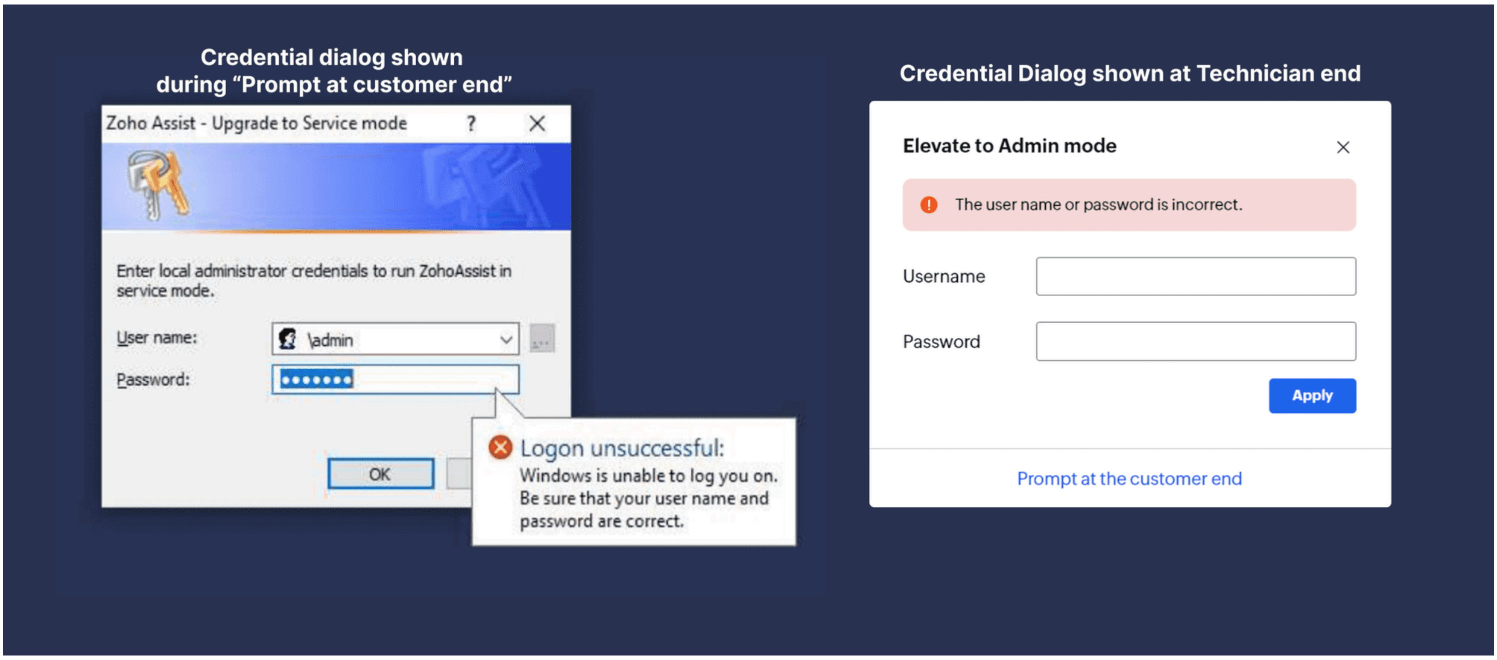
# Troubleshooting Elevate to Admin mode

### 1. Why is the Assist Credential dialog not displayed?

- If the network on the other end is slow, there might be a delay in the window showing up.
- If the desktop has any priority windows or dialogs, the Assist credential dialog may be hidden from view. To view the dialog, minimize any other unnecessary application windows and dialogs.
- If the session is on a desktop with multiple monitors attached, the Assist Credential dialog may be displayed on any of the secondary monitors. Try switching monitors in the viewer section.

### 2. Why am I getting "The user name or password is incorrect" or "Logon unsuccessful"?


Credential dialog shown during "Prompt at customer end"

Zoho Assist - Upgrade to Service mode

Enter local administrator credentials to run ZohoAssist in service mode.

User name: \admin

Password: •••••••

Logon unsuccessful:
Windows is unable to log you on. Be sure that your user name and password are correct.

Credential Dialog shown at Technician end

Elevate to Admin mode

The user name or password is incorrect.

Username

Password

- The above dialog box indicates that either the username or the password is wrong. Login is unavailable with the respective user credentials.
- Try logging in using pre-populated local admin accounts available in the username dropdown box in the *Prompt at customer end* window.
- If you are still having problems elevating, follow the below steps:
    1. Open Command Prompt by Start -> Run, then type "**cmd**".

2. Type the following command, "**runas /user:domain\username notepad.exe**". For example, If you had a user named "Dave Maria", the command would be **"runas /user:mydomain\Dave Maria notepad.exe"** (without quotes).

3. This will display a password prompt on the terminal screen. When the user enters the appropriate password, a notepad instance is launched on the user's desktop indicating that the username and password are correct.

