Zoho Corporation

# Elevate to Admin mode on Windows OS

Table of contents

During a remote session, attempting to perform admin-level operations, such as using Run as administrator or accessing any secure desktops like Windows UAC through the session,  may cause screen freezing for technicians. To perform these tasks and gain admin privileges, the assist application must be elevated using the **Elevate to Admin mode** option.

## Session Elevation Methods

There are two primary methods to elevate a session to Admin mode:

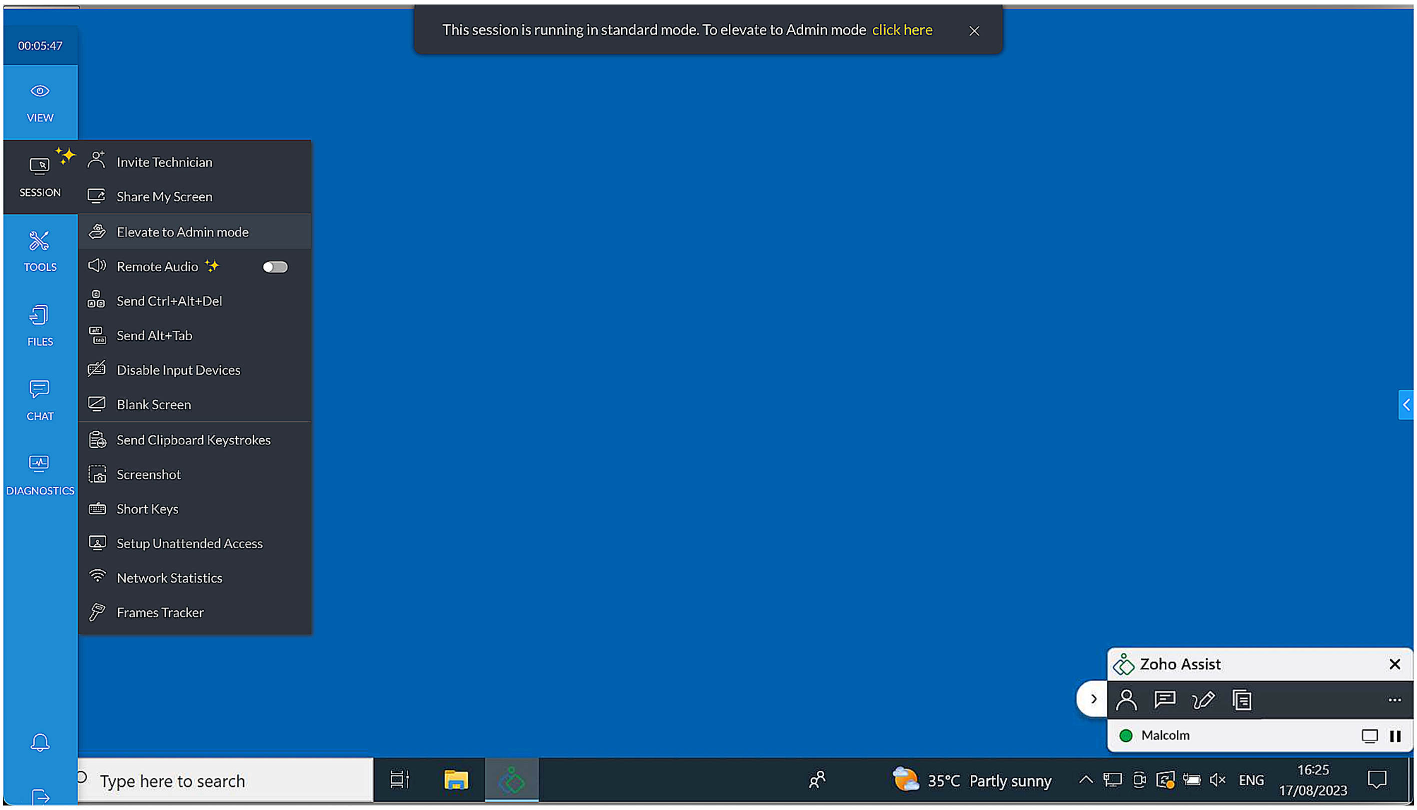
Technician-Side Elevation: In this method, the Technician initiates the elevation process and enters Admin credentials.
End User Elevation: This method involves prompting the customer to enter Admin credentials from their end**.**

