Configuring the SPLUNK Enterprise Application
By: Keziah Rogers

Topic 1 - Log Collection with Splunk
Topic 2 - Encrypting Sensitive Data
Topic 3 - Enable Multifactor Authentication
Actions:

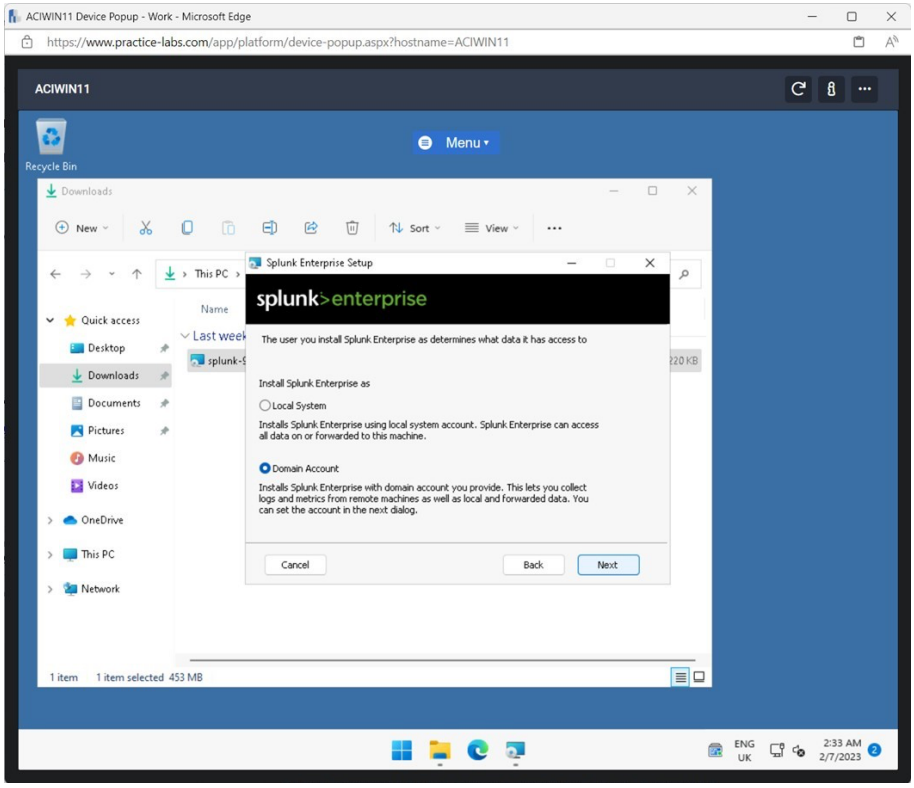
a. Installed and Configured the Splunk Enterprise Application
b. Configured a Splunk Client
c. Collected Logs using Splunk Enterprise
d. Installed the BitLocker Drive Encryption Feature
e. Encrypted a Local Drive on a Server
f. Enabled Multifactor Authentication
g. Verified Multifactor Authentication

Topic 1 - Log Collection with Splunk

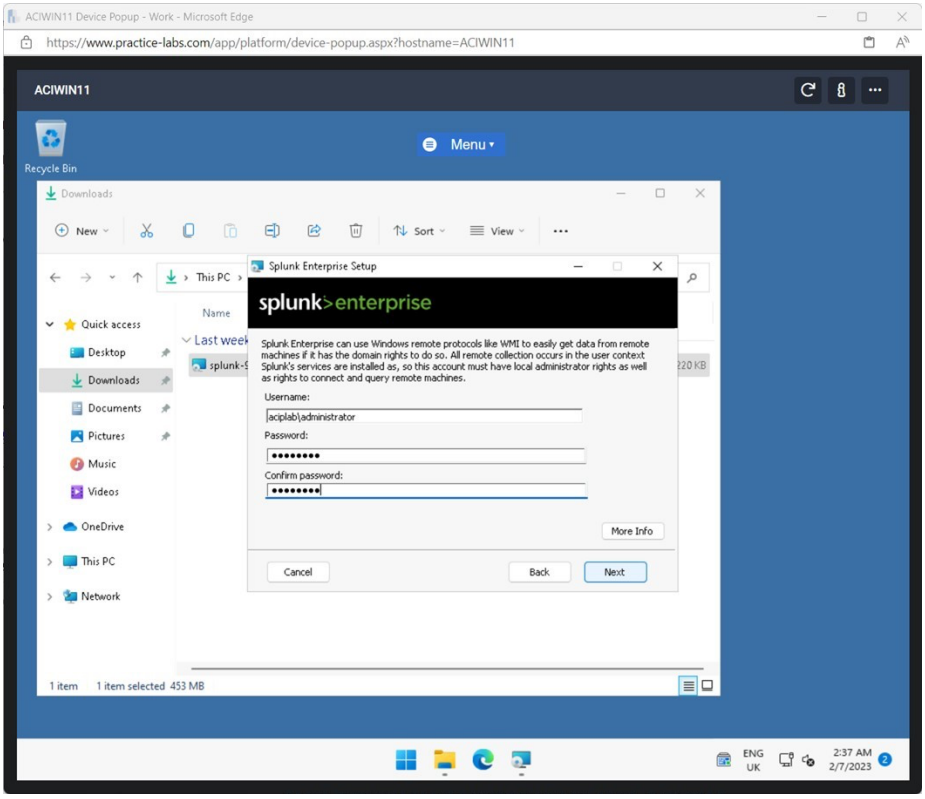
- The Splunk Enterprise application can be used to collect logs of devices on the network. Using the application, a centralized point of all the logs of the devices can be monitored.
- I installed and configured the Splunk Enterprise application to collect the logs of devices on the network.
- I also used a Windows virtual machine (VM) to perform these actions.

