

## How to view Windows 7 file access failure

The howto shows how to view file access failure in the Windows 7 Event Viewer. The howto believes you have already accessed a file that your logon does not have permission.

Preuss

2/12/2012



Recycle Bin



Adobe Reader X



LibreOffice 3.4



Mozilla Firefox

A logon on this system has already attempted to access a file that the logon does not have permission.  
  
We are now logon as administrator to view the log entry.



Local Security Policy

File Action View Help

Security Settings

- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Firewall with Advanced Security
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Computer
- Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	Success, Failure
Audit account management	Failure
Audit directory service access	No auditing
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit system events	No auditing

These are the Local Security Policy settings to record the file access failure.

Administrative Tools

Size

- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 2 KB
- 3 KB

Taskbar and Start Menu

VMware Tools

Windows Defender

Windows Anytime Upgrade

Windows Firewall

User Accounts

Windows CardSpace

Windows Update

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 554 (!) New events available

Level	Date and Time	Source	Ev...	Task Category
Information	2/12/2012 5:03:19 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:18 PM	Microsoft Wind...	4656	File System
Information	2/12/2012 5:03:09 PM	Microsoft Wind...	4673	Sensitive Privilege Use
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...
Information	2/12/2012 5:03:07 PM	Microsoft Wind...	4656	Other Object Access...

Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

PREUSS-WIN7-X64\nxt  
 next  
 PREUSS-WIN7-X64  
 0x12b5cc

Microsoft Windows security  
 Logged: 2/12/2012 5:03:19 PM  
 Task Category: File System  
 Keywords: Audit Failure  
 Computer: preuss-win7-x64

[Event Log Online Help](#)

Actions

- Security
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help
- Event 4656, Microsoft Wind...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

Open the Event Viewer | Windows Logs | Security.

Event Viewer

File Action View Help

Event Viewer (Local)

- Custom Views
- Windows Logs
  - Application
  - Security
  - Setup
  - System
  - Forwarded Events
- Applications and Services Logs
- Subscriptions

Security Number of events: 554 (!) New events available

Level	Date and Time	Source	Ev...	Ta
Information	2/12/2012 4:58:44 PM	Microsoft Wind...	4656	Fi
Information	2/12/2012 4:58:01 PM	Microsoft Wind...	4957	M

Event Properties - Event 4656, Microsoft Windows security auditing.

General Details

A handle to an object was requested.

Subject:

Security ID:	PREUSS-WIN7-X64\preuss
Account Name:	preuss
Account Domain:	PREUSS-WIN7-X64
Logon ID:	0xd1c6f

Log Name: Security

Source:	Microsoft Windows security	Logged:	2/12/2012 4:58:44 PM
Event ID:	4656	Task Category:	File System
Level:	Information	Keywords:	Audit Failure
User:	N/A	Computer:	preuss-win7-x64
OpCode:	Info		

More Information: [Event Log Online Help](#)

Copy Close

This log entry shows failure to access a file.

Use the copy button to get the complete information.

- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help
- Event 4656, Microsoft Wind...
- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

```

Log Name: Security
Source: Microsoft-windows-Security-Auditing
Date: 2/12/2012 4:58:44 PM
Event ID: 4656
Task Category: File system
Level: Information
Keywords: Audit Failure
User: N/A
Computer: preuss-win7-x64
Description:
A handle to an object was requested.

subject:
  Security ID: PREUSS-WIN7-X64\preuss
  Account Name: preuss
  Account Domain: PREUSS-WIN7-X64
  Logon ID: 0xd1c6f

object:
  Object Server: Security
  Object Type: File
  Object Name: C:\windows\system32\compmgmt.msc
  Handle ID: 0x0

Process Information:
  Process ID: 0x71c
  Process Name: C:\windows\system32\mmc.exe

Access Request Information:
  Transaction ID: {00000000-0000-0000-0000-000000000000}
  Accesses:
  READ_CONTROL
  SYNCHRONIZE
  WriteData (or AddFile)
  AppendData (or AddSubdirectory or CreatePipeInstance)

```

The copy button gives us complete information about the event. The description shows "A handle to an object was requested". We see the object that was requested and denied under object name.

Copy Close ? Help