

Lab 5 - Ticketing + Windows Troubleshooting and Event Viewer.

Lab 5 – In Lab 5 I practiced creating tickets in Jira and fixing common issues, like resetting a password, installing Microsoft Teams, and giving access to a shared drive. I also used Event Viewer to check logs for logons, restarts, and an unexpected shutdown. This gave me practice with the kind of tasks done in a Help Desk role.

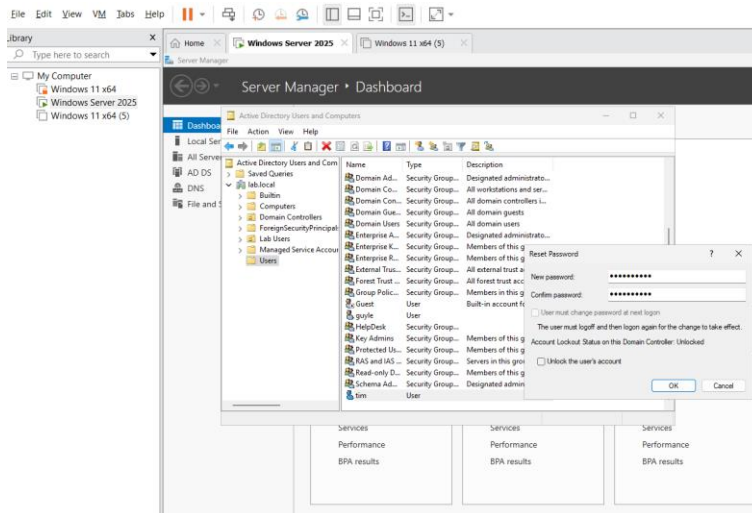
Ticket 1

I created a mock ticket in Jira with the summary “*User cannot log in to Windows.*” The ticket was raised under my name, **Tim**, and initially left unassigned. Its status was set to *Open* on **23 September 2025**, with a due date scheduled for **29 September at 13:00**.

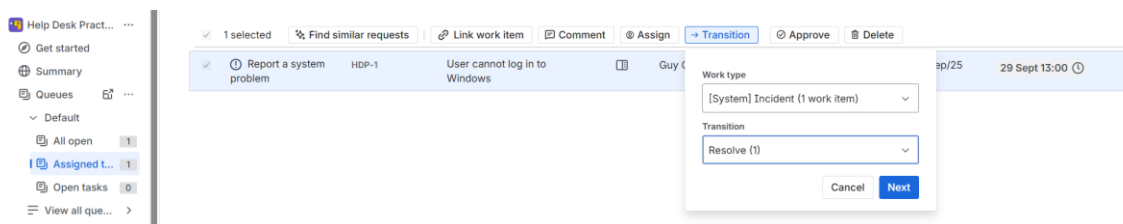
This ticket simulates a common help desk scenario where a user is locked out of their account or experiencing login issues. I assigned the ticket to myself, documented the troubleshooting process, and began investigating possible causes such as incorrect credentials, account lockouts, or password expiration. Once the simulated resolution steps were completed, I would close the ticket and update the status accordingly.

The screenshot displays the Jira Service Management interface. On the left, a sidebar contains navigation options: 'For you', 'Recent', 'Starred', 'Apps', 'Projects', and 'Recent'. Under 'Recent', 'Help Desk Pract...' is selected. The main content area shows the 'All open' queue for 'Help Desk Practice / Queues'. A search bar and filter buttons (Request type, Status, Assignee, More filters) are at the top. Below, a table lists 1 work item:

<input type="checkbox"/>	Request Type	Key	Summary	Reporter	Assignee	Status	Created	Time to resolution
<input type="checkbox"/>	Report a system problem	HDP-1	User cannot log in to Windows	Guy Cheneval	Unassigned	OPEN	23/Sep/25	29 Sept 13:00



