ezaudit

TROUBLESHOOTING AUTOMATED AUDITS

These are the steps that most commonly resolve issues where automated audits aren’t running either at all or for some users.

One or more of these reasons account for well over 90% of our tech support requests.

And less than 10% of our users ever contact us for support, so they’re pretty rare altogether.

So, it’s a good bet one or more of these will get your issue resolved.

You should also check www.ezaudit.net/guide and look at the troubleshooters there for new or less common issues and solutions.

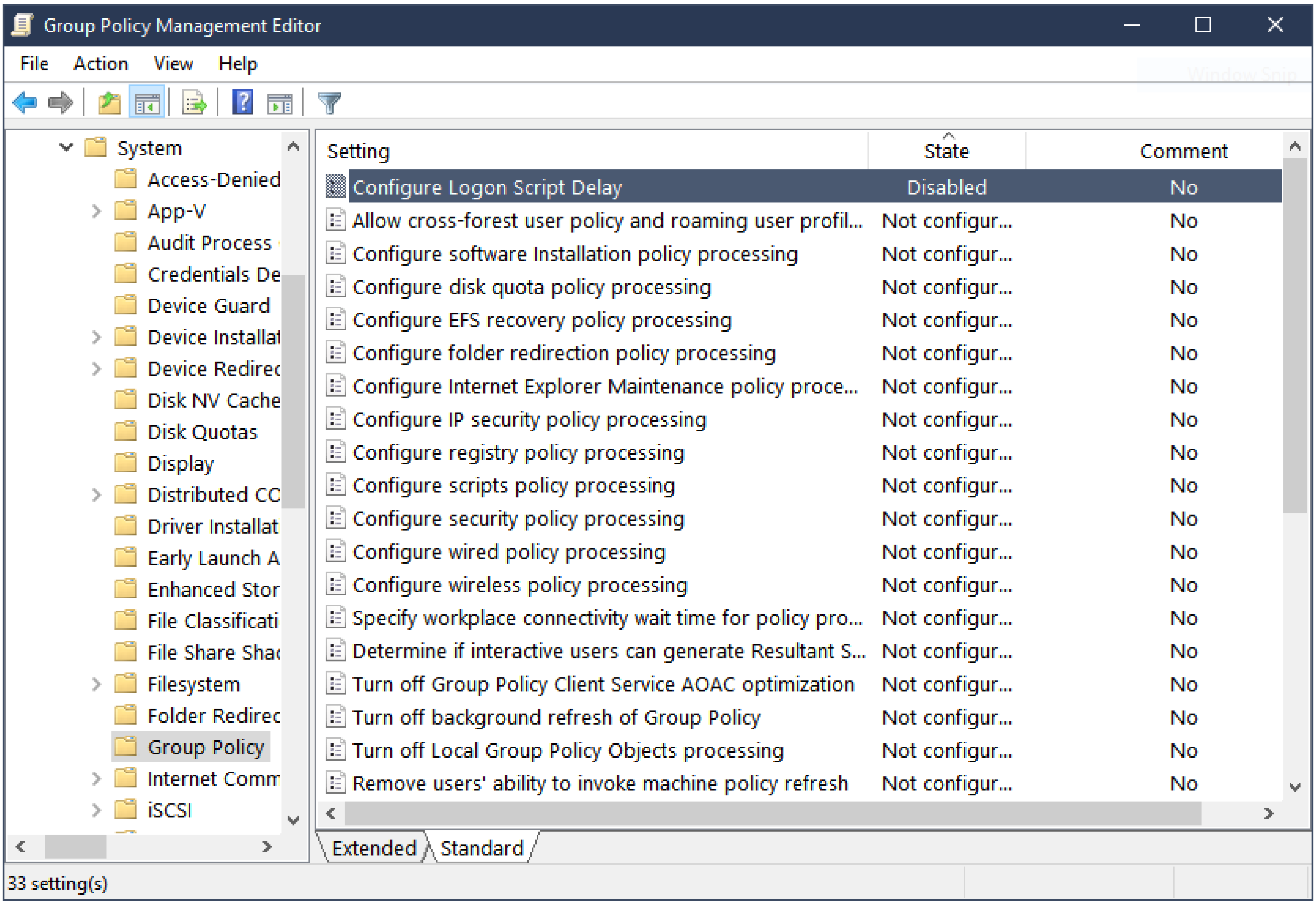
Current "Hot Topic" if you've moved from Windows 7 to Windows 10 clients on Server 2012 R2 or Server 2016

This actually started with Windows 8.1, but has persisted for many Windows 10 users.

