

Service Accounts and Sysinternals

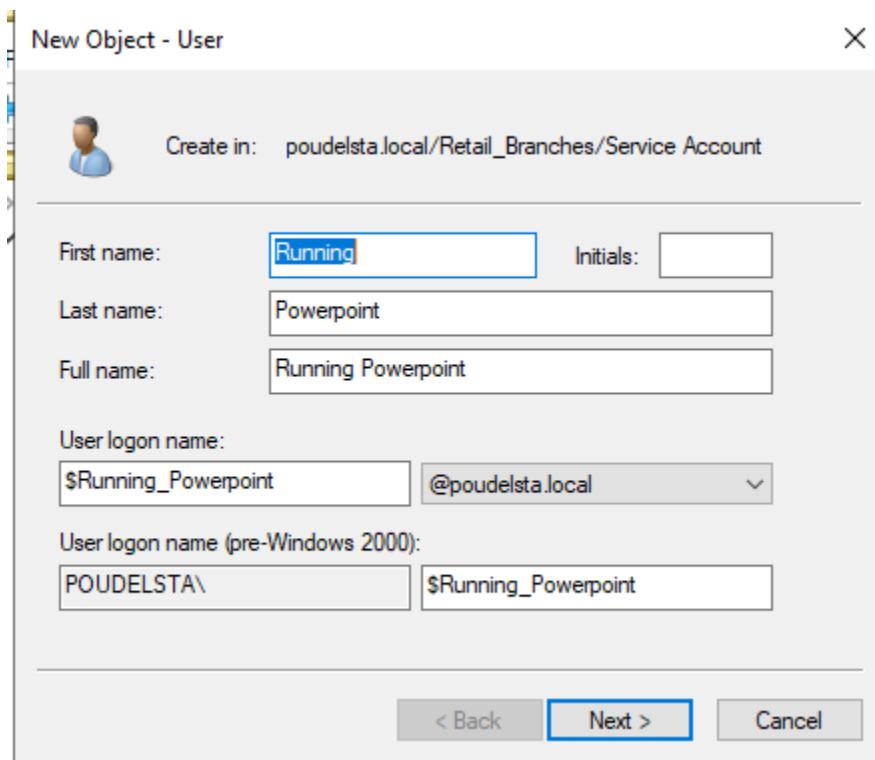
Part 1: Creating the Service Account

1. Create the Service Account OU:

- We will open **Active Directory Users and Computers (ADUC)**.
- We will create a separate Organizational Unit (OU) called **Service Accounts** for organizational clarity.

2. Create the Service Account User:

- Within the **Service Accounts** OU, right-click and select **New > User**.
- We will name the account based on its function, e.g., **Running PowerPoint**.
- **User Logon Name:** As a best practice for easy identification, we will use a distinct naming convention, such as starting the name with a dollar sign (\$) and using underscores (_) instead of periods, e.g., **\$Running_Powerpoint**.



- Click **Next**, and create a strong password.

- **Critical Security Settings:** We must **uncheck** "User must change password at next logon," and instead check "**User cannot change password**" and "**Password never expires.**" Click **Next** and **Finish**.

3. Add Description (Best Practice):

- **Right-click** on the new service account, click **Properties**, and add a detailed **Description** explaining the account's purpose (e.g., "Used for auto-login on display kiosk at Retail Branch").

Part 2: Configuring Auto-Logon on the Client VM

1. Log In and Download Sysinternals:

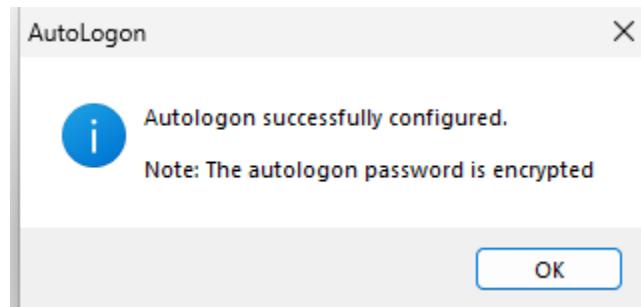
- We will now log into our client Windows 11 VM using the newly created **\$Running_Powerpoint** service account.
- Open the web browser and search for **Sysinternals Suite**. (Sysinternals is a free set of advanced tools from Microsoft.)
- We will navigate to the Microsoft documentation link and click the option to **Download Sysinternals Suite**.

