**Easily Find Local Administrators on all Computers**

July 26, 2022 by [Robert Allen](https://activedirectorypro.com/author/mug/)

In this article, I’ll show you how to find users that have local administrator rights on local and remote computers.

The first option is to use a GUI tool called local admin report. If you don’t want to use third party [Active Directory Tools](https://activedirectorypro.com/tools/) then I’ll show you a second option using PowerShell.

Users that have local administrator rights have full control over the local computer. This allows users to install unwanted software, change computer settings, and makes it easier for viruses and malicious software to be installed. It also makes it easier for hackers to take control of your computer.

*In a Microsoft Vulnerability report, they found that 85% of critical vulnerabilities could have been mitigated by removing admin rights.*

**What are local administrators?**

On the local computer, there is a group called Administrators. Users of this local group will have administrator rights on the local computer. You can see this group by going to Computer Management -> Local users and Group -> Groups

Graphical user interface, text, application

Description automatically generated

In the screenshot above you can see I have four members in the local administrator group. Two of these members are domain groups (ADPRO\Domain Admins and ADPRO\Domain Users). It’s normal for domain admins and the local administrator account to be in this group.

Domain Users should not be in this group. This means every user in the domain has full admin rights to the computer.

Let’s check out two methods for hunting down users that have local administrator rights.

**Method 1: Find Local Administrator Rights with AD Pro Toolkit**

This first method I’ll show you is the [local admin reporting too](https://activedirectorypro.com/local-admins-reporting-tool/)l. This is one 1 of 13 tools from the AD Pro toolkit. This tool makes it super easy to scan computers for local administrators.

**Requirements:**

1. AD Pro Toolkit – [You can download a free trial here.](https://activedirectorypro.com/download-thank-you/)
2. WMI needs to be allowed on the [Windows Firewall Settings](https://activedirectorypro.com/windows-firewall-best-practices/). If you have this blocked you can use group policy to open this up on all computers.

**Step 1:** Open Toolkit

Under Tools select “Local Admins Report”

**Step 2:** Select Seach Options

Next, choose which computers to scan. You can scan the entire domain, select an OU/Group or search computer objects.

**Step 3:** Click Run

Now just click the run button. The results will be displayed in the report section.

You can see in the screenshot above I have several users and groups that are a member of the local Administrators group on multiple computers. The Principal Source column will tell you if the account is a local account or a domain account.

**Step 3:** Export Results to CSV file.

To export just click the export button, select format, and select “export all rows”

Now you will have a report of all local administrators on all computers. In the screenshot below I highlighted some accounts that should not have admin rights. I’ll need to investigate these computers.

Table

Description automatically generated

**Get All Local Group Members**

By default, this tool gets the members of the Administrators group only. If you want to get a report of all local groups then select the “Show All Groups” box.

Here is a screenshot from a few computers on my network.

Try the Local Admin Report for free, [download your copy here](https://activedirectorypro.com/download-thank-you/).

**Method 2: Find Local Administrator Rights with PowerShell**

To find local administrators with PowerShell you can use the Get-LocalGroupMember command.

Here is an example of running on a local computer

Get-LocalGroupMember -Group "Administrators"

[Text

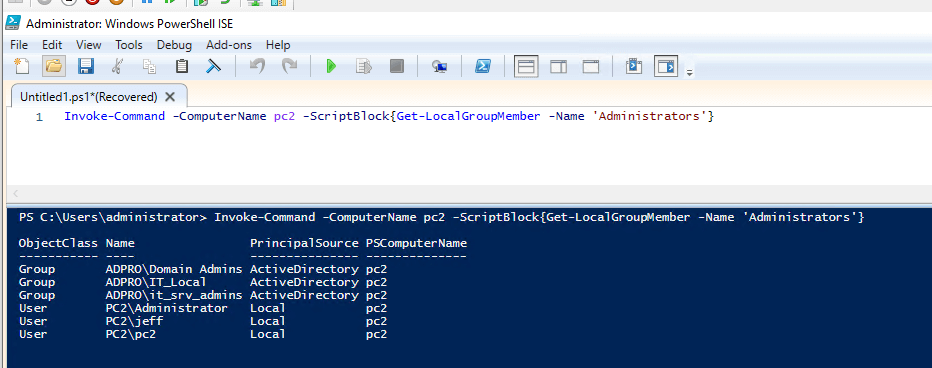
Description automatically generated](https://activedirectorypro.com/wp-content/uploads/2021/11/find-local-admins-powershell-1.png)

The above example is running the command on the local computer. To run on a remote computer you can use the invoke-command. For this command to work you will need to have PowerShell Remoting enabled. It’s disabled by default.

You can use the command Enable-PSRemoting to enable PowerShell Remoting. You would need to use group policy or some other deployment method to enable on all computers.

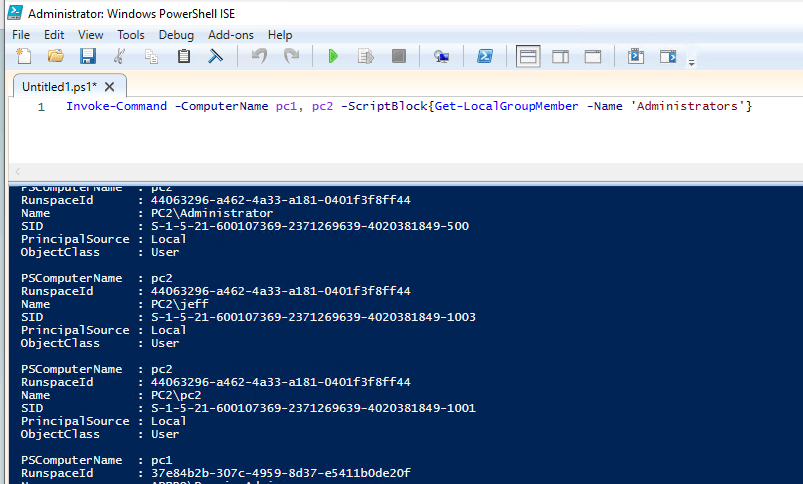
When PowerShell Remoting is enabled you can use this command to get the local administrators on remote computers.

Invoke-Command -ComputerName pc2 -ScriptBlock{Get-LocalGroupMember -Name 'Administrators'}

[](https://activedirectorypro.com/wp-content/uploads/2021/11/find-local-admins-powershell-2.png)

To run this command on multiple computers just separate them with a comma. Here is an example of running this command on computers with the hostname of PC1 and PC2.

Invoke-Command -ComputerName pc1, pc2 -ScriptBlock{Get-LocalGroupMember -Name 'Administrators'}

[](https://activedirectorypro.com/wp-content/uploads/2021/11/find-local-admins-powershell-3.png)

You can see in the above screenshot the output is not ideal and would require some additional work. This is why I created the [Local Admin Report Tool](https://activedirectorypro.com/local-admins-reporting-tool/), it makes scanning multiple computers for local admins very easy and the output is simple to read.

**Removing Local Administrator Rights**

I’ve just shown you two methods for finding administrator rights. Now you need to identify the users that do not need these rights and remove them.

The best way to remove local administrator rights is to use group policy and Restricted groups. Restricted groups allow you to centrally manage the local groups on all computers in your domain. You can also target specific computers or OUs instead of the entire domain.