### *Technician-Side Elevation*

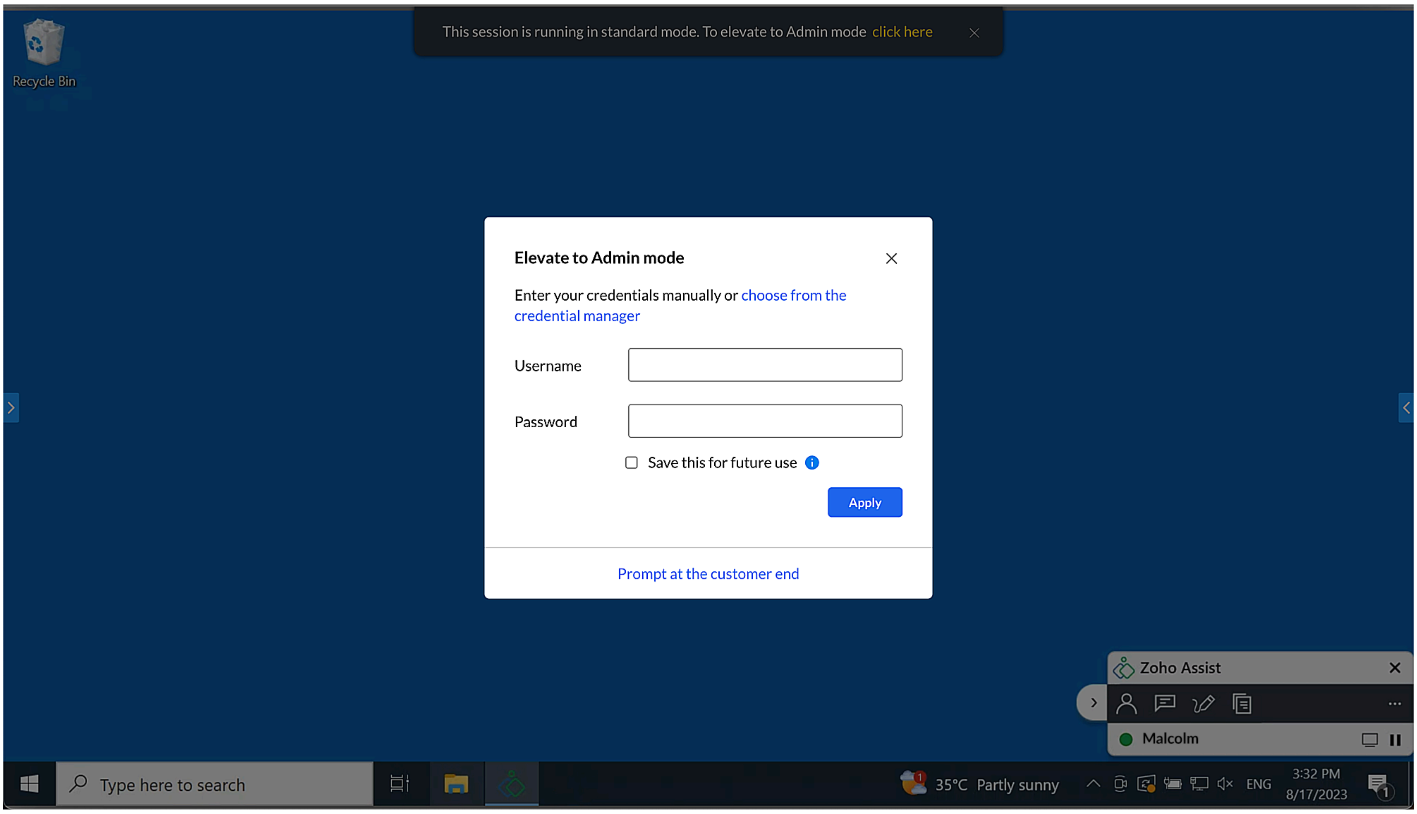
#### Elevate to Admin mode by entering the credentials manually

During an active remote session,

1. Navigate to **Session > Elevate to Admin Mode.**


This session is running in standard mode. To elevate to Admin mode click here

2. Enter the credentials manually in the prompt as shown below and click Apply.


This session is running in standard mode. To elevate to Admin mode click here

Elevate to Admin mode

Enter your credentials manually or choose from the credential manager

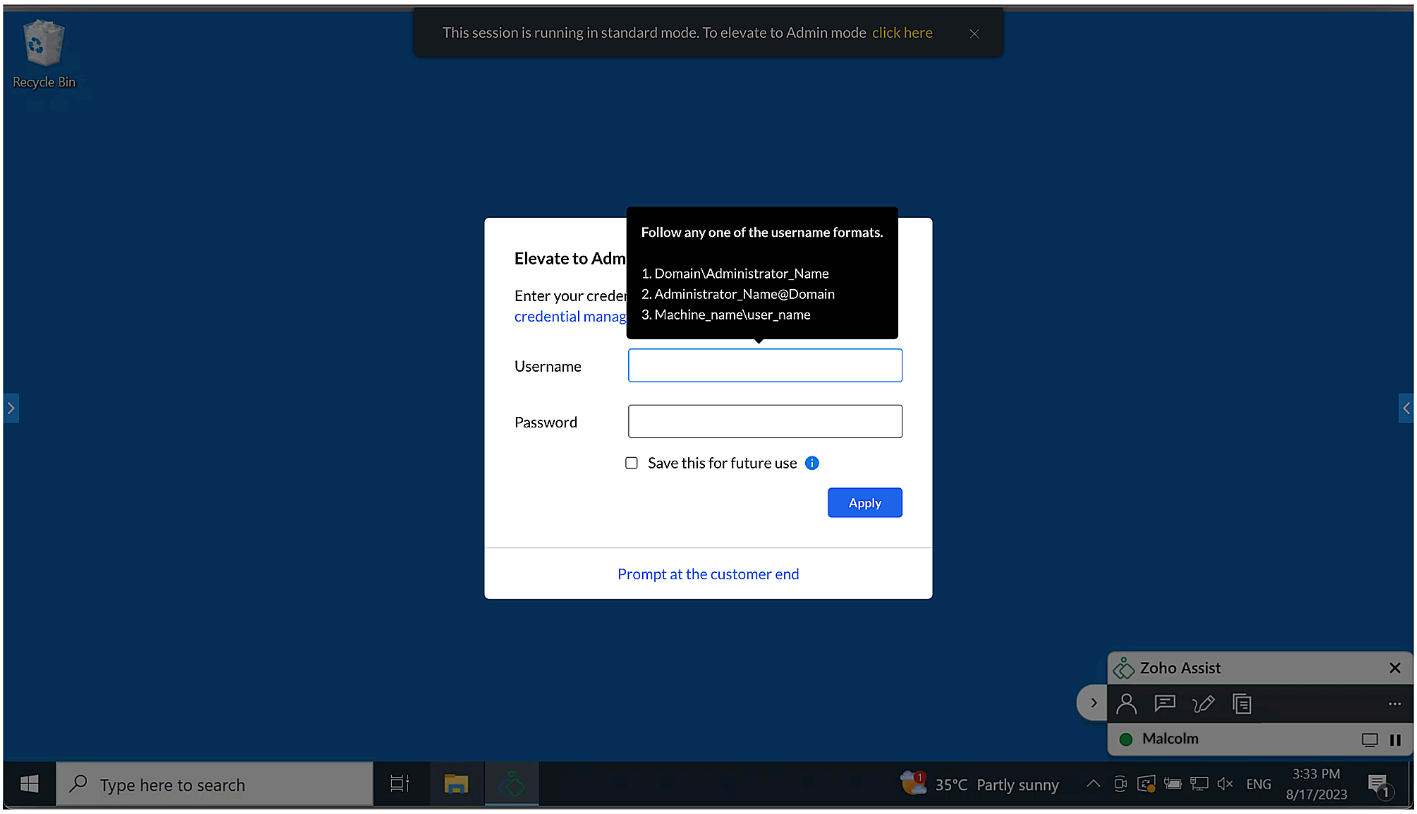
Username

Password

□ Save this for future use

3. The entered Admin credentials should be in one of the following formats:
   - **<domain>\username**
   - **<machine_name>\username**
   - **username@domain**

   Optionally, you can choose to save these credentials in Credential Manager for future use by checking the **Save this for future use** option.