4. Try the same user credentials in the *Assist Credential* dialog.

### 3. Why are my Azure/Entra Admin credentials are not working in Assist Credential dialog?

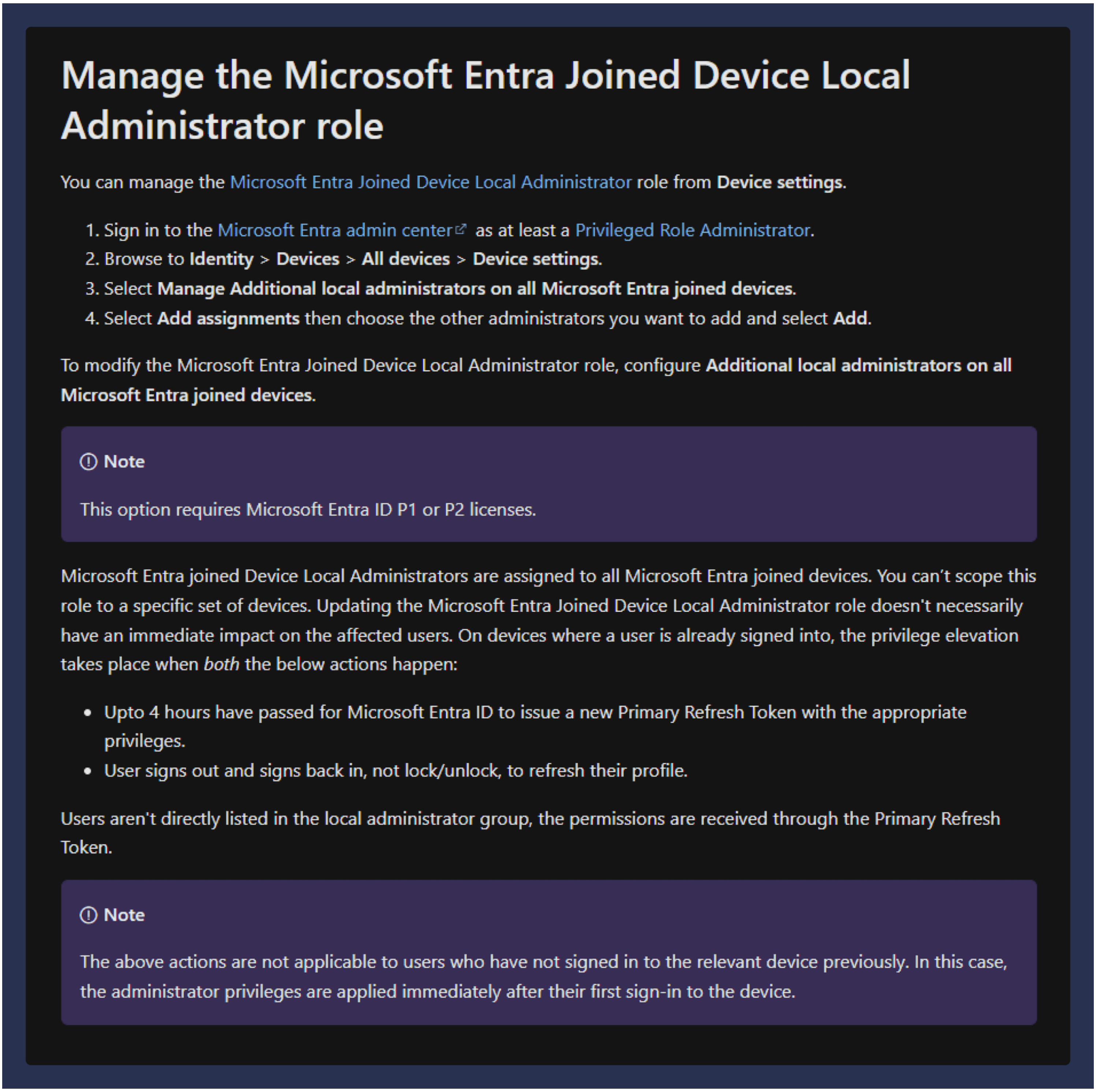
- The issue arises when Azure machines may not have pushed domain administrator accounts as local admins, resulting in "**Logon unsuccessful**" or "**The user name or password is incorrect**" error messages.

- This can be resolved via Azure by adding the **Azure domain administrators in the Local Administrators Group.**

- There are two ways in which we can achieve the above.

    i. By command line method on the remote machine (Single)
        1. Log in to the PC with the Azure AD user account you want to grant local admin privileges to. This gets the GUID onto the PC.
        2. Log out from the Azure AD user account and log in using a local admin account.
        3. Open the **Command prompt** as an administrator on the remote machine and use the below command to add the user to the Local Admin group in the machine. For example, If you had a user named "Dave Maria", the command would be "**net localgroup administrators MyAzureAD\Dave Maria /add**" (without quotes).

    ii. Azure refresh policy (Bulk) Reference link (recommended for cases where you cannot directly access the machine)



## Manage the Microsoft Entra Joined Device Local Administrator role

You can manage the Microsoft Entra Joined Device Local Administrator role from **Device settings**.

1. Sign in to the Microsoft Entra admin center as at least a Privileged Role Administrator.
2. Browse to **Identity** > **Devices** > **All devices** > **Device settings**.
3. Select **Manage Additional local administrators on all Microsoft Entra joined devices**.
4. Select **Add assignments** then choose the other administrators you want to add and select **Add**.

To modify the Microsoft Entra Joined Device Local Administrator role, configure **Additional local administrators on all Microsoft Entra joined devices**.

> ⓘ **Note**
>
> This option requires Microsoft Entra ID P1 or P2 licenses.

Microsoft Entra joined Device Local Administrators are assigned to all Microsoft Entra joined devices. You can't scope this role to a specific set of devices. Updating the Microsoft Entra Joined Device Local Administrator role doesn't necessarily have an immediate impact on the affected users. On devices where a user is already signed into, the privilege elevation takes place when *both* the below actions happen:

- Upto 4 hours have passed for Microsoft Entra ID to issue a new Primary Refresh Token with the appropriate privileges.
- User signs out and signs back in, not lock/unlock, to refresh their profile.

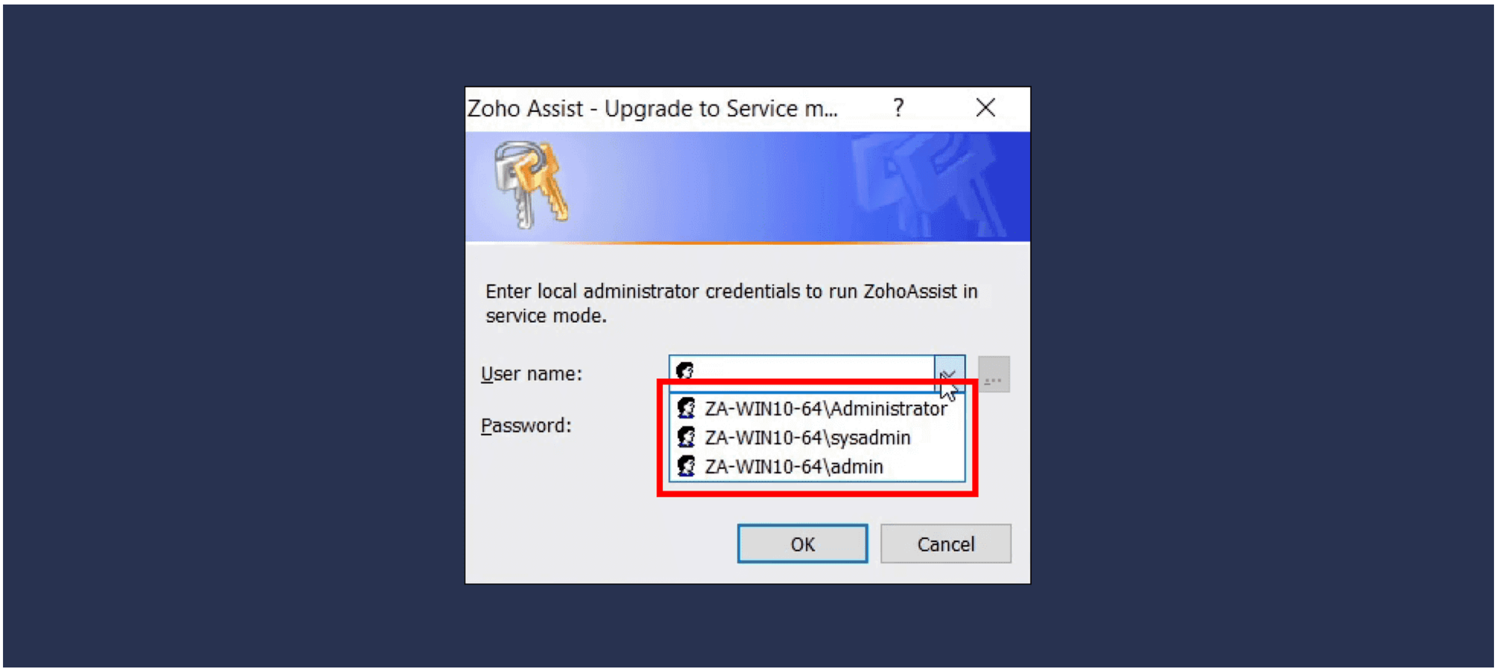
Users aren't directly listed in the local administrator group, the permissions are received through the Primary Refresh Token.