Notes: Logged into my AD server and from here I reset Tims password

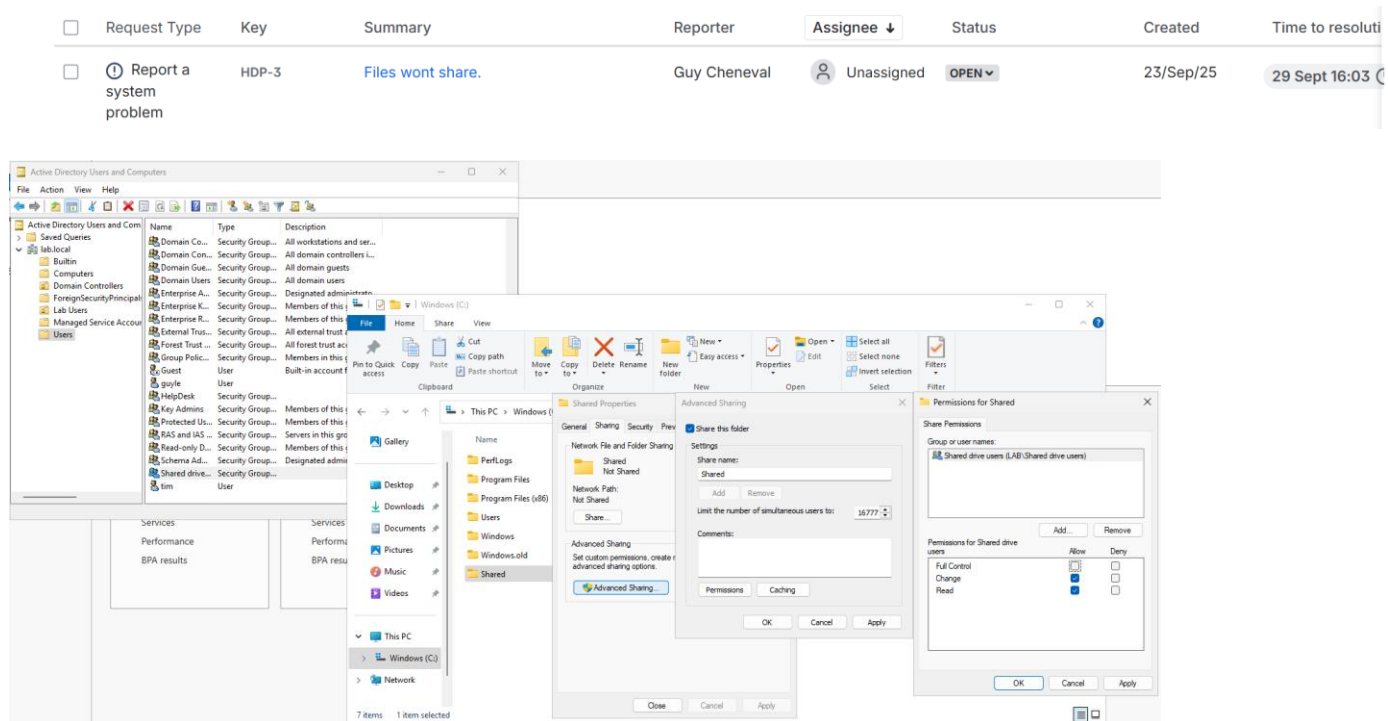


Notes: I resolved the login issue by accessing my VMware server that hosts the Active Directory domain controller. I located Tim's account in Active Directory Users and Computers, reset his password, and confirmed that he was able to log in successfully. The ticket was updated with these details and marked as *Resolved*.

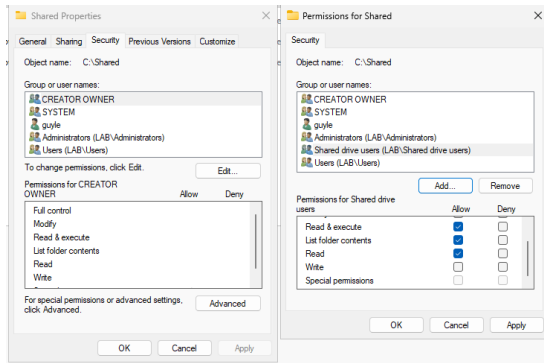
Ticket 2

I created a mock ticket in Jira with the summary, 23 September 2025, with a due date scheduled for 29 September 2025 at 4:03 pm.