This session is running in standard mode. To elevate to Admin mode click here

Elevate to Adm

Enter your creden

credential manag

Follow any one of the username formats.

1. Domain\Administrator_Name
2. Administrator_Name@Domain
3. Machine_name\user_name

Username

Password

□ Save this for future use

Apply

Prompt at the customer end

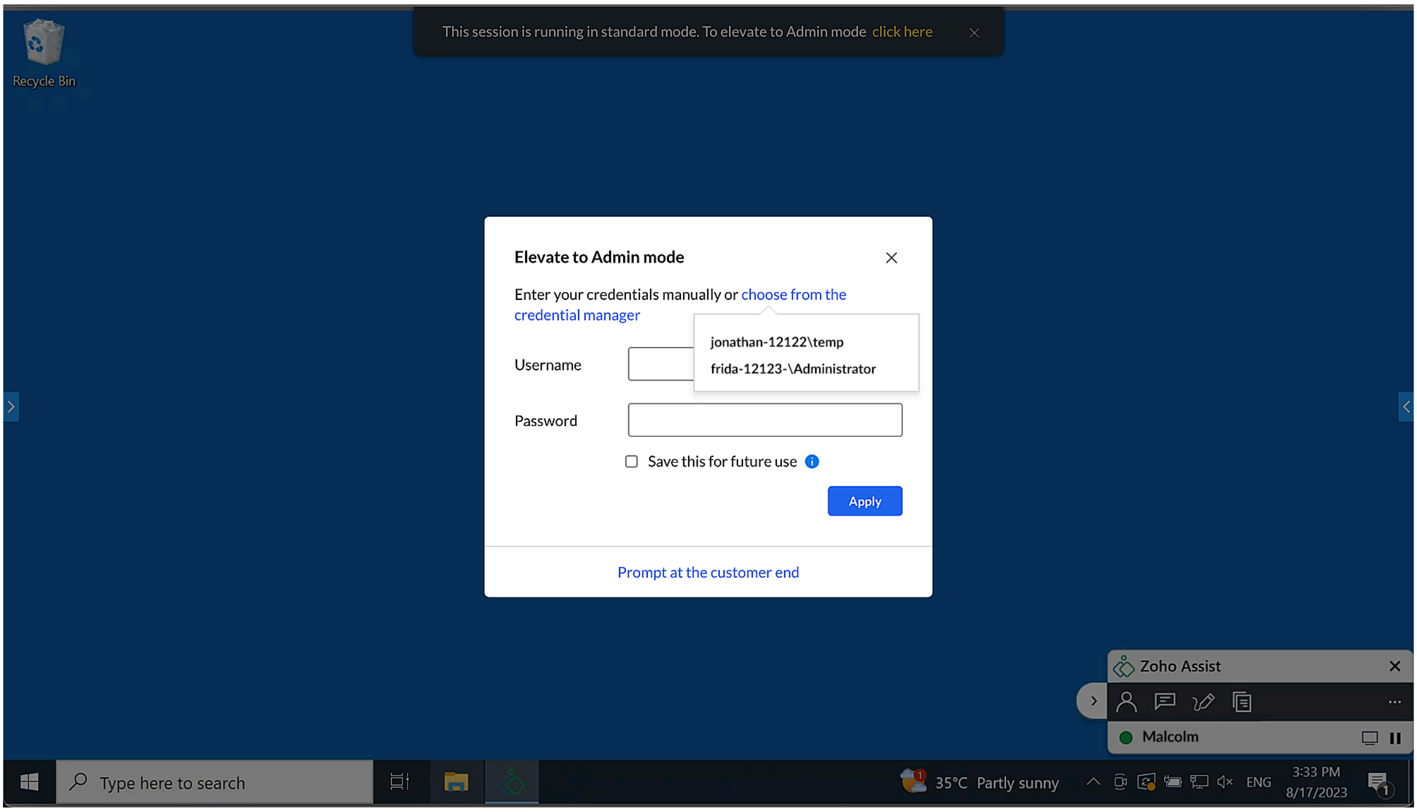
Note that credentials will only be saved if they're successfully validated on the customer's device.

## Elevate to Admin mode by using the Credential Manager

Alternatively, you can also use the credentials using the Credential Manager.
During an active remote session,

1. Navigate to S**ession** > **Elevate to Admin Mode.**
2. Click **Choose** from the Credential Manager to choose the saved credentials.

3. Select the appropriate credentials from the Credential Manager and click **Apply**.



This session is running in standard mode. To elevate to Admin mode click here

Elevate to Admin mode

Enter your credentials manually or choose from the credential manager

Username: jonathan-12122\temp / frida-12123-\Administrator

Password:

□ Save this for future use

[Learn more about the Credential Manager](#)

## *End User Elevation*

The elevation API supports the following authentication mechanisms:

- Local Admin User Authentication
- Physical/Virtual Smartcard Admin User Authentication (in remote machine)

> Note: Operating systems prior to Windows Vista support only Local Admin User Authentication.