> ⓘ **Note**
>
> The above actions are not applicable to users who have not signed in to the relevant device previously. In this case, the administrator privileges are applied immediately after their first sign-in to the device.

- Follow it by restarting the machine and joining a new session in Assist. Try again to elevate with the Azure Admin credential that you have added as Local Administrator.

### 4. How do I identify the Local Admin credential of the remote machine?

1. Local administrator user accounts on the remote machine are listed in the drop-down menu of the *Prompt at customer end* credential dialog.



Zoho Assist - Upgrade to Service m...

Enter local administrator credentials to run ZohoAssist in service mode.

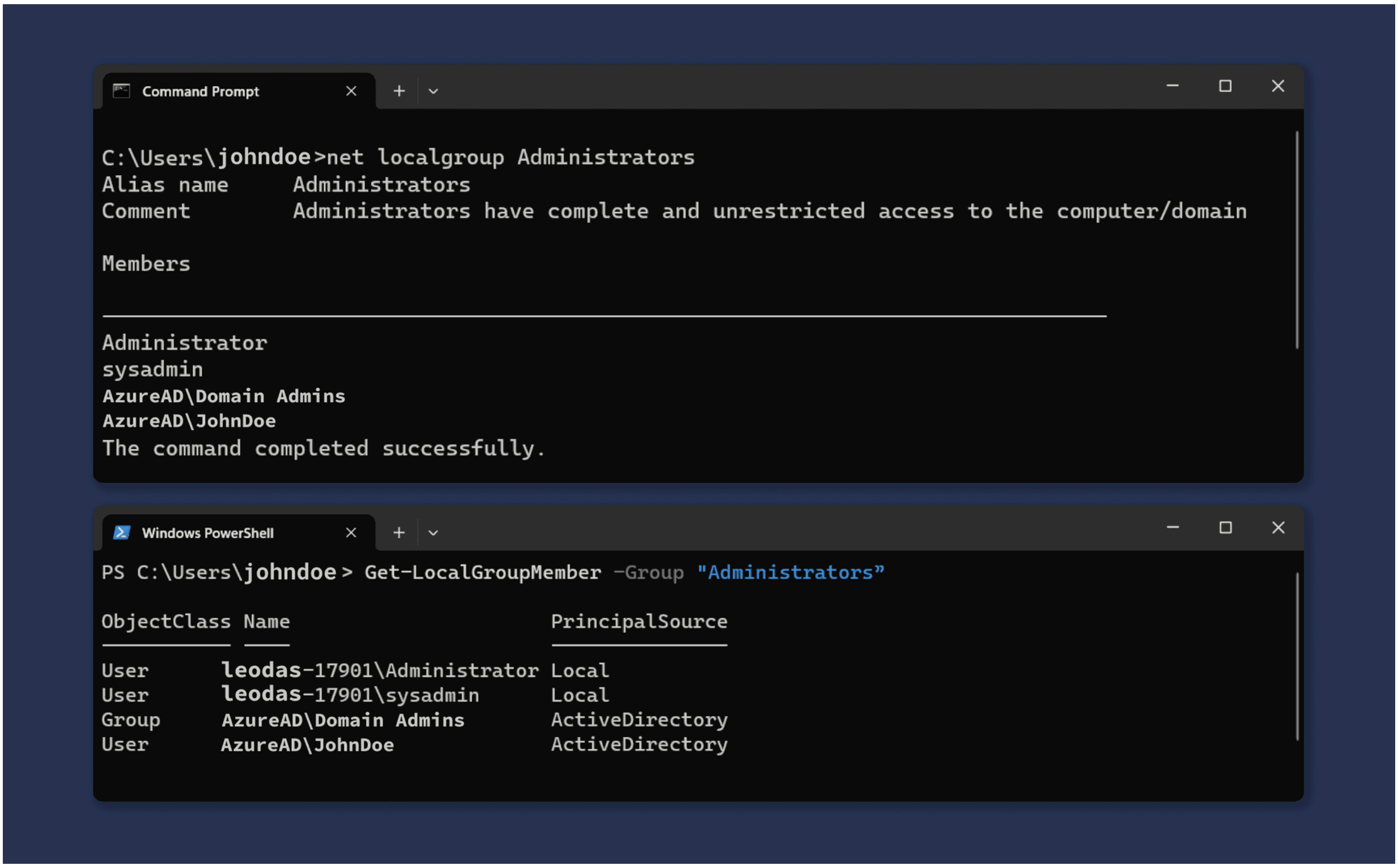
User name:

Password:

- ZA-WIN10-64\Administrator
- ZA-WIN10-64\sysadmin
- ZA-WIN10-64\admin

2. To list the local administrator accounts on the remote machine, use the following commands:

- For command prompt : **net localgroup Administrators**
- For powershell : **Get-LocalGroupMember -Group "Administrators”**



```
C:\Users\johndoe>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
sysadmin
AzureAD\Domain Admins
AzureAD\JohnDoe
The command completed successfully.
```

```
PS C:\Users\johndoe> Get-LocalGroupMember -Group "Administrators"

ObjectClass Name                         PrincipalSource
----------- ----                         ---------------
User        leodas-17901\Administrator Local
User        leodas-17901\sysadmin      Local
Group       AzureAD\Domain Admins        ActiveDirectory
User        AzureAD\JohnDoe              ActiveDirectory
```