In a nutshell, there's a GP setting to delay, for who know what logical reason, the running of Group Policy for 5-minutes *after* the user authenticates to your network. This is pretty daft on the face of it, but what's worse is that for a lot of users *Group Policy never runs*.

You have to disable that delay to ensure GP runs as it has always done before:

Go to Computer Configuration > Administrative Templates > System > Group Policy then "Configure Logon Script Delay" and Disable it.



Setting	State	Comment
Configure Logon Script Delay	Disabled	No
Allow cross-forest user policy and roaming user profil...	Not configur...	No
Configure software Installation policy processing	Not configur...	No
Configure disk quota policy processing	Not configur...	No
Configure EFS recovery policy processing	Not configur...	No
Configure folder redirection policy processing	Not configur...	No
Configure Internet Explorer Maintenance policy proce...	Not configur...	No
Configure IP security policy processing	Not configur...	No
Configure registry policy processing	Not configur...	No
Configure scripts policy processing	Not configur...	No
Configure security policy processing	Not configur...	No
Configure wired policy processing	Not configur...	No
Configure wireless policy processing	Not configur...	No
Specify workplace connectivity wait time for policy pro...	Not configur...	No
Determine if interactive users can generate Resultant S...	Not configur...	No
Turn off Group Policy Client Service AOAC optimization	Not configur...	No
Turn off background refresh of Group Policy	Not configur...	No
Turn off Local Group Policy Objects processing	Not configur...	No
Remove users' ability to invoke machine policy refresh	Not configur...	No

Group Policy Issues

It seems pretty obvious, but it's often overlooked: *is* Group Policy launching at users PCs that are not being audited?

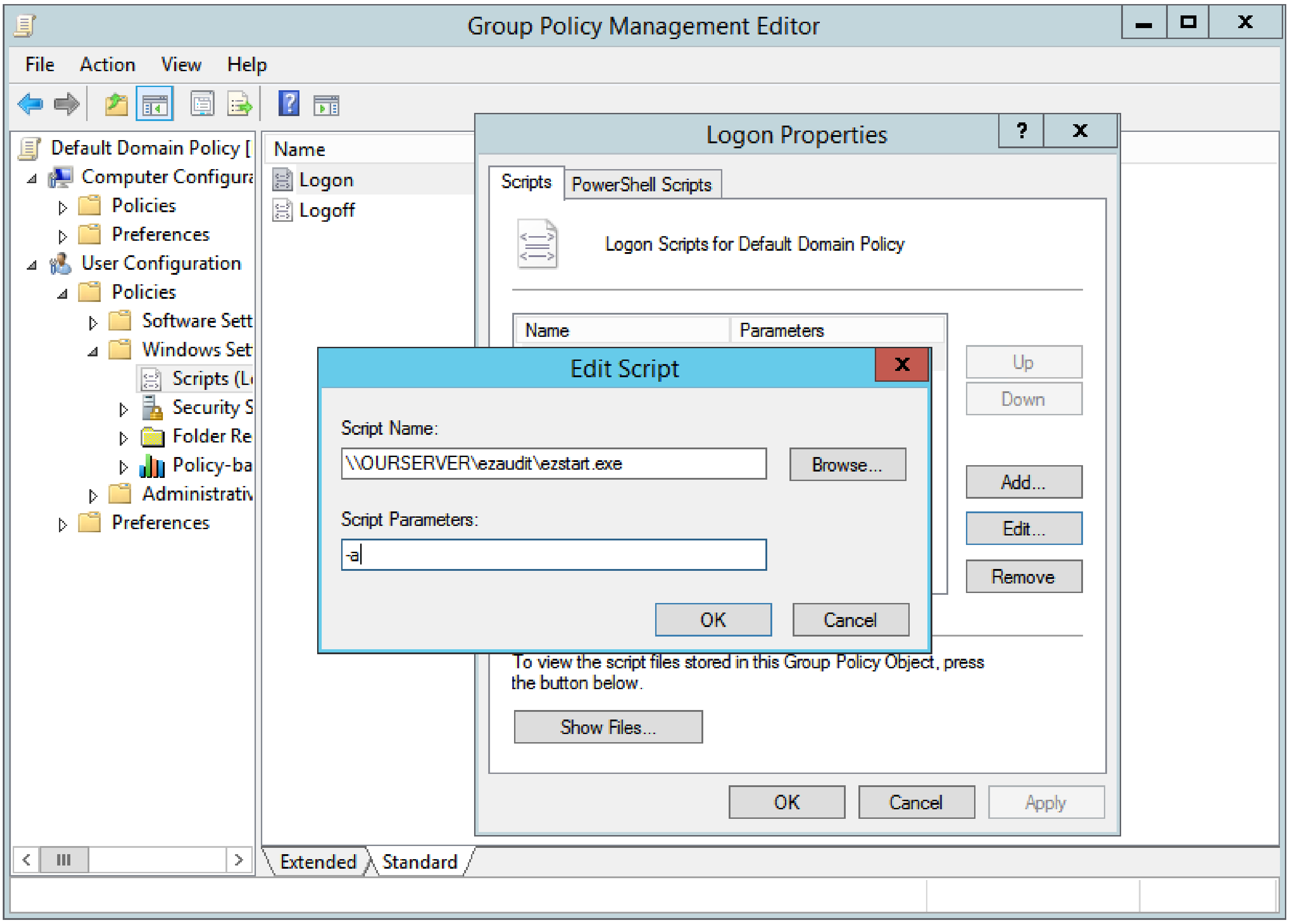
Or is something failing in your GP?