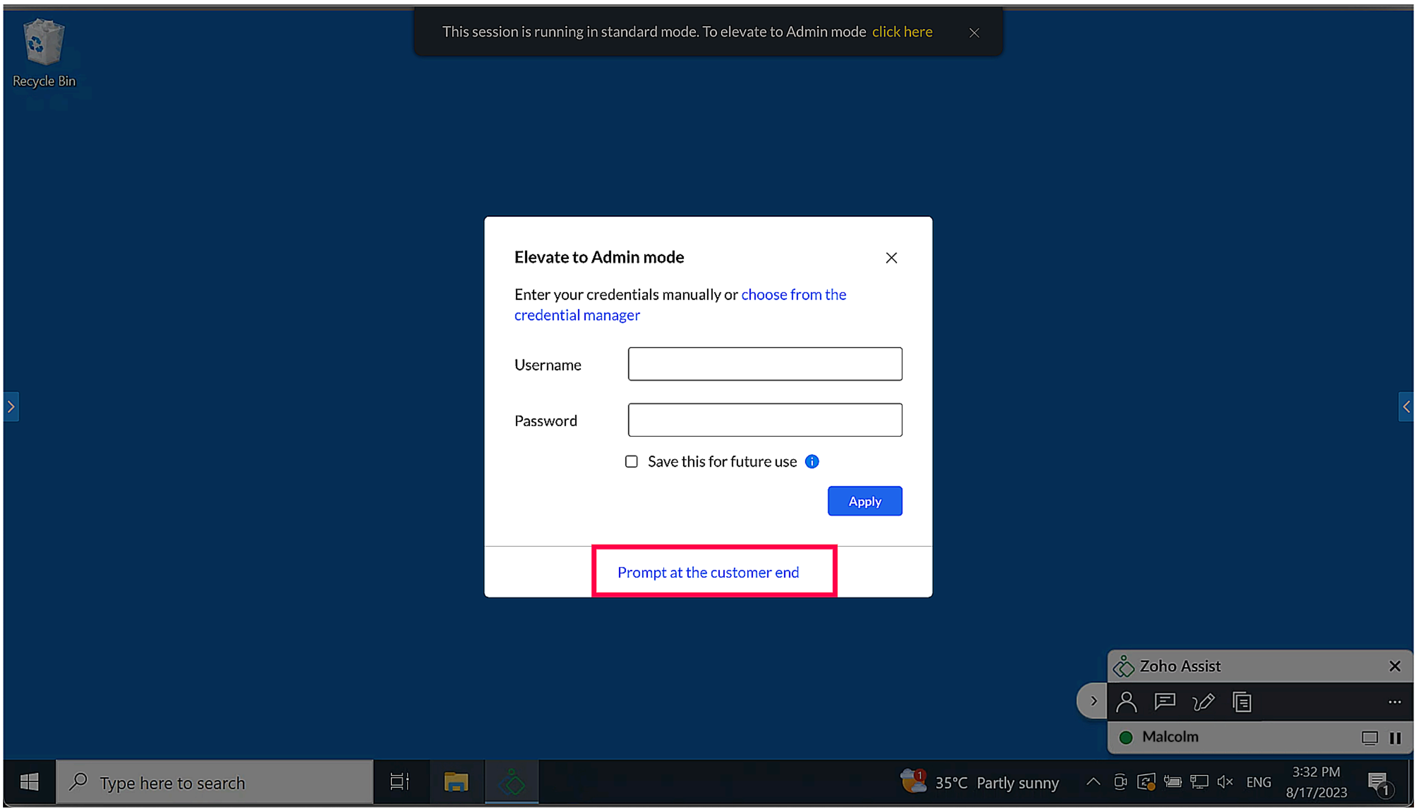
### Things to note before elevation

The user credential provided in the Assist UAC dialog must be a member of the Windows Administrator group. You must have access to %localppdata%, %programdata% & %programfiles (x86)% folder path with Read/Write/Execute/Modify permissions.

[Learn more about detailed troubleshooting steps.](#)

### *Local Admin User Authentication*

1. Once the technician console opens up, go to **Session** > **Elevate to Admin mode.**
2. To elevate to Admin mode on the customer end, the Technician can click on the Prompt at the customer end where the customer can enter the credentials.