The screenshot shows a web browser displaying the Microsoft Learn website at <https://learn.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>. The page title is "Sysinternals Suite". It features a sidebar on the left with links like "Downloads", "Community", and "Resources". The main content area includes a search bar, navigation links for "Learn", "Documentation", "Training", "Q&A", and "Topics", and a "Sign in" button. Below the navigation is a "Find by title" input field. The main content area displays the "Sysinternals Suite" page, which is updated by Mark Russinovich on November 20, 2025. It lists several download options: "Download Sysinternals Suite" (166.5 MB), "Download Sysinternals Suite for Nano Server" (9.6 MB), "Download Sysinternals Suite for ARM64" (15.2 MB), and "Install Sysinternals Suite from the Microsoft Store". There is also a "Ask Learn" button.

2. Run Autologon Utility:

- After the download is complete, we will extract the contents of the ZIP file.
- We will open the extracted folder and find **Autologon64.exe**.
- **Double-click Autologon64.exe**.

- If prompted for administrator credentials, input the **Administrator** username and password for the domain (or a user with elevated rights).
- Click **Agree** to the license agreement.
- **Enable Autologon:** We will be asked to enter the username and password for the service account we just created:
 - **Username:** \$Running\Powerpoint
 - **Domain:** poudelsta.local
 - **Password:** The password we created for the service account.
- Click **Enable**. A confirmation will appear that Autologon is successfully configured.



- **Test:** We can reboot the computer to verify that it logs in automatically without user interaction.

Part 3: Kiosk Application and Power Configuration

1. Configure Application for Startup:

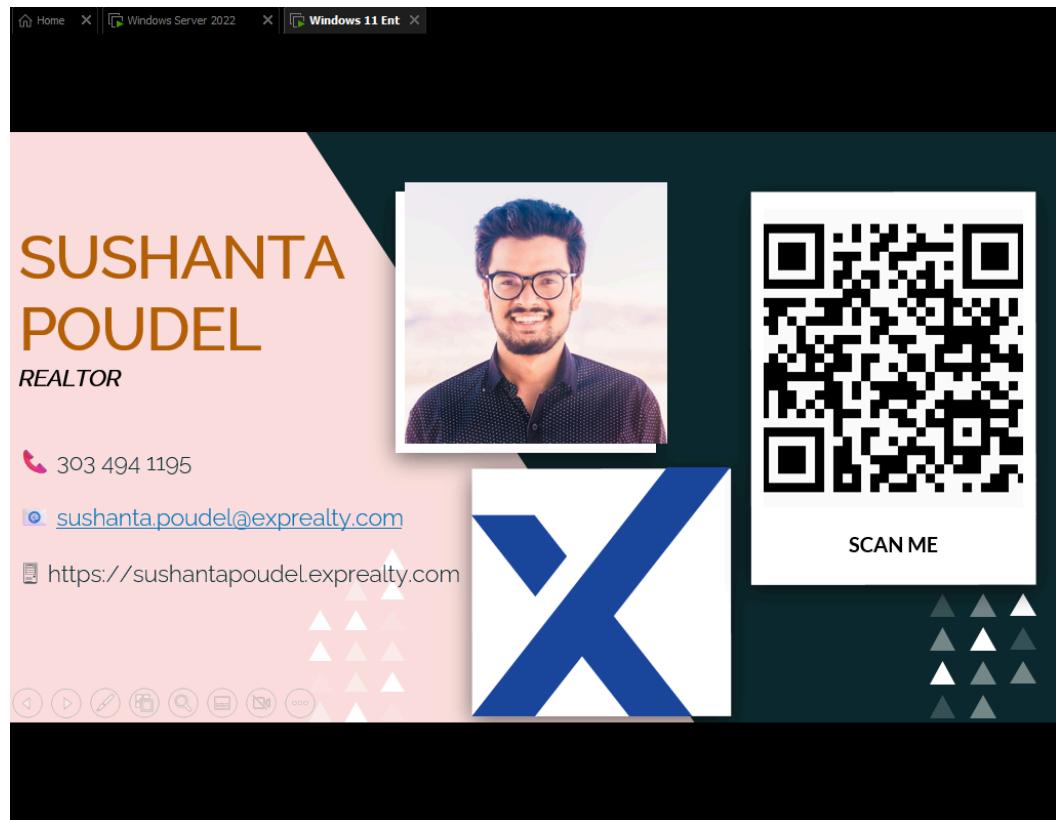
- We will prepare the application (e.g., a PowerPoint presentation) to run automatically.
- **PowerPoint Tip:** Save the presentation as a **PowerPoint Show (.ppsx)** file. When opened, this file automatically starts in full-screen presentation mode.
- **Add to Startup Folder:** Press **Win + R** to open the Run command, and type `shell:startup`. This opens the user's Startup folder.
- We will **drag and drop** the .ppsx file (or a shortcut to any program we want to auto-start) into this folder.
-