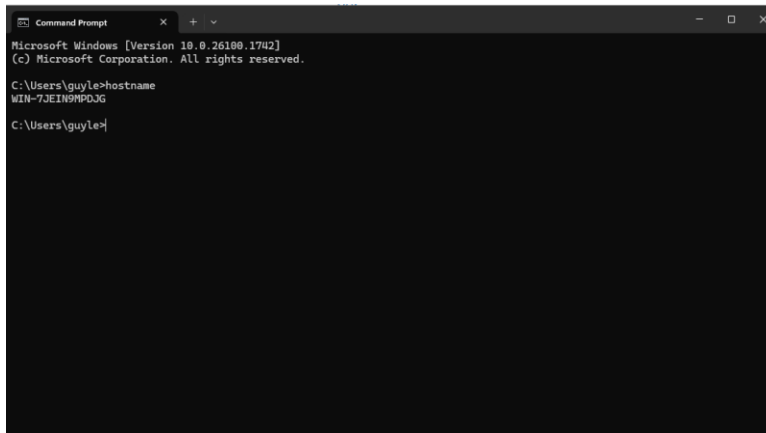
The description explained that employees were unable to share or access files on the file server, which suggested a possible permissions problem with the shared folder. To resolve the issue, I logged into Active Directory and opened *Active Directory Users and Computers*. I reviewed the affected accounts and confirmed they were not members of the *Shared drive users* group. I added the accounts to the group and verified that the group had the appropriate share and NTFS permissions on the C:\Shared folder. After the users logged out and back in, they were able to share and access files without further issues. I then updated the ticket with the resolution details, changed the status to *Resolved*, and closed the request.



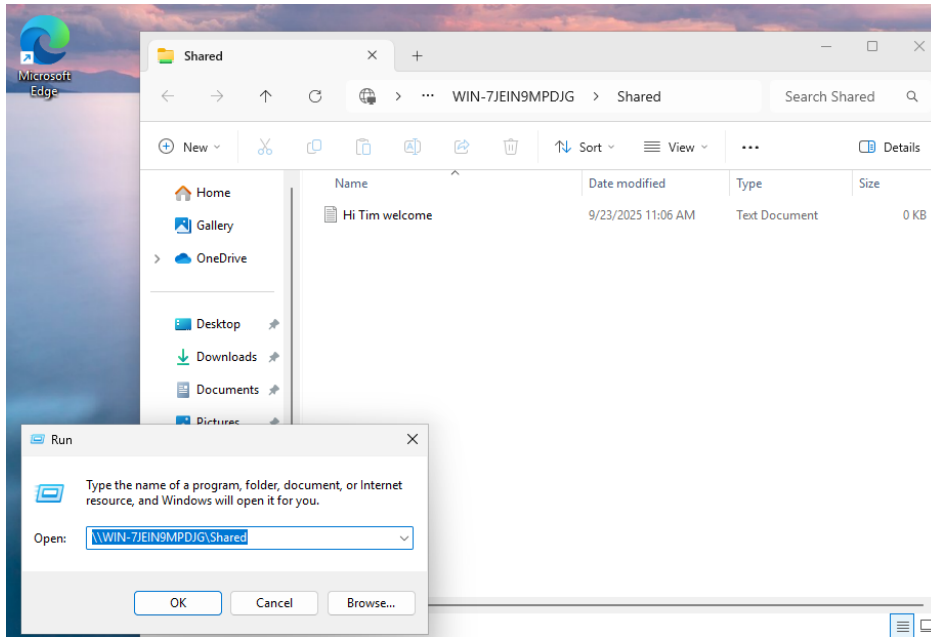
Notes: In Active Directory Users and Computers, I created a new security group called *Shared drive users*. I then created a folder called C:\Shared on the file server and opened the folder's properties to configure sharing. I enabled advanced sharing and added the *Shared drive users* group to control access.