This session is running in standard mode. To elevate to Admin mode click here

Elevate to Admin mode

Enter your credentials manually or choose from the credential manager

Username

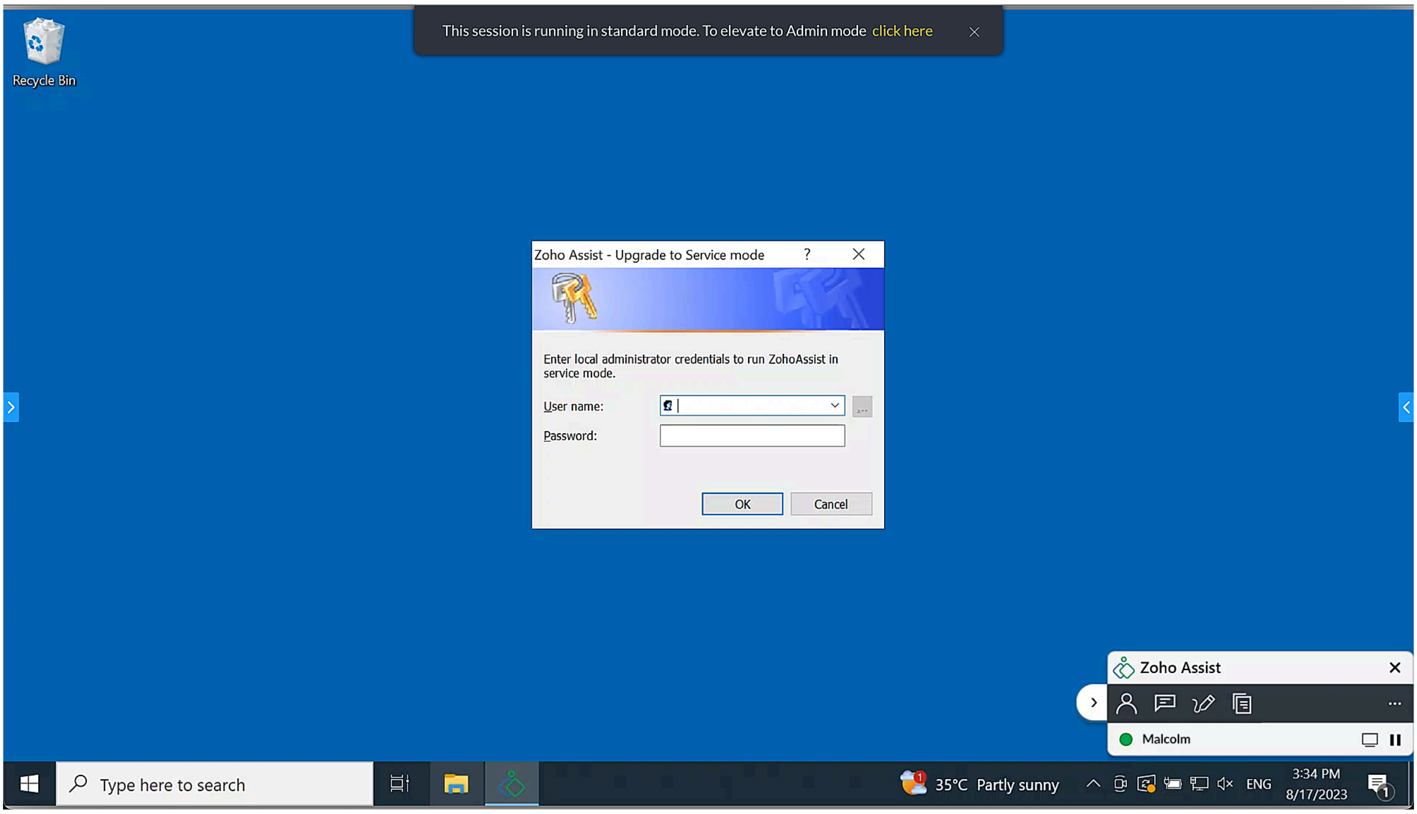
Password

□ Save this for future use

Apply

Prompt at the customer end

3. A prompt will open on the remote device. The customer or technician can enter the remote computer's credentials. The technician will provide the local admin credential via Assist UAC.



This session is running in standard mode. To elevate to Admin mode click here

Zoho Assist - Upgrade to Service mode

Enter local administrator credentials to run ZohoAssist in service mode.

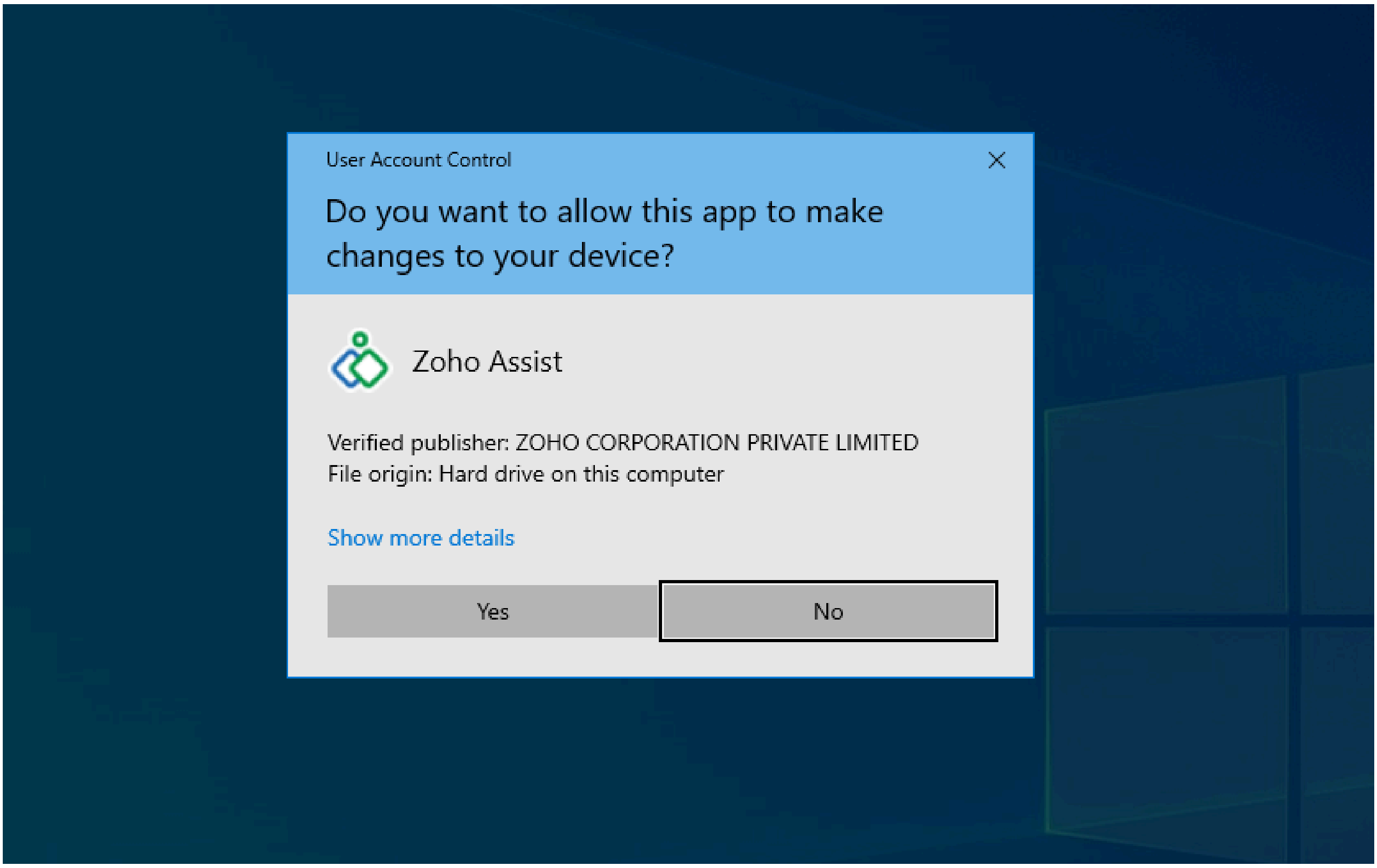
User name:

Password:

OK Cancel

4. The technician needs to choose the pre-populated local admin names from the drop-down box or enter the local administrator credentials in the Assist UAC in the following format:
   a. **<domain>\username**
   b. **<machine_name>\username**
   c. **username@domain**

5. If the proper credentials have been provided, they'll be validated against the Windows authentication mechanism, followed by the Windows UAC consent pop-up at the remote end as shown below. The end user needs to select Yes thereby approving to proceed further.