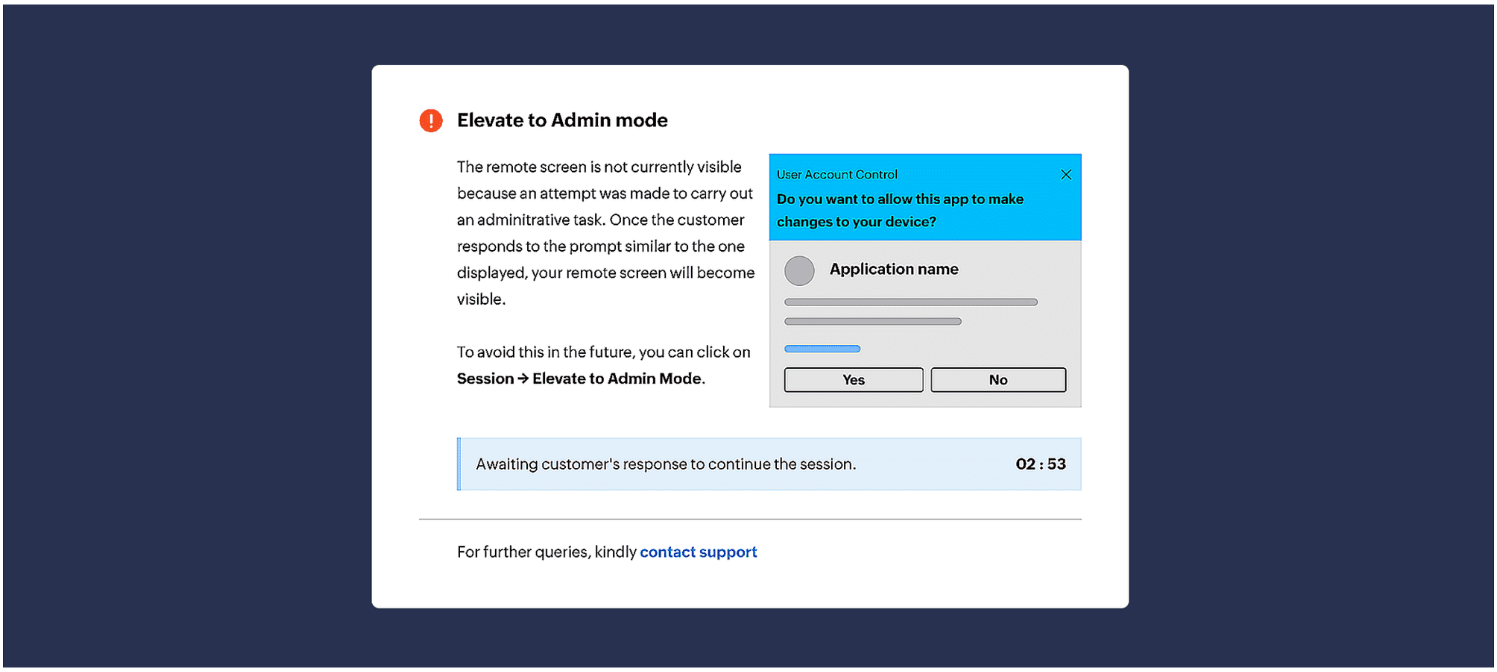
### 5. Why am I getting an error message stating "Either a required impersonation level was not provided, or the provided impersonation level is invalid"?

This occurs when the technician inputs a credential that is not a local administrator account on the remote machine. Retry with a valid admin credential.

### 6. Why am I getting an error message stating "We can't sign you in with this credential because your domain isn't available. Makesure your device is connected to your organization's network and try again. If you previously signed in on this device with another credential, you can sign in with that credential"?

Ensure that you're connected to your organization's network. The error indicates that your device needs to be on the same network as the domain controller for successful sign-in.

### 7. Why am I getting an error stating "The remote screen is not currently visible because an attempt was made to carry out an administrative task"?



**Elevate to Admin mode**

The remote screen is not currently visible because an attempt was made to carry out an adminitrative task. Once the customer responds to the prompt similar to the one displayed, your remote screen will become visible.

To avoid this in the future, you can click on **Session → Elevate to Admin Mode**.

User Account Control
Do you want to allow this app to make changes to your device?
Application name
Yes
No

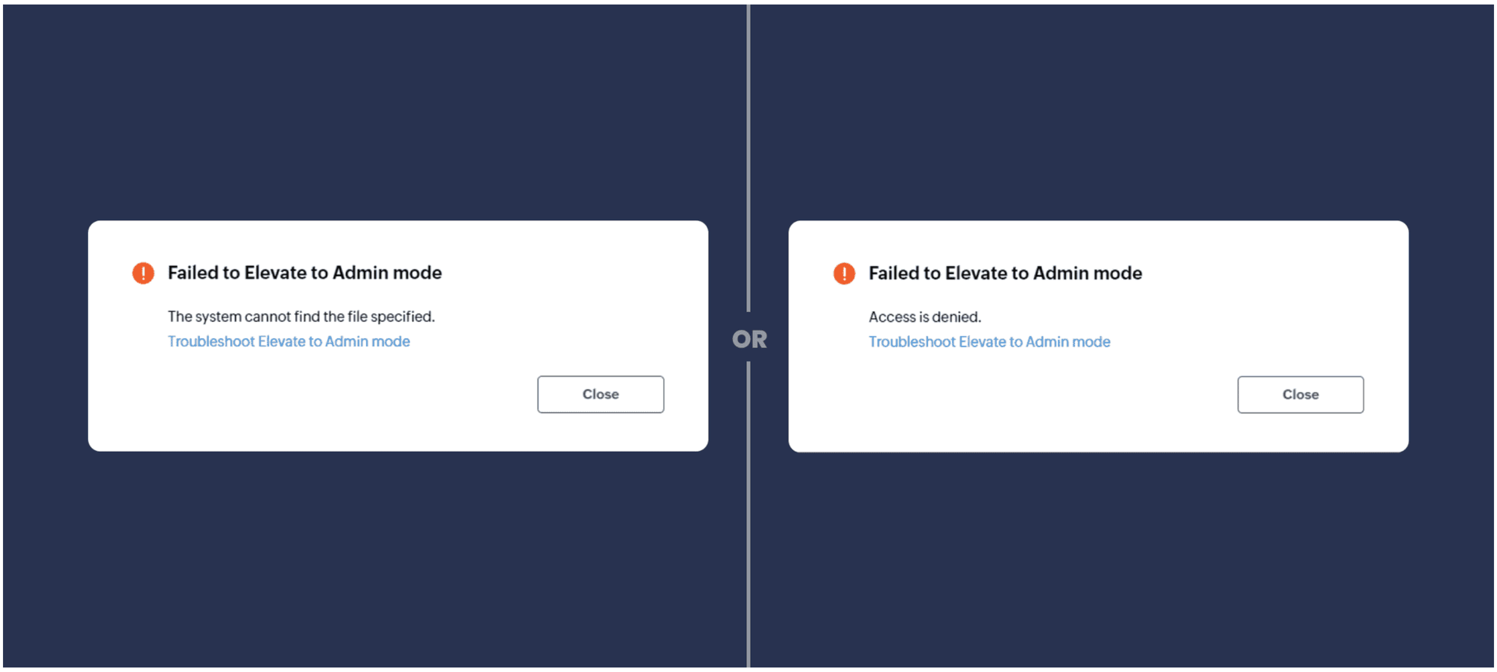
Awaiting customer's response to continue the session. **02 : 53**

