

Domain 04 Demo 06

Configuring Logon Hours in Active Directory

Objective: To configure the Logon hours in the Active Directory for enhancing security and access control using Attribute-Based Access Control (ABAC)

Tools required: Windows Server 2022

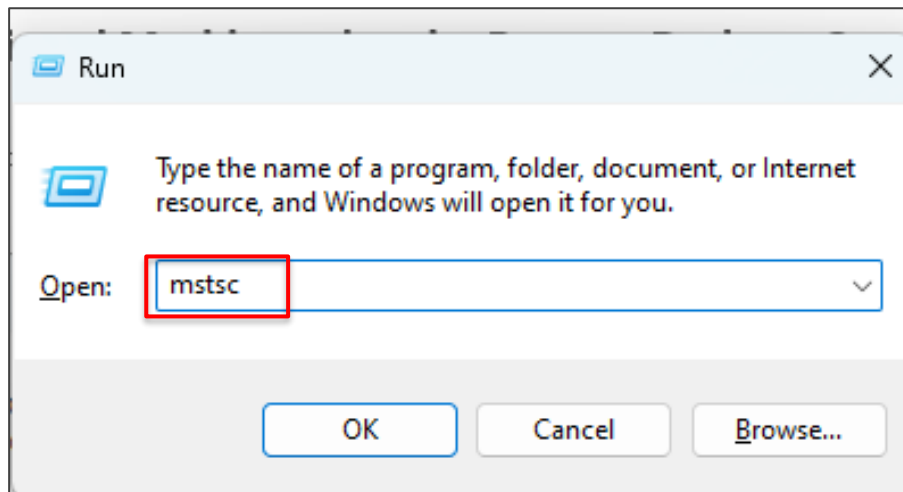
Prerequisites: Windows Server 2022 with Active Directory installed

Steps to be followed:

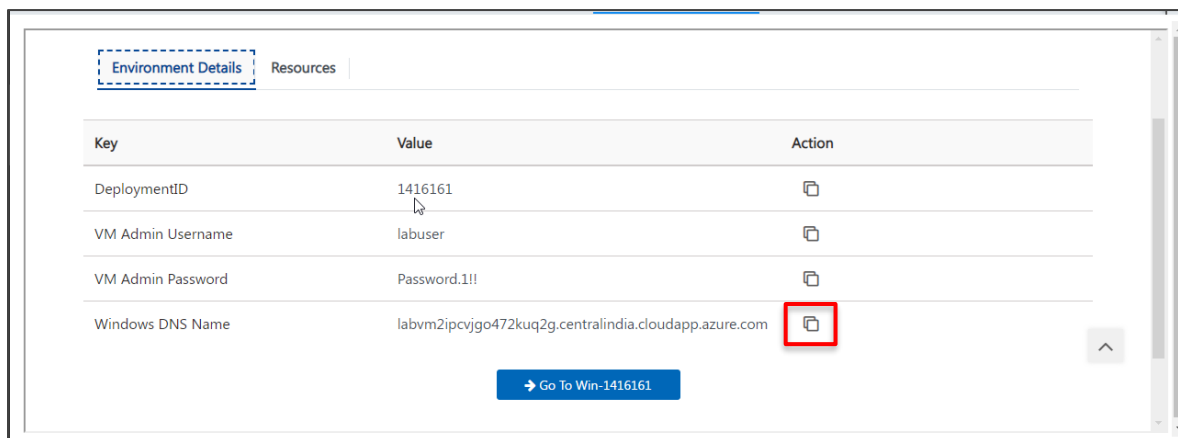
1. Open a virtual machine using the remote desktop connection
2. Open Active Directory Users and Computers (ADUC)
3. Create and locate the user account
4. Configure the Logon hours
5. Apply and close the Logon Hours window