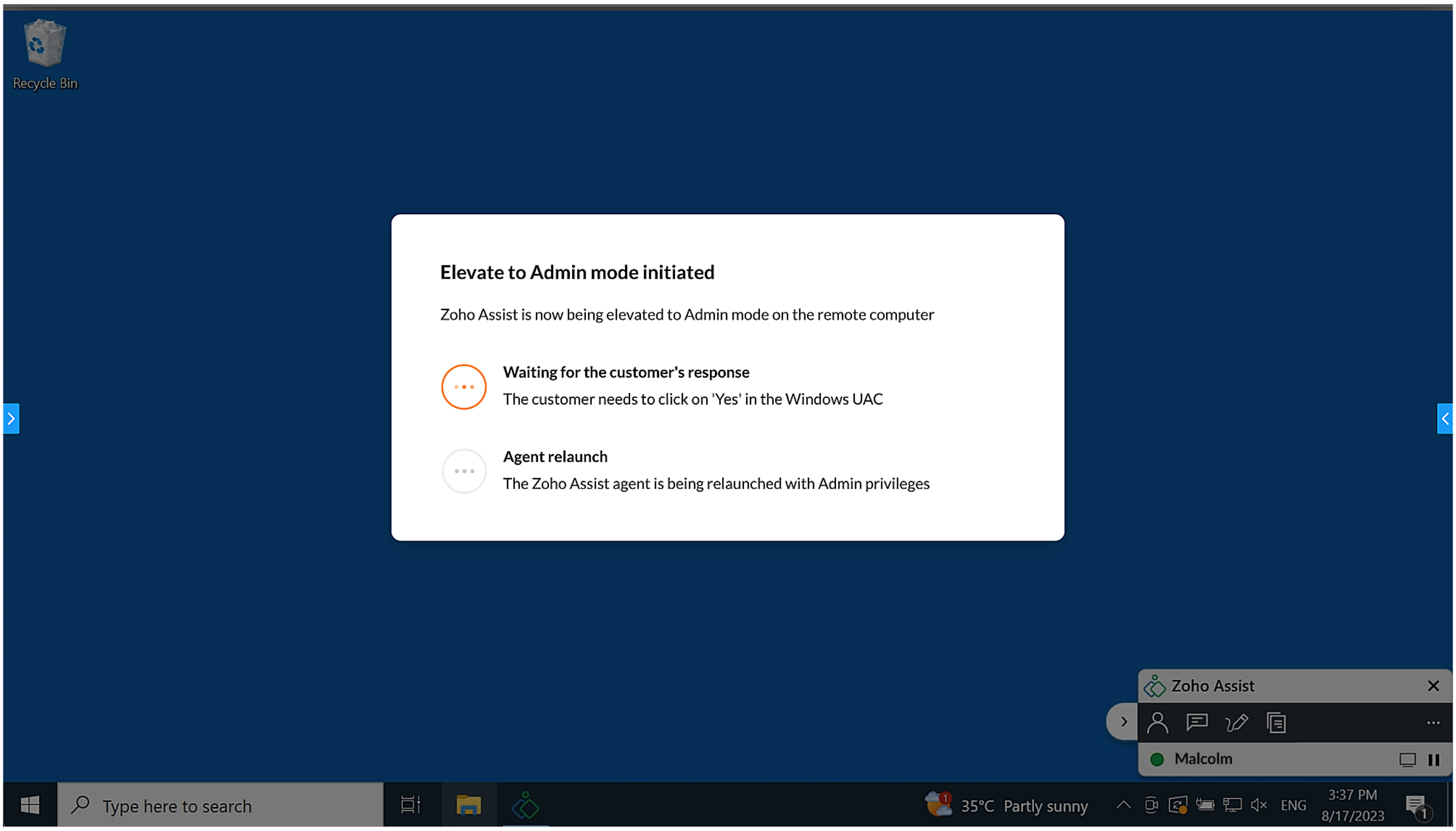
User Account Control

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

Simultaneously, the technician's screen will display the elevation status as shown below.