Remote into an affected user's PC and run RSoP.

Fix any errors reported.

How are you launching the audit from Group Policy?

The recommended method is to enter the command needed to launch our audits directly into your GP, i.e. via GMPC.msc to the domain server, then do it as per this screen cap:



Logon Scripts for Default Domain Policy

Script Name: \\OURSERVER\ezaudit\ezstart.exe

Script Parameters: -a

To view the script files stored in this Group Policy Object, press the button below.

The minimum required is the server path in UNC format with the "-a" switch to launch ezstart.exe.

Scripting Issues

If you script your logon functions like drive mapping, printer mapping, etc., and add E-Z Audit to your existing script, check the script carefully.

If you're using a batch file (.BAT or .CMD) and added us to it, look at it carefully.

GOTO commands are a huge problem in these legacy type of scripts.

We've seen it time and again that all or some users are sent to some GOTO skipping right past the line to launch ezstrart.exe.

And of course, check the code – syntax errors matter. If you're using a VBScript, here's an example of what it *should* look like – although some of you might reduce the verbosity of it (meant to be easier than using nested quotes, etc.)

```
Dim WSHShell

Set WSHShell = CreateObject("WScript.Shell")

shellthis = "\\your_server_name\ezaudit\ezstart.exe"

shellcmd = Chr(32) & "-a

WSHShell.Run Chr(34) & shellthis & Chr(34) & shellcmd ,1,False
```

Permissions Issues

The should have been the #1 issue on the list, but we do get a lot of pushback that "I know how to set permissions", and in the end it was, well, permissions.

If permissions are not correct either the audits will never launch, or they do but can't save. And if they do launch and an error happens and they can't write to the corresponding error logs.

> UPDATE 17 December 2017 – To address the above scenario, the ezstart.exe, ezscan.exe and ondemand.exe modules will write errors to the PC or server being audit into the Application Event Log. So you can remote into it and see what happened. The modules are all 15.99.7408 or higher.

So review permissions:

The two folders you share from your domain server, for example…

\\server-name**ezaudit\audits**

…require the following permissions:

\ezaudit\ require read, write, create, modify, delete and execute permissions. This is the folder where you should have ezstart.exe, ezscan.exe and optionally ondemand.exe and config.exe

You also need at least one configuration file, by default config.ezc, created in the config.exe tool either here or from the Admin Console at your PC then saved here.

The **\audits** folder require the same as above but execute is not needed.

TIP: Don't assume "Everyone" > Full Control will always work.

We've seen plenty of situations that where the folders for E-Z Audit reside *below* folders where Admins have set explicit Deny permissions for Everyone *above* then which take precedence over Allow permissions.