Step 1: Open a virtual machine using the remote desktop connection

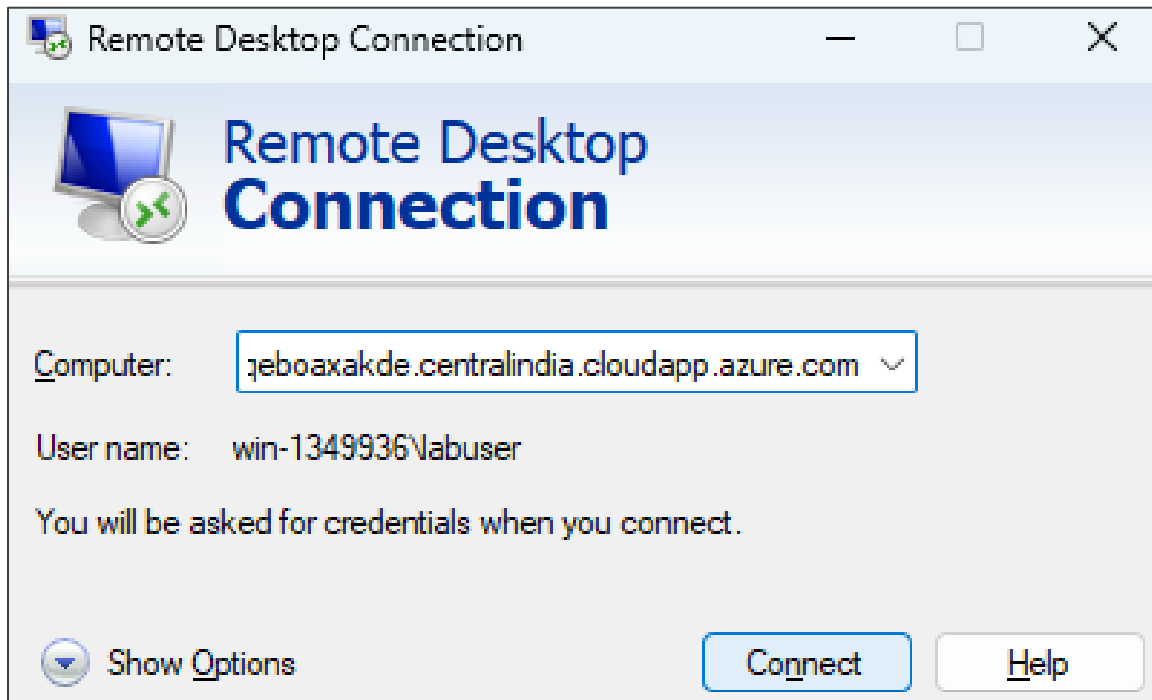
- 1.1 In your Windows Server 2022 lab, open the **Run** dialog box, type **mstsc**, and press **OK** to open the Remote Desktop Connection application



- 1.2 Copy the **Windows DNS Name** of your lab

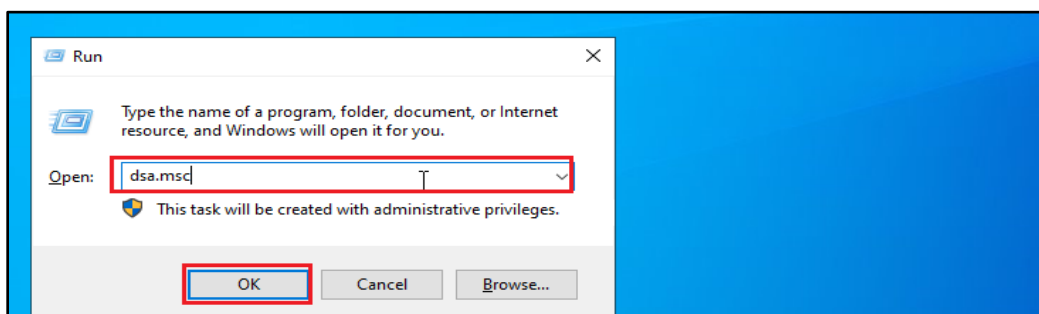


- 1.3 Paste the copied DNS name in the **Computer** field, click on **Connect**, and log in with appropriate credentials