2. Disable Sleep/Screen Timeout:

- We need to ensure the machine never sleeps or turns off the screen.
- **Troubleshooting GPO Conflict:** When we try to access Power settings, we will encounter a restriction because we previously restricted access to the Control Panel/Settings via GPO.
- **Solution:** We will temporarily return to the server, modify the **Restrict Control Panel** GPO to not apply to the Service Accounts OU, and run gpupdate /force on the client.
- **Configuration:** Now that we have access, we will search for **Sleep** or **Power & Sleep** settings on the client. We will change the **Turn off screen after** setting to **NEVER**.

3. Final Test:

- We will reboot the client VM. It should auto-logon, and the PowerPoint presentation should immediately launch in full-screen mode.

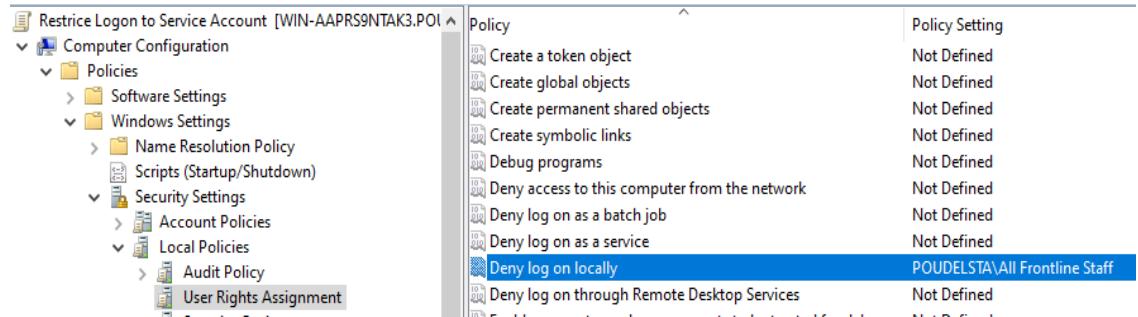


Part 4: Restricting Log On Locally (Security Hardening)

Since this is a service account, it should not be used by branch staff to log on interactively.

1. Create Restrictive GPO:

- We will return to the server and open **Group Policy Management** (gpmc.msc).
- Under **Group Policy Objects**, we will right-click and create a new GPO named **Restrict Logon to Service Account**.
- **Right-click** the GPO and click **Edit**.
- **Configuration:** We navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
- **Deny Log On Locally:** We will double-click this policy, check **Define these policy settings**, and click **Add User or Group**.
- We will select a group that includes regular branch employees, such as **All Frontline Staff**. Click **OK** and **Apply**.



Policy	Policy Setting
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Not Defined
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	POUDELSTA\All Frontline Staff
Deny log on through Remote Desktop Services	Not Defined

2. Link the GPO:

- We will drag and drop the **Restrict Logon to Service Account** GPO from the Group Policy Objects folder to the **Retail_Branches > Computers** OU.
- **Update:** Run gpupdate /force on the server and client to apply the policy immediately.