For further queries, kindly contact support

- When the remote customer joins using a Windows standard user account, they do not have the administrator privilege. During a remote session, the technician may experience screen freezing when attempting for admin-level tasks such as using "Run as administrator" or accessing secure desktops like Windows UAC.
- In such cases, a Blocking Dialog appears on the technician's screen, indicating that the **customer must promptly respond to the Windows UAC consent pop-up shown remotely or the technician must wait for three minutes for the pop-up to close automatically.**

To prevent these issues and gain admin privileges for certain tasks, it is recommended to elevate the assist application using the **Session -> Elevate to Admin mode** feature.

### 8. Why did the process fail with a "The system cannot find the file specified" or "Access denied" error ?



Failed to Elevate to Admin mode

The system cannot find the file specified.

Troubleshoot Elevate to Admin mode

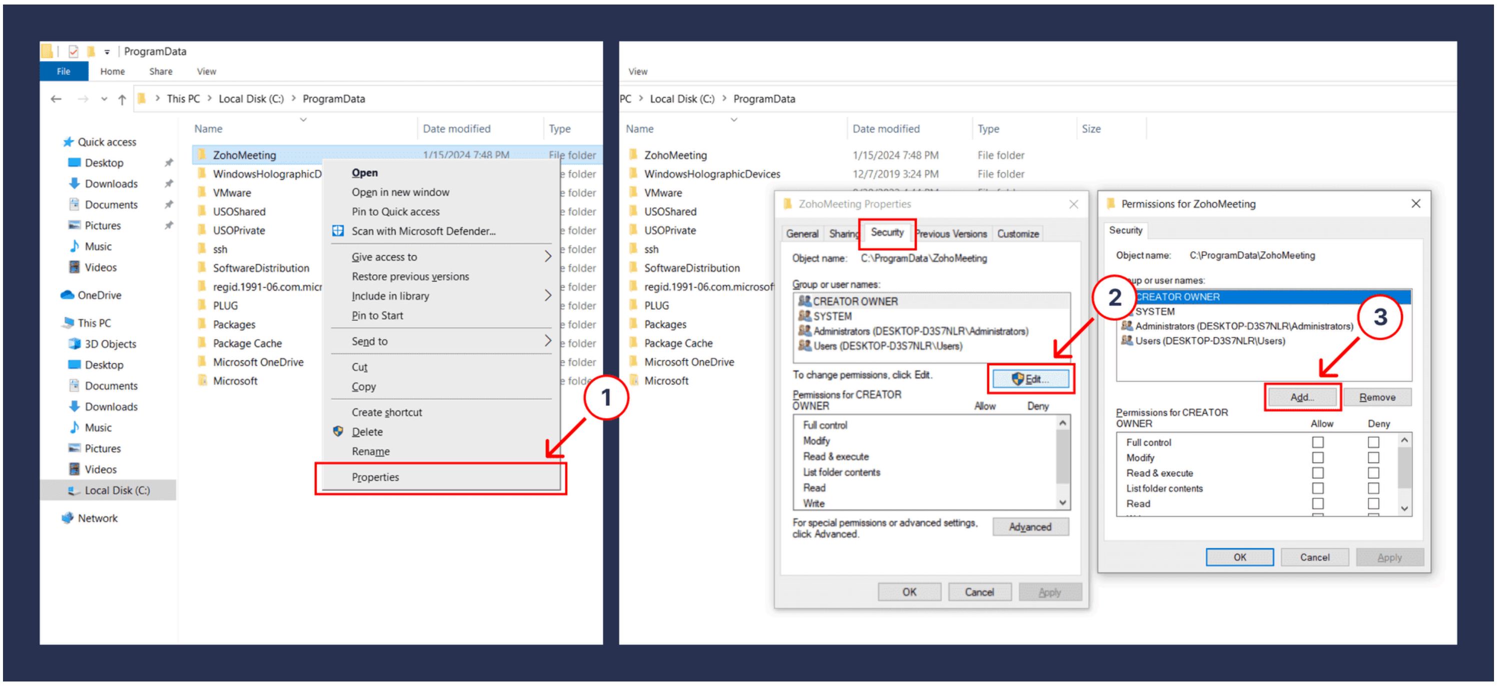
Failed to Elevate to Admin mode

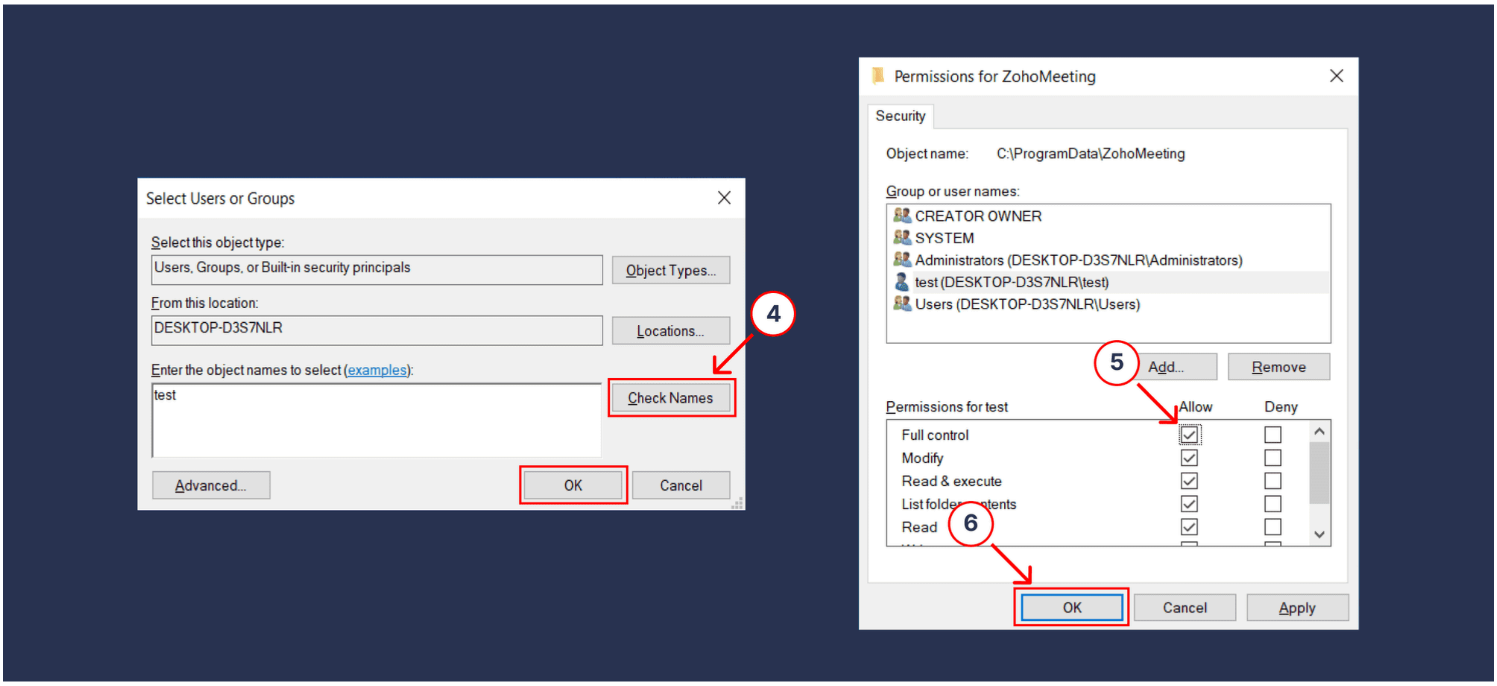