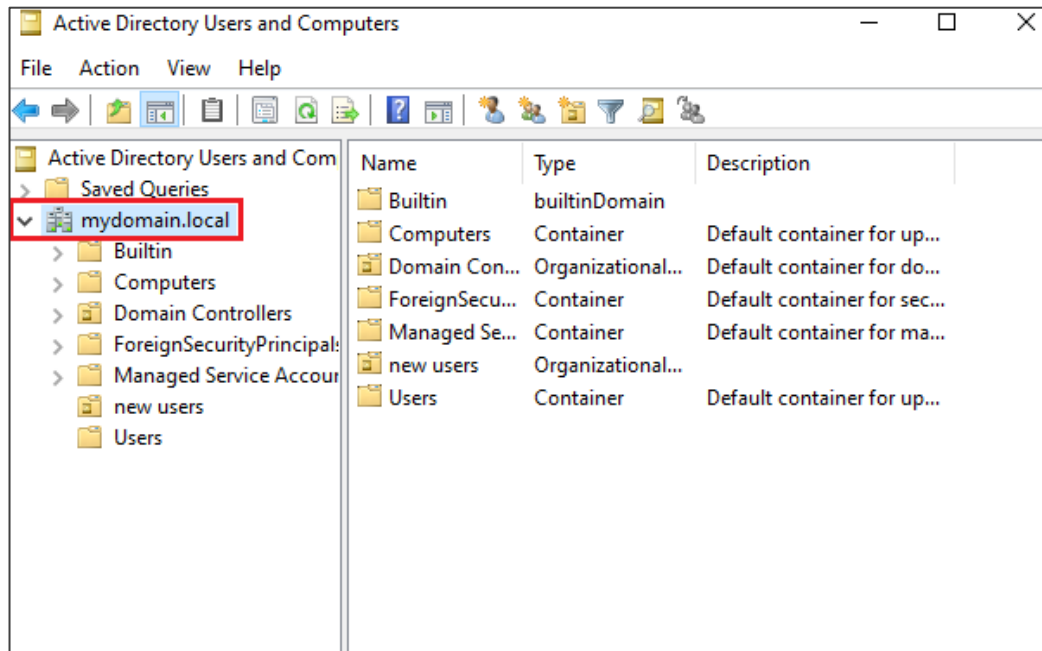


Step 2: Open Active Directory Users and Computers (ADUC)

- 2.1 In the Window VM, press Win + R, type **dsa.msc**, and press **OK** to open the **Active Directory Users and Computers (ADUC)** console