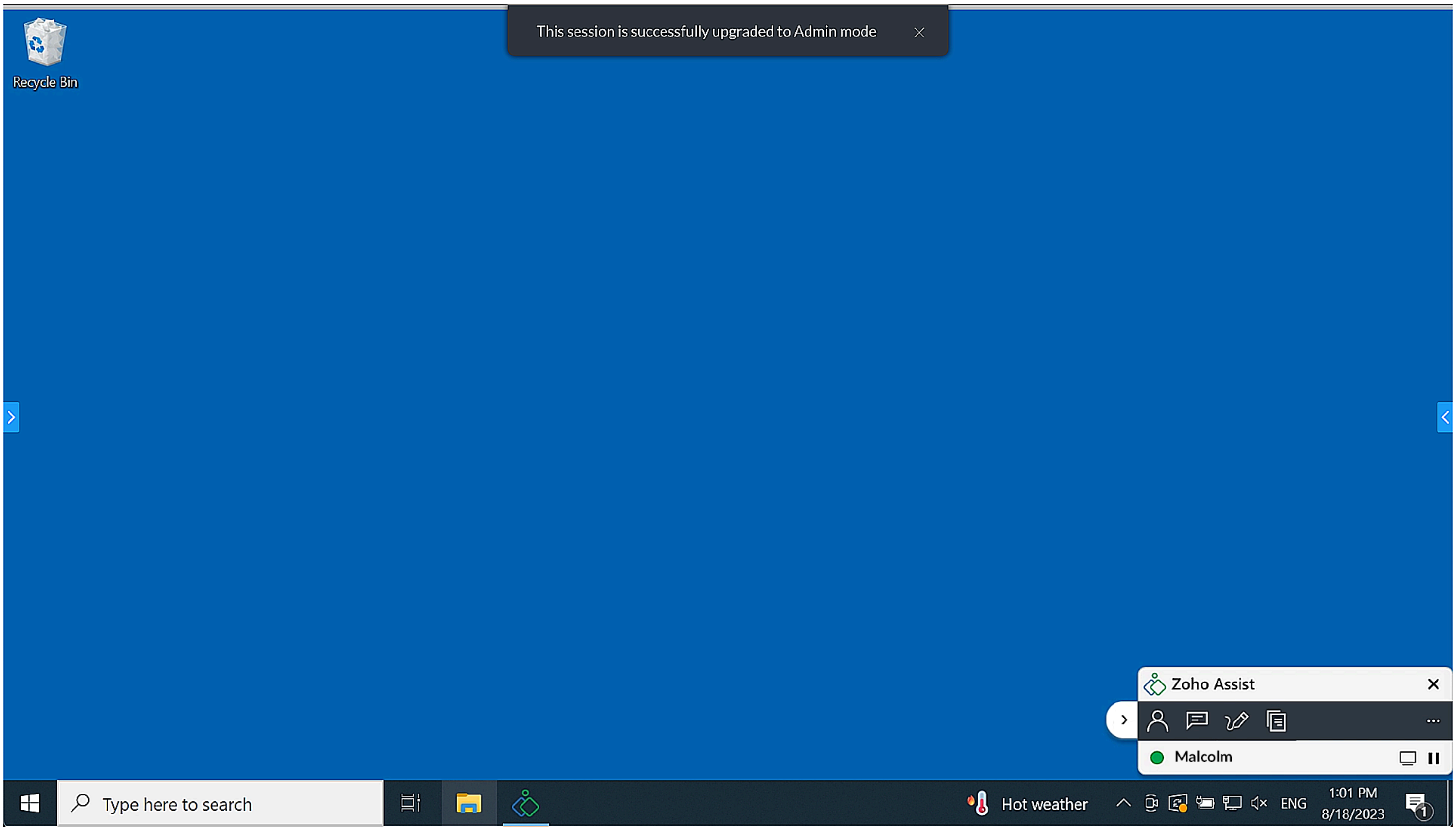
**Elevate to Admin mode initiated**

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

Once the Admin mode elevation is successful, a notification will be shown on the technician end as shown below.



This session is successfully upgraded to Admin mode

**Note:**
**If the customer joins the session using an admin account, there's no need to provide the account credentials when the technician attempts to elevate the session. Instead, a UAC window will be shown as below for customer's approval. If the customer clicks YES, the session will automatically be initiated in the admin mode. If customer clicks NO, the session will commence in standard user mode and may need elevation if there are any admin-privileged tasks.**

### Smart Card

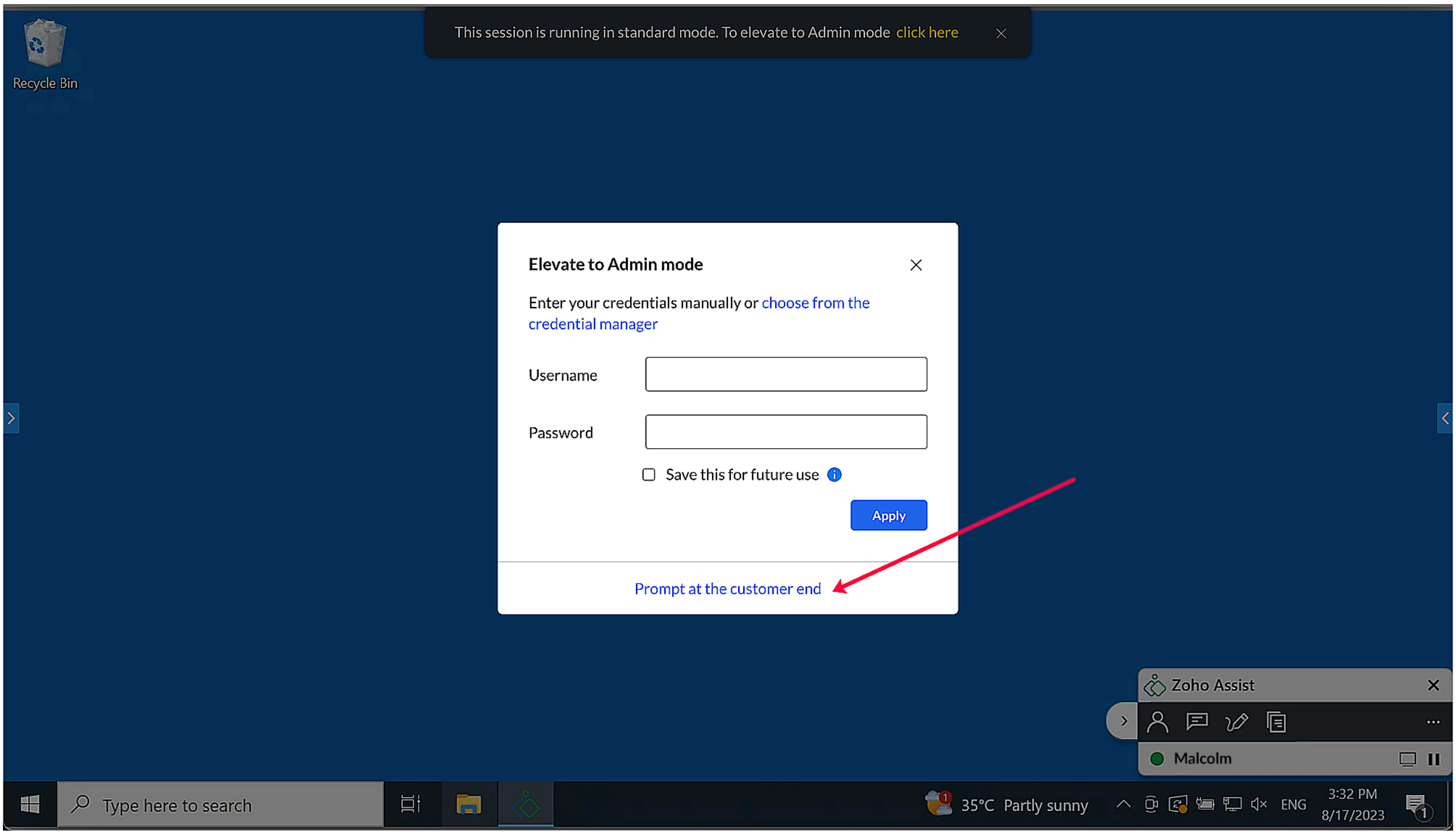
Smart cards are portable storage devices that enhance security by authenticating clients, signing code, securing email, and allowing Windows domain account login. They also protect private keys and personal information through tamper-resistant storage.