Access is denied.

Troubleshoot Elevate to Admin mode

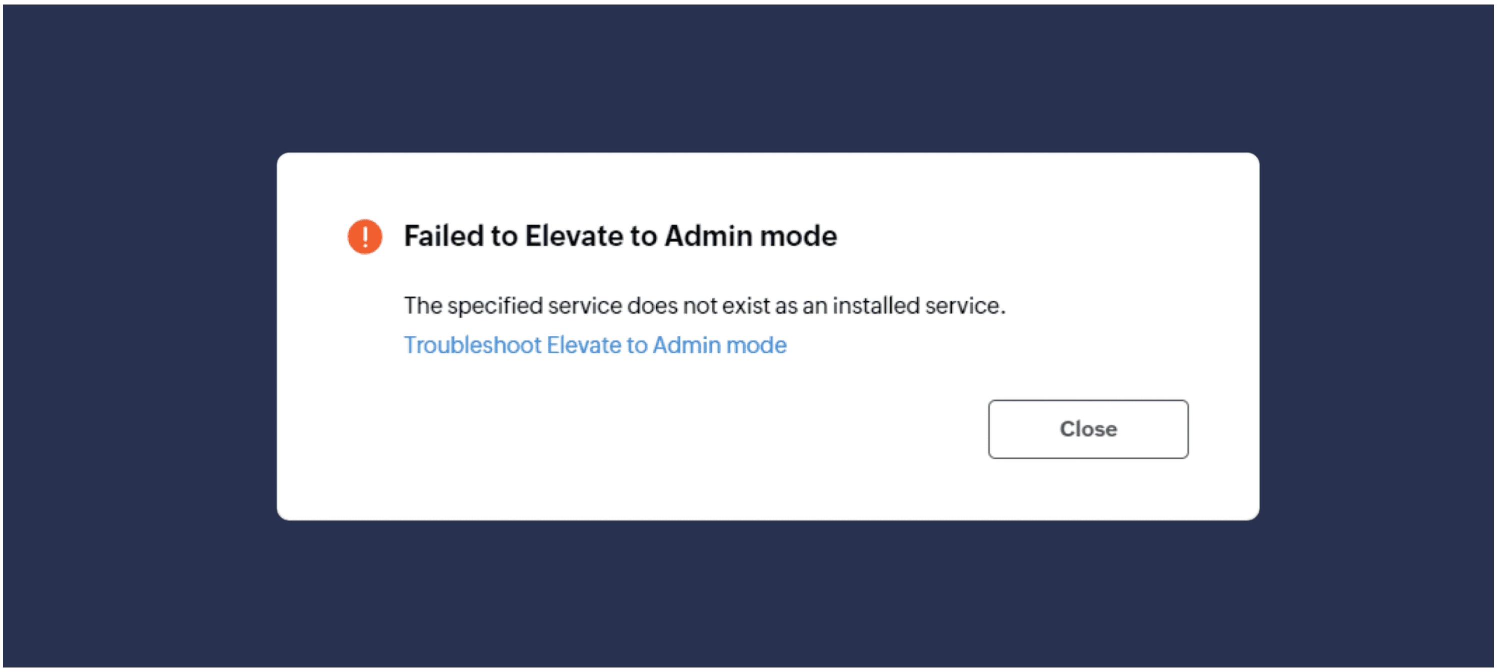
- This error occurs when the necessary folder permissions are not granted to the Windows user accounts.
- The local administrator and the current user (user account from which the customer has joined the session) doesn't have necessary permissions like (Read/Write/Modify) files to %programdata%\ZohoMeeting" folder.
- Give necessary permissions to the respective users by following the below steps

1. Navigate to **Start** -> **Run**, Type "**%programdata%\ZohoMeeting**", and click **OK**. Right-click on the folder and select **Properties**.
2. Access the **Security** tab and click **Edit**.
3. Choose the user account for which you need to enable permission from the list. If not listed, click **Add**.
4. Manually enter the username in the text area and click **Check Names** to display a list of user accounts containing the specified substring.
5. Select the desired user account from the list and enable the **Full control** checkbox under the *Allow* section.
6. Click **OK** to apply the permission changes.