Notes: In the Security tab of the C:\Shared folder, I verified that the *Shared drive users* group was added with the necessary NTFS permissions. I allowed the group *Read & execute*, *List folder contents*, and *Read* permissions, which ensures users in the group can open and view files in the shared directory.



Notes: On the file server, I ran the `hostname` command in Command Prompt. The result was **WIN-7JEIN9MPDJG**, which is the hostname required to connect to the shared folder using the UNC path (`\\WIN-7JEIN9MPDJG\Shared`).

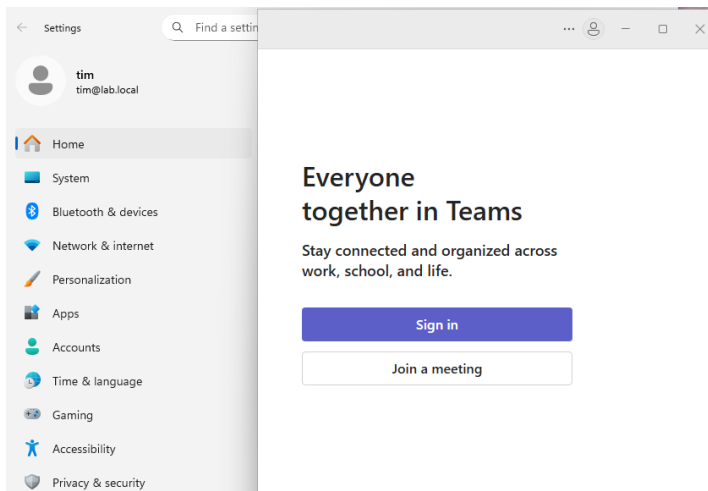


Notes: On a workstation, I tested access to the shared folder by entering the UNC path \\WIN-7JEIN9MPDJG\\Shared in the Run dialog. The folder opened successfully, showing a test file called *Hi Tim welcome*, confirming that the share was accessible to members of the *Shared drive users* group.

Ticket 3

I created a mock ticket in Jira with the summary “*User requires Microsoft Teams installed on their workstation.*” Its status was set to *Waiting for support* on 23 September 2025, with a due date scheduled for 1 October 2025 at 09:43.

This ticket simulates a common help desk request where a user needs new software installed but does not have the necessary local administrator rights to complete the installation themselves. I assigned the ticket to myself and downloaded the official Microsoft Teams installer from Microsoft’s website. Once the application was installed, I launched Teams to confirm it opened correctly. After verifying the installation, I updated the ticket with a clear resolution note, marked it as *Resolved*, and closed the request.



Notes: I finished the Microsoft Teams installation on Tim’s workstation while he was still logged in. To do this, I right clicked the installer file (Teams_windows_x64.msi) and chose Run as administrator. When the UAC prompt came up, I entered my admin username and password so the installer could run with elevated permissions. That let me install Teams successfully without logging Tim out. Once the installation was done, I opened Teams to check it worked and made sure Tim could sign in with his Microsoft 365 account. After confirming everything was fine, I updated the ticket, marked it as Resolved, and closed it.