### Physical smart card and virtual smart card

| Physical smart card | Virtual smart card |
|---|---|
| Protect private keys by using smart card media. | Protect private keys by using the TPM of the computer. |
| The smart card must be configured on the remote device and inserted into the smart card reader before it can be used. | Virtual configuration must be done in the remote device via TPM. |

## Smart Card Authentication

To elevate Assist using smart card Admin credentials, select **prompt at the customer end** on the technician side.



This session is running in standard mode. To elevate to Admin mode click here

**Elevate to Admin mode**

Enter your credentials manually or choose from the credential manager

Username

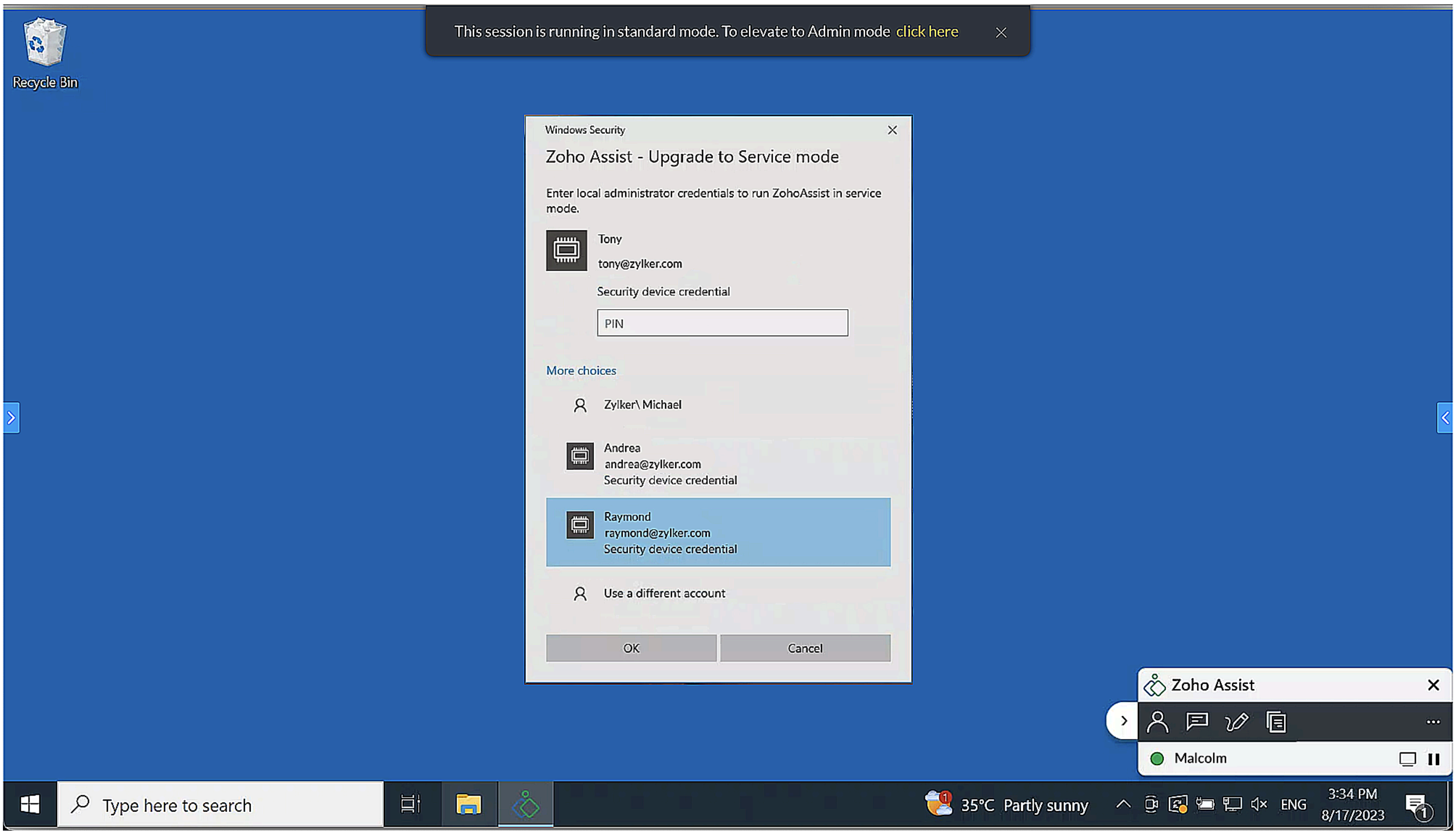
Password

□ Save this for future use

Apply

Prompt at the customer end

Select the smart card username option in the list, then enter the respective pin.



This session is running in standard mode. To elevate to Admin mode click here

Windows Security

Zoho Assist - Upgrade to Service mode

Enter local administrator credentials to run ZohoAssist in service mode.

Tony
tony@zylker.com
Security device credential

PIN

More choices

Zylker\ Michael

Andrea
andrea@zylker.com
Security device credential

Raymond
raymond@zylker.com
Security device credential

Use a different account

OK Cancel