## 9. Why did the process fail with a "The specified service does not exist as an installed service" error ?



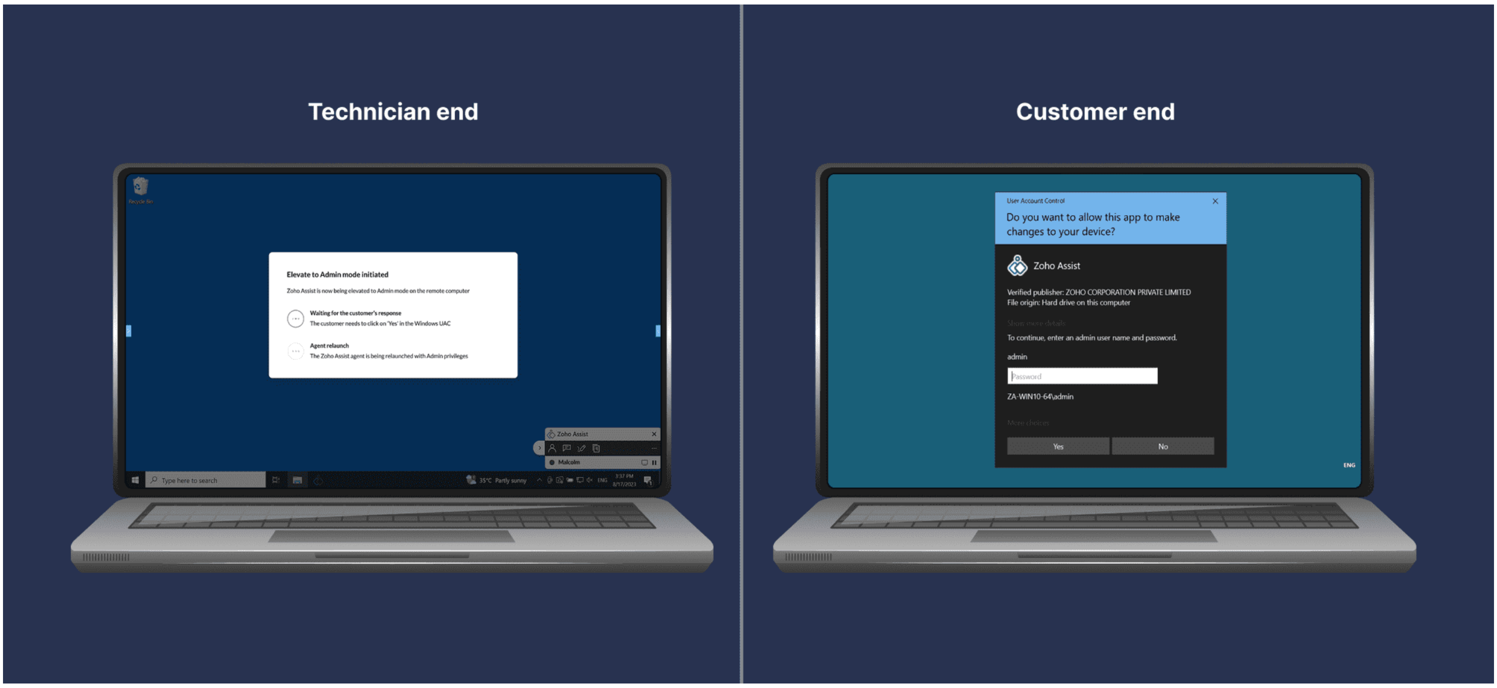
Failed to Elevate to Admin mode

The specified service does not exist as an installed service.

Troubleshoot Elevate to Admin mode

- The above dialog box implies that the elevation has been initiated successfully by validating the admin credentials, but the service installation has failed during the run time.
- Contact support with logs and screenshots to get it resolved **(Follow step 12)**.

### 10. Why is the UAC dialog shown with a password field at the customer end?



Elevate to Admin mode initiated

Zoho Assist is now being elevated to Admin mode on the remote computer

Waiting for the customer's response

The customer needs to click on 'Yes' in the Windows UAC

Agent relaunch

The Zoho Assist agent is being relaunched with Admin privileges

User Account Control

Do you want to allow this app to make changes to your device?

Zoho Assist

Verified publisher: ZOHO CORPORATION PRIVATE LIMITED
File origin: Hard drive on this computer

To continue, enter an admin user name and password.