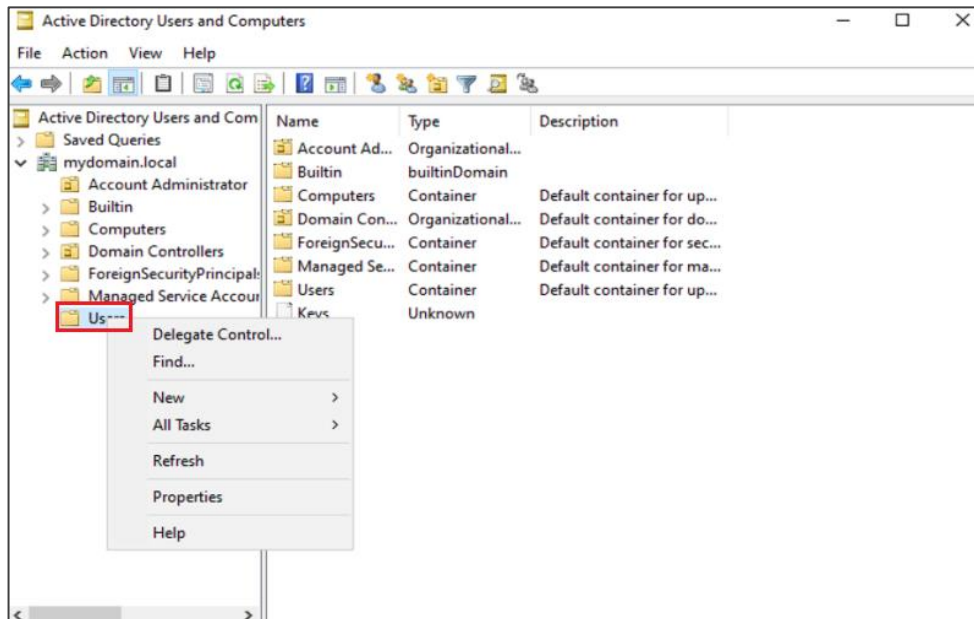


2.2 In the Active Directory Users and Computers console, expand the domain **mydomain.local**

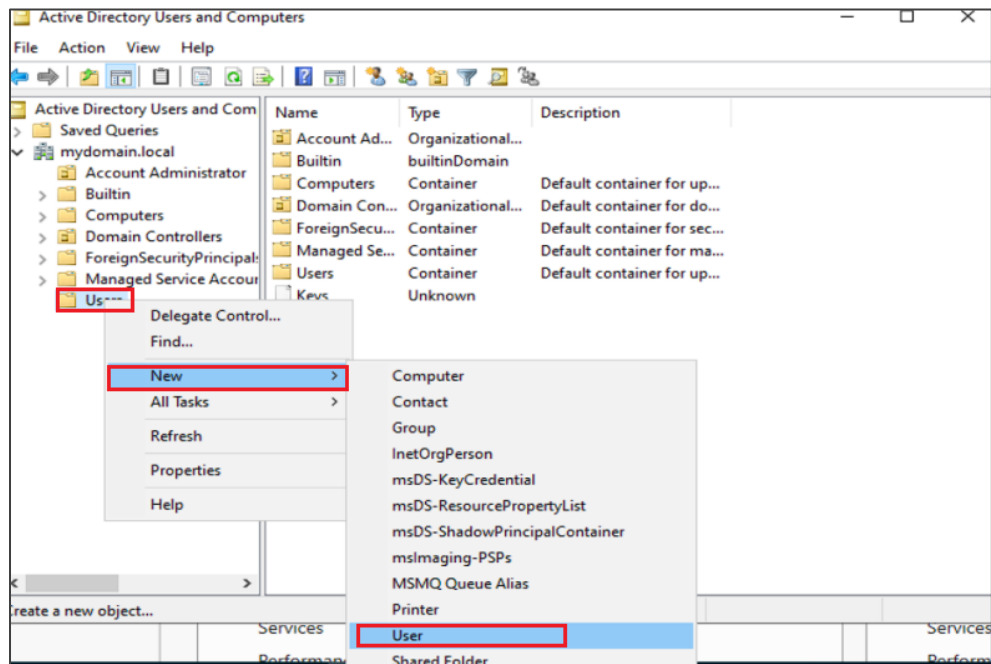


Step 3: Create and Locate the User Account

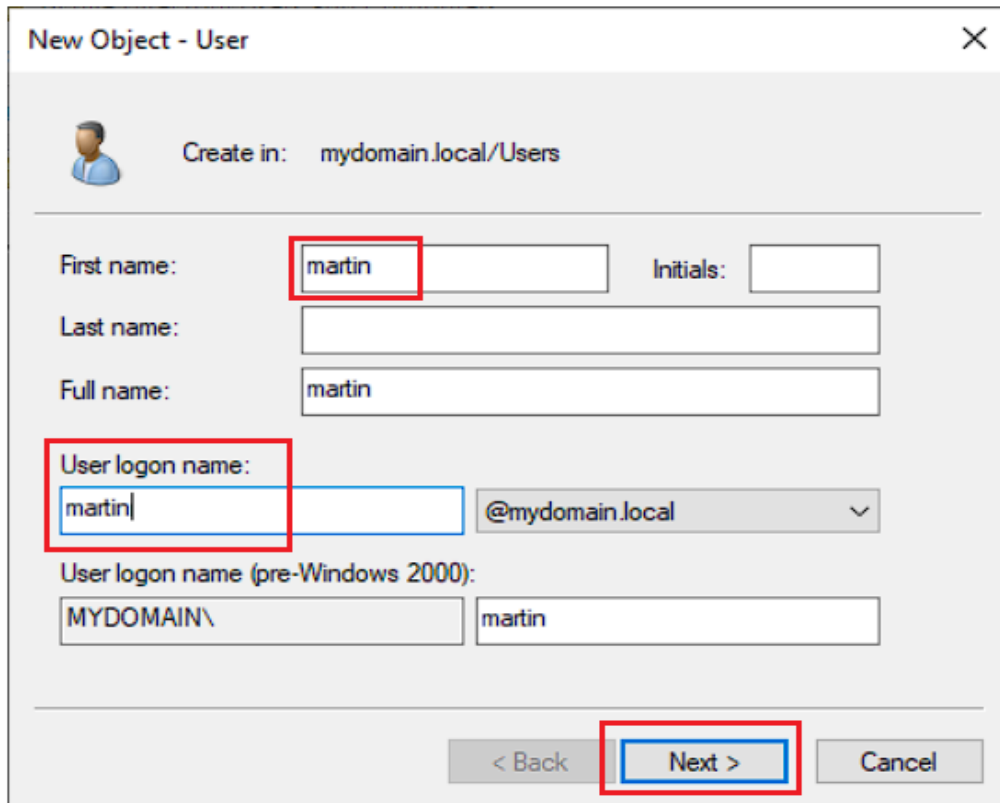
3.1 In the Active Directory Users and Computers console, navigate to the **Users** container