Results: won't run. Denied.

And Everyone > Full Control isn't the most secure thing to do – but that's another story.

Consider using Domain Users or Authenticated Users and set the needed permissions for them.

Read, Write, Create, Delete, Modify, Execute.

TRY IT: go to or remote into a user's PC that's not auditing *using their logon* in Explorer navigate to the share like \\server\ezaudit and click ezscan.exe.

Do you get the manual audit interface? Ok, now run a Basic Audit as that's just few seconds and this is just a test.

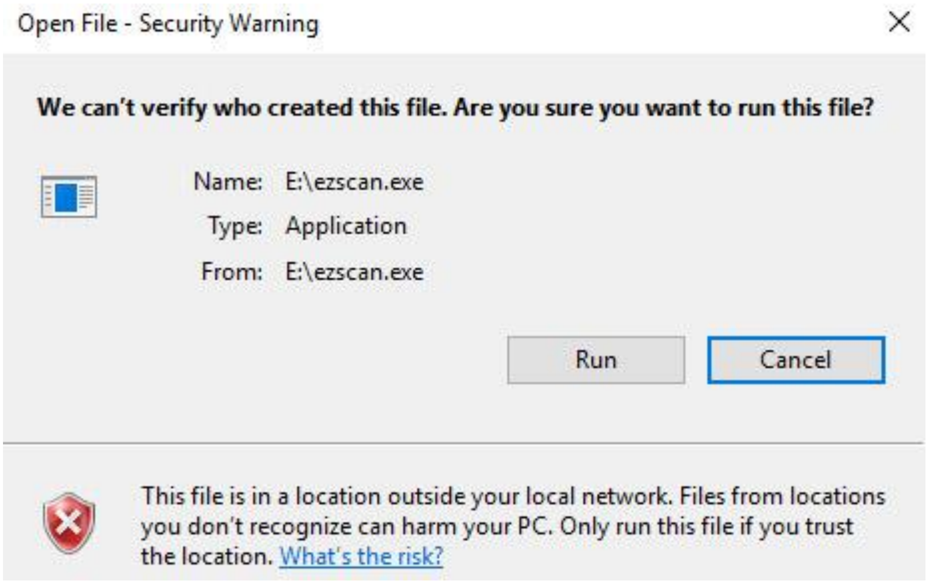
When it's done, try saving to \\server\ezaudit\audits. Does it save?

Ok, if it does, then next test:

Go back into \\server\ezaudit\. Open Notepad. Drag the config.ezc file into Notepad. Does it open?

If you get an error – they can't read so they audit module can't run configured as they can't read the contents of the configuration file.

Or do you get a security warning like this from Windows:



Open File - Security Warning

We can't verify who created this file. Are you sure you want to run this file?

Name: E:\ezscan.exe

Type: Application

From: E:\ezscan.exe

This file is in a location outside your local network. Files from locations you don't recognize can harm your PC. Only run this file if you trust the location. What's the risk?

If you do, then there's some trust relationship problem with that PC and the server where the modules are located. You'll need to hunt those down – we can't assist with fixing domain issues, just point to what could be wrong, etc.

Config file issues (*.ezc)

By default E-Z Audit saves config files as config.ezc.

But there are power user options to create as many as you want for different purposes/groups/whatever and call them whatever you want.

If you want a *specific* config file used, you have to pass the file name, e.g.

```
ezstart.exe -a -f:some-other-file-name.cfg
```

If you have multiples and don't set a specific file, E-Z Audit looks for config.ezc and if it finds it uses that one.

If there a multiples and there *isn't* a config.ezc, the audit fails. An error is logged and the process terminates.

Another frequent issue, related to not getting *fresh* audits is when the configuration was set to do audits every, say, 120 days. And the Admin forgot that. And wonders why no new audits. Because it's not that many days apart.

Or, **related to permissions**, you get *one* audit then no more because we can't delete the old one with the new one. Make sure users can delete stuff from where you're saving the audits.

PCs that are never shut down

Lots of issues have been resolved by finding out that users *never* shut down or log off their PCs.

So, login scripts don't run – the machines just come back from sleep or hibernate or not even that - they just sit there causing global warming 24/7/365.

These are not going to run a new audit. They're good candidates for On-Demand audits. Learn more about those from the User's Guide.