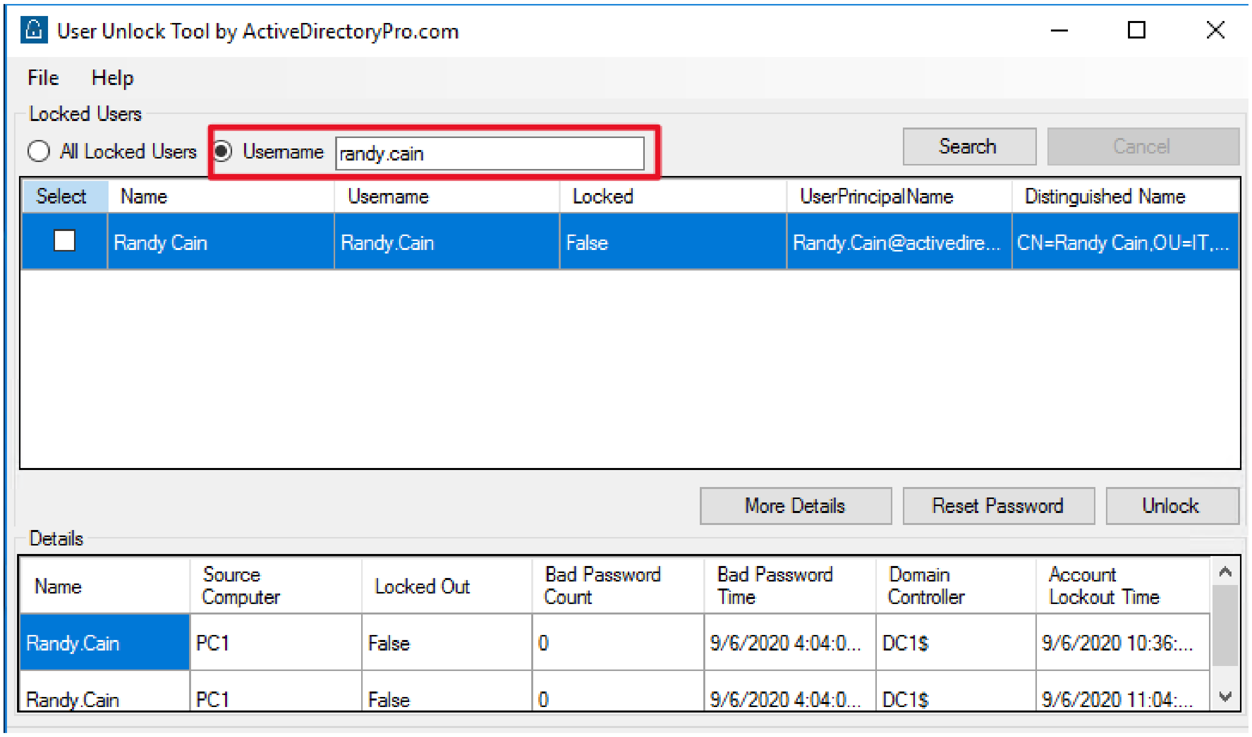
Confirm Password ***************

□ User Must Change Password

□ Copy Password to Clipboard

Example 4: Check Status on a single account

If you want to check the status on a single account or reset a users password select the username radio button, type the logon name into the box and click search.



○ All Locked Users ● Username randy.cain

Select	Name	Username	Locked	UserPrincipalName	Distinguished Name
□	Randy Cain	Randy.Cain	False	Randy.Cain@activedire...	CN=Randy Cain,OU=IT,...