admin

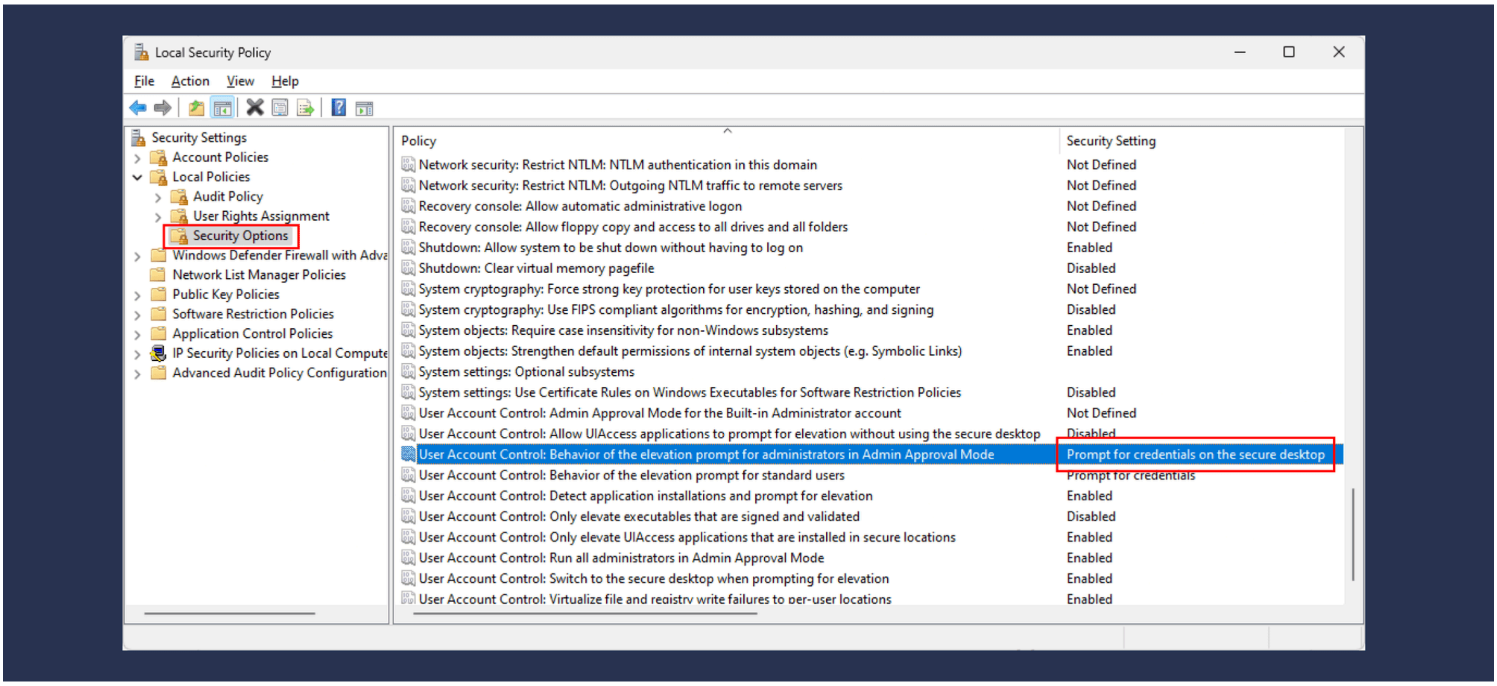
Password

ZA-WIN10-64\admin

This is due to the local security policy set by your system administrator.
To change the policy,

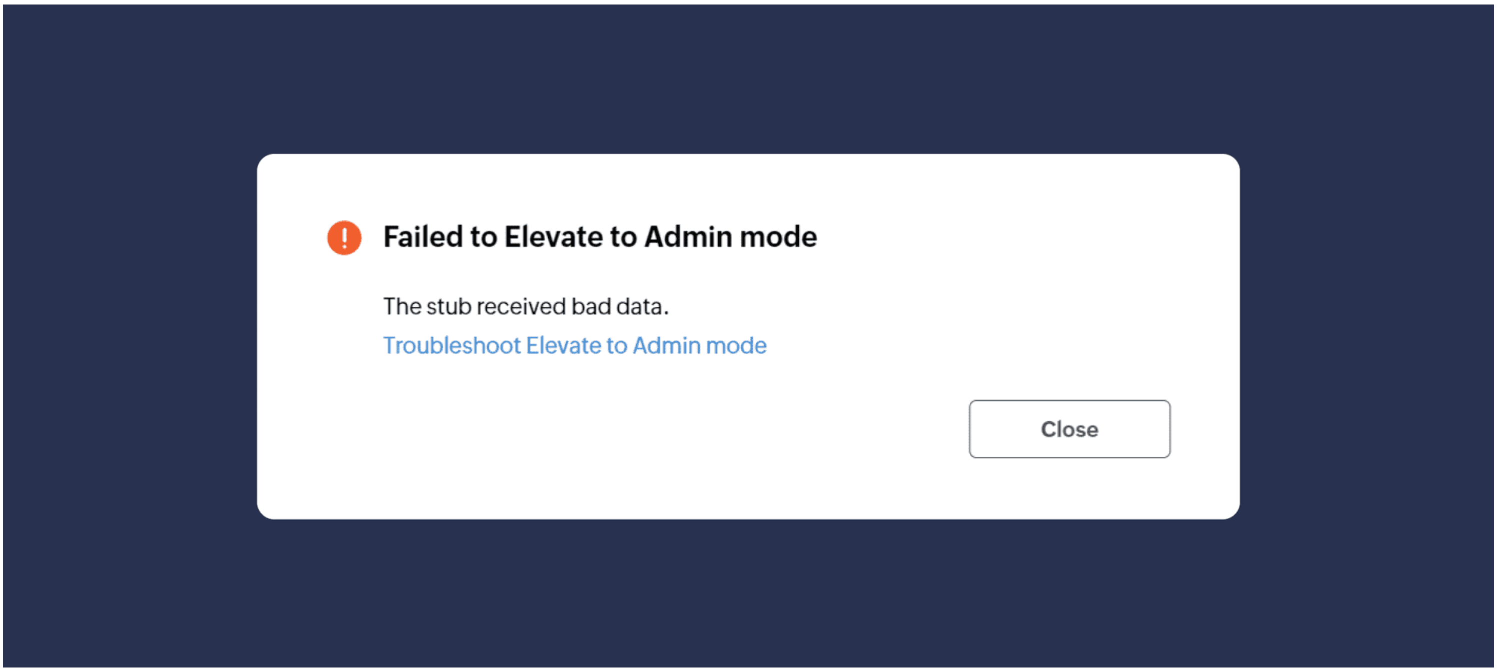
1. Click Start, then type "Local Security Policy".
2. Navigate to *Security Options*, as shown in the below image.

3. Change the "**User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode"** policy to "**Prompt for consent on the secure desktop"**.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

| Policy | Security Setting |
|---|---|
| Network security: Restrict NTLM: NTLM authentication in this domain | Not Defined |
| Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers | Not Defined |
| Recovery console: Allow automatic administrative logon | Not Defined |
| Recovery console: Allow floppy copy and access to all drives and all folders | Not Defined |
| Shutdown: Allow system to be shut down without having to log on | Enabled |
| Shutdown: Clear virtual memory pagefile | Disabled |
| System cryptography: Force strong key protection for user keys stored on the computer | Not Defined |
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Disabled |
| System objects: Require case insensitivity for non-Windows subsystems | Enabled |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled |
| System settings: Optional subsystems | |
| System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies | Disabled |
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Not Defined |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode | Prompt for credentials on the secure desktop |
| User Account Control: Behavior of the elevation prompt for standard users | Prompt for credentials |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Disabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

### 11. Why did the process fail with a "The stub received bad data" error?



Failed to Elevate to Admin mode

The stub received bad data.

Troubleshoot Elevate to Admin mode

This error occurs when the technician provides credentials without a domain name. To resolve this kindly ensure that the credentials are provided in one of the below specified formats.

- **<domain>\username**
- **<machine_name>\username**
- **username@domain**

### 12. If you are unable to troubleshoot yourself, you can contact support with the necessary data as follows:

1. Screenshot the exact error message encountered during the process of elevation.
2. Zip the necessary logs from the remote machine
    1. Navigate to Start -> Run, then type "%localappdata%\ZohoMeeting\".
    2. Right-click on the folder named "log" & choose **Compress to zip**.
    3. Navigate to Start -> Run, then type "%programdata%\ZohoMeeting\".
    4. Right-click on the folder named "log" and choose **Compress to zip**.

Email all these files to our support team at support@zohoassist.com.