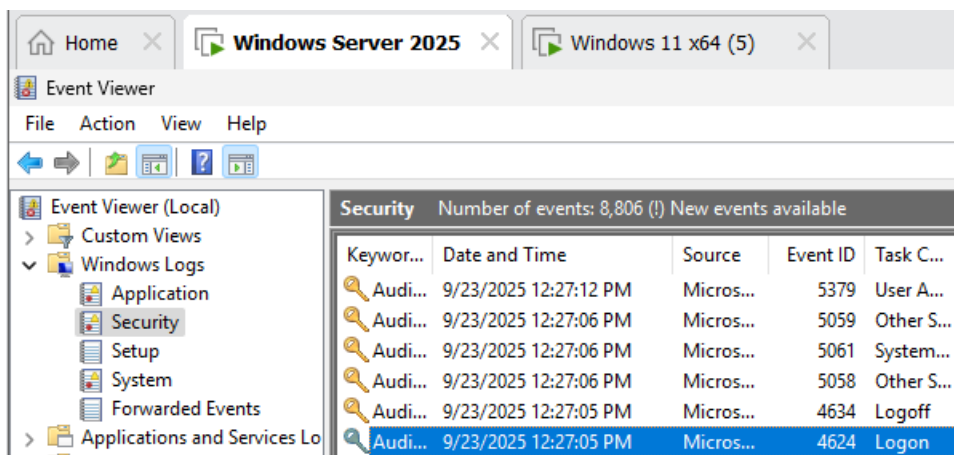
Event Viewer Windows Troubleshooting

As part of this lab, I spent some time using Event Viewer to practice basic troubleshooting in Windows. Event Viewer keeps a record of what's happening on the system, like application errors, logins, and system changes.

I tested a few simple scenarios that a help desk tech would normally check, such as logging in and out, restarting services, and looking at network changes. This helped me see how those actions show up in the logs and how they can be used to figure out what's going on when a user reports an issue.

Event Viewer

Event 1












Notes: To simulate a standard logon event, I signed out of my test account and then logged back in. After logging in, I opened Event Viewer and navigated to Windows Logs → Security.

In the Security log, I found Event ID 4624, which records a successful logon. The details included the account name, domain, logon type, and time of access.



This confirmed that Event Viewer accurately tracks user logons, which can be useful for troubleshooting access issues and monitoring account activity.

Event 2

Event ID: 6005 (8)				
	Information	9/23/2025 12:39:06 PM	EventL...	6005 None
	Information	9/23/2025 10:53:40 AM	EventL...	6005 None
	Information	9/23/2025 9:25:36 AM	EventL...	6005 None
	Information	9/22/2025 10:55:16 AM	EventL...	6005 None
	Information	9/22/2025 9:45:27 AM	EventL...	6005 None
	Information	9/22/2025 8:35:22 AM	EventL...	6005 None
	Information	9/21/2025 6:00:36 PM	EventL...	6005 None
	Information	9/21/2025 5:56:07 PM	EventL...	6005 None
Event ID: 6006 (5)				
	Information	9/23/2025 12:38:50 PM	EventL...	6006 None

Notes: I restarted my workstation and checked Event Viewer under Windows Logs → System. Event ID 6005 showed that the Event Log service started after reboot, confirming the exact time the machine came back online. This type of event is important for troubleshooting because it helps track when a system was restarted, whether it shut down cleanly or unexpectedly, and how long it was offline. It can also be used to confirm user reports of unexpected restarts or downtime.’ And when paired with event id 6006 with matching time stamps it means a normal system session occurred.

Event 3

Event ID: 6008 (2)				
	Error	9/23/2025 9:25:36 AM	EventL...	6008 None
	Error	9/22/2025 9:45:27 AM	EventL...	6008 None

Notes: When I checked the System log in Event Viewer, I found Event ID 6008. This shows that the computer had an unexpected shutdown and didn't turn off the normal way. These logs are useful because they can confirm if a PC lost power, crashed, or was restarted suddenly. They help work out what happened and give a starting point for troubleshooting issues like power problems or crashes.

Lab 5 – Summary

Summary, in this lab, I worked on creating and resolving tickets in Jira while also practicing Windows troubleshooting with Event Viewer. I created three mock tickets to cover common help desk tasks: resetting a user's password in Active Directory, installing Microsoft Teams with admin rights, and fixing a shared drive access issue by adding users to the right security group. Each ticket was written in clear language, assigned to me, and then closed after I completed the steps to resolve it.

Alongside the ticketing practice, I used Event Viewer to see how Windows logs different types of activity. I captured three events: a successful logon (4624), a normal system restart (6005/6006), and an unexpected shutdown (6008). These examples showed me how Event Viewer can confirm user activity and system problems, which is useful for both troubleshooting and verifying what actually happened on a machine.

Lab 5 gave me the chance to bring together ticket management, technical troubleshooting, and documentation. It helped me understand how day-to-day issues get reported, tracked, and resolved, and gave me confidence in handling the type of work expected in a Level 1 Help Desk role.