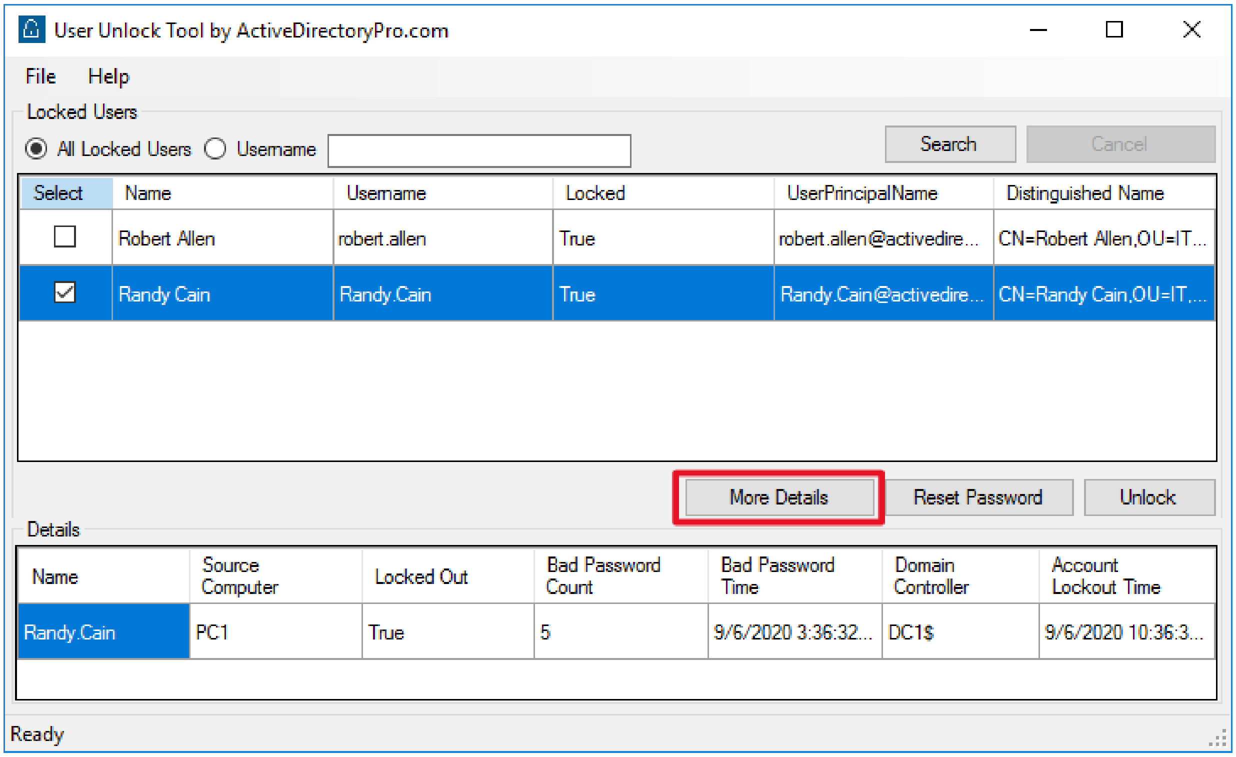
Name	Source Computer	Locked Out	Bad Password Count	Bad Password Time	Domain Controller	Account Lockout Time
Randy.Cain	PC1	False	0	9/6/2020 4:04:0...	DC1$	9/6/2020 10:36:...
Randy.Cain	PC1	False	0	9/6/2020 4:04:0...	DC1$	9/6/2020 11:04:...

You can see the account is not locked out. You can click the more details button to check when the users last bad password attempt, he domain controller and the source computer. You can also click the Reset Password button to change the users password.

Example 5: Display additional lockout details

Important: This requires auditing to be enabled. Please see the top of this document for steps on enabling auditing.

The more details button is a very helpful feature when it comes to troubleshooting account lockouts. When accounts are locked out an event 4740 is recorded in the security event logs on the DC. This tool will query the those logs and display the details in an easy to read format.



Locked Users

● All Locked Users ○ Username

Select	Name	Username	Locked	UserPrincipalName	Distinguished Name
□	Robert Allen	robert.allen	True	robert.allen@activedire...	CN=Robert Allen,OU=IT...
☑	Randy Cain	Randy.Cain	True	Randy.Cain@activedire...	CN=Randy Cain,OU=IT,...

Details

Name	Source Computer	Locked Out	Bad Password Count	Bad Password Time	Domain Controller	Account Lockout Time
Randy.Cain	PC1	True	5	9/6/2020 3:36:32...	DC1$	9/6/2020 10:36:3...

Ready

In the above example, you can see the source computer was PC1. This tells you the lockout came from PC1. can also see other details like the last bad password time, count, domain controller and lockout time.

For issues, questions or feature requests please email me at robert@activedirectorypro.com