3.2 Right-click on the **Users** container, select **New**, and then click on **User**



3.3 Enter the username as **martin** and click on **Next**



New Object - User [X]

Create in: mydomain.local/Users

First name: Initials:

Last name:

Full name:

User logon name: @mydomain.local [v]

User logon name (pre-Windows 2000):

< Back **Next >** Cancel

3.4 Set a password for the user, select **User cannot change password** and **Password never expires**, and click **Next**

New Object - User

Create in: mydomain.local/Users

Password:

Confirm password:

☐ User must change password at next logon

☒ User cannot change password

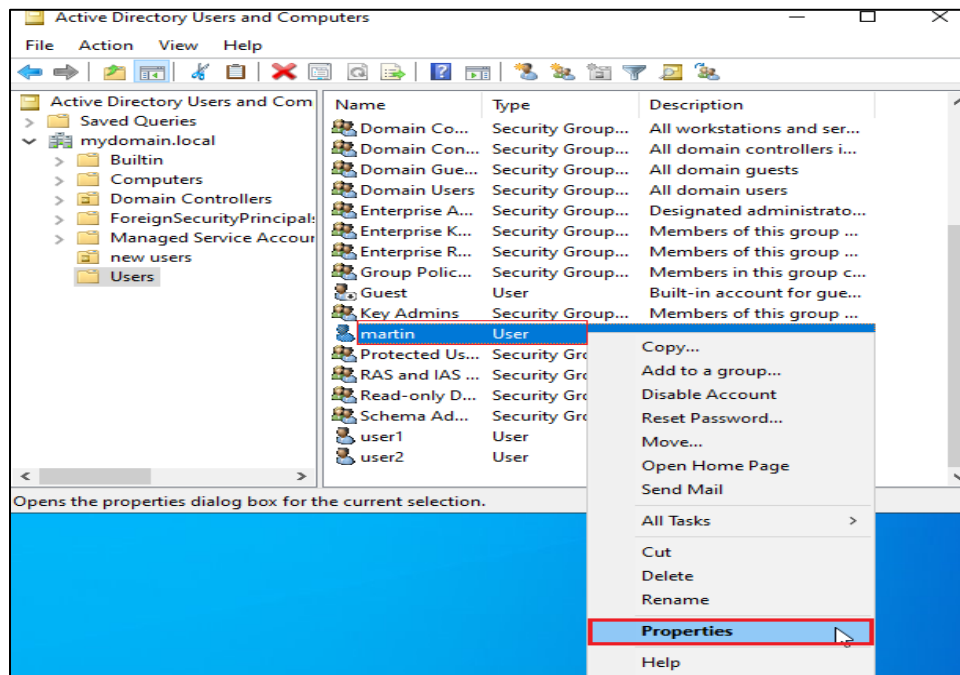
☒ Password never expires

☐ Account is disabled

< Back Next > Cancel

Step 4: Configure the Logon hours

4.1 Right-click on the user **martin** and select **Properties** in the Active Directory Users and Computers console

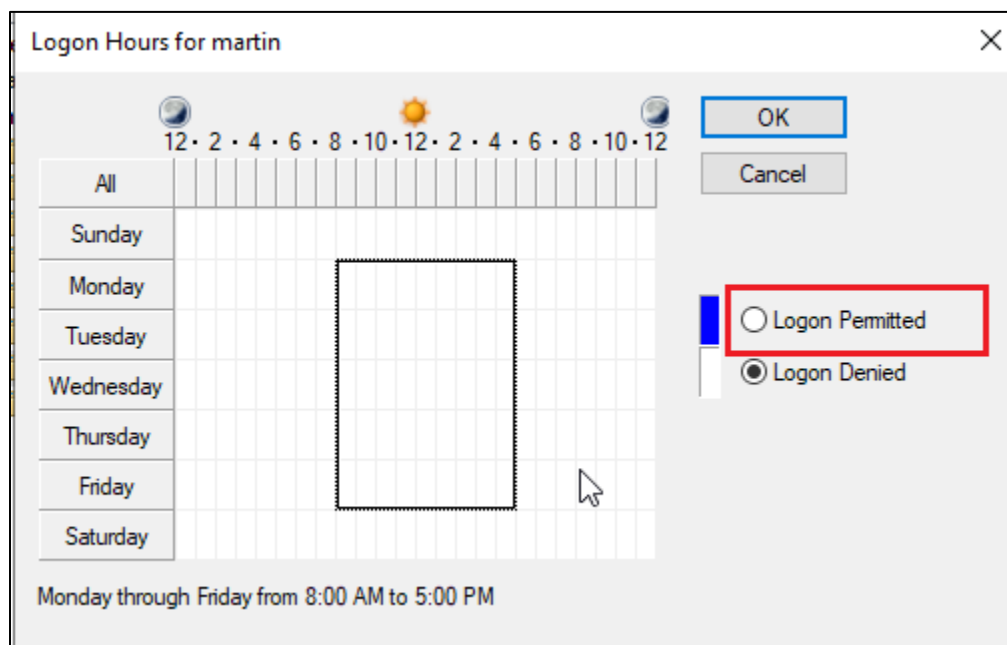
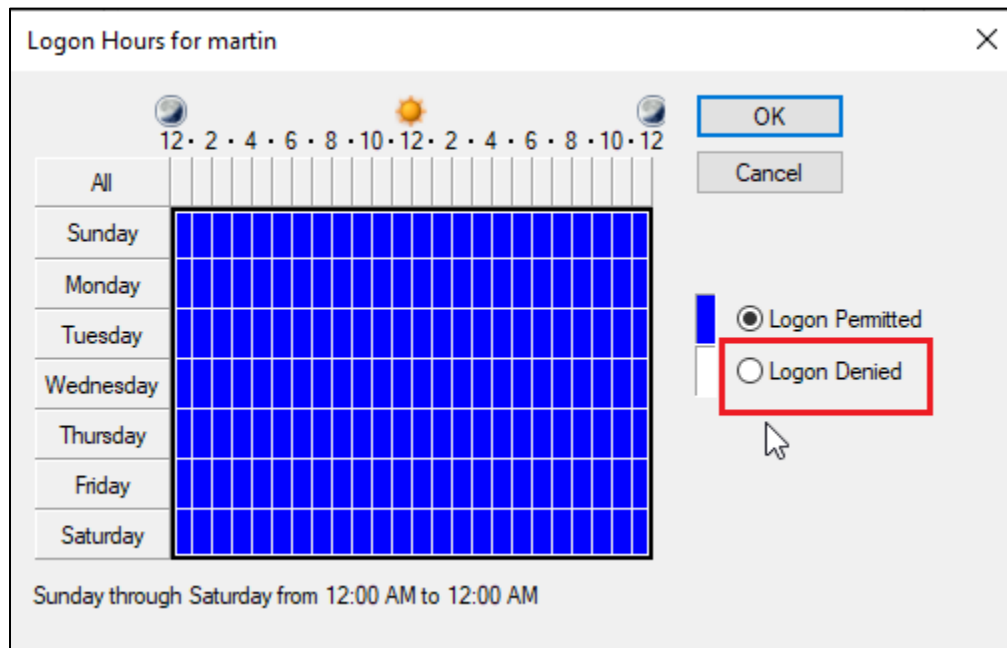


4.2 In the properties window, go to the **Account** tab and click **Logon Hours...**

The screenshot shows the 'martin Properties' window with the 'Account' tab selected. The 'Logon Hours...' button is highlighted with a red box. The window contains the following elements:

- Member Of:** Remote control, Remote Desktop Services Profile, General, Address, **Account**, Profile, Telephones, Sessions, COM+, Organization.
- User logon name:** martin, @mydomain.local
- User logon name (pre-Windows 2000):** MYDOMAIN\, martin
- Logon Hours...** (highlighted with a red box)
- Log On To...**
- ☐ Unlock account
- Account options:**
 - ☐ User must change password at next logon
 - ☒ User cannot change password
 - ☒ Password never expires
 - ☐ Store password using reversible encryption
- Account expires:**
 - ☒ Never
 - ☐ End of: Friday, August 2, 2024
- Buttons:** OK, Cancel, Apply, Help

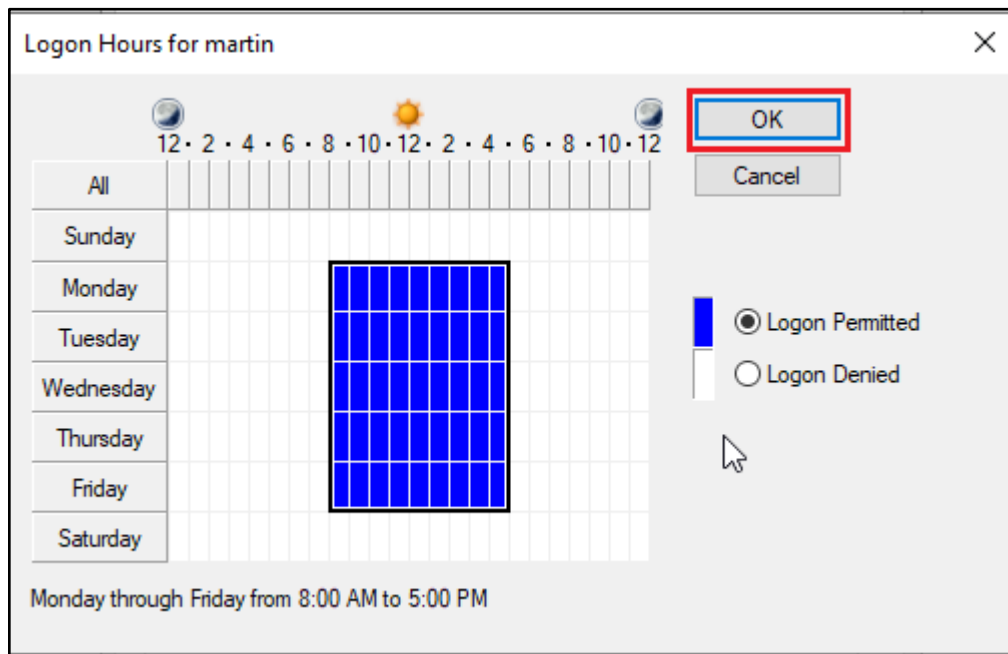
4.3 In the Logon Hours window, use the grid to specify permitted Logon times by clicking and dragging to select the time slots, then select either **Logon Denied** or **Logon Permitted** as appropriate



Ensure the user can only log in during the permitted times

Step 5: Apply and close the Logon Hours window

5.1 Click **OK** in the Logon Hours window to save the settings



5.2 Click **Apply** in the Properties window and then click **OK** to close it

The screenshot shows the 'martin Properties' window with the 'Account' tab selected. The 'User logon name' is 'martin' and the domain is '@mydomain.local'. The 'User logon name (pre-Windows 2000)' is 'MYDOMAIN\' and the name is 'martin'. There are buttons for 'Logon Hours...' and 'Log On To...'. The 'Unlock account' checkbox is unchecked. Under 'Account options', 'User must change password at next logon' is unchecked, 'User cannot change password' is checked, 'Password never expires' is checked, and 'Store password using reversible encryption' is unchecked. Under 'Account expires', 'Never' is selected. At the bottom, the 'OK' and 'Apply' buttons are highlighted with red rectangles.

By following these steps, you have successfully configured the Logon hours in the Active Directory to enhance security and access control using Attribute-Based Access Control (ABAC).