Action 1 - Installed and Configured the Splunk Enterprise Application
The Splunk Enterprise application collects logs from devices on the network. In this task, the Splunk Enterprise application will be installed and configured.

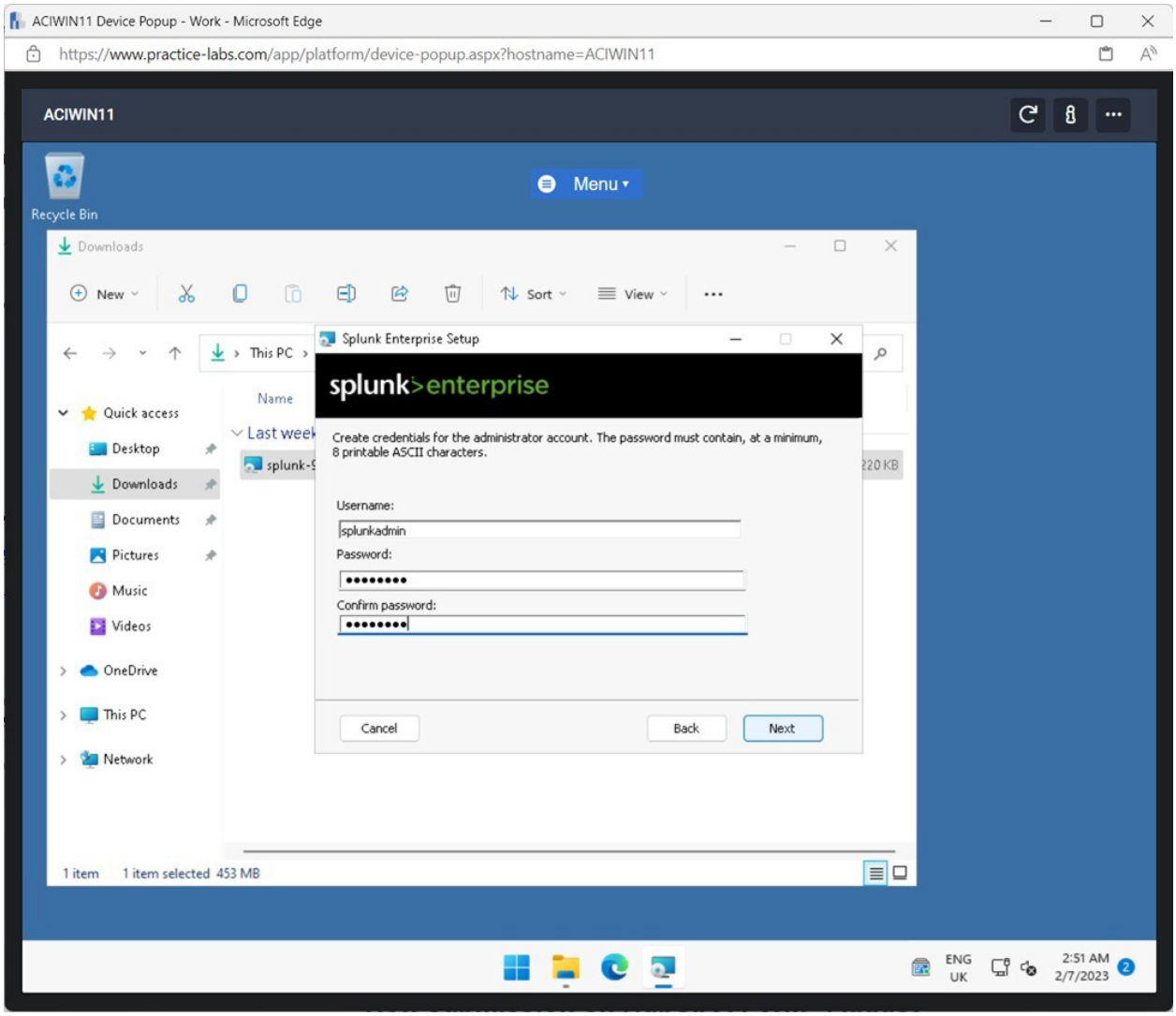
- **Connected to VM, opened File Explorer, clicked downloads, and double clicked splunk-9.0.33-dd**
- On the **Splunk Enterprise Installer** pop-up window, I ticked the **Check this box to accept the License Agreement** tick box
- Clicked **Customize Options**.
- **Clicked Next on the Install Splunk Enterprise screen.**
- Selected **Domain Account** on the **Install Splunk Enterprise as** screen.
- Clicked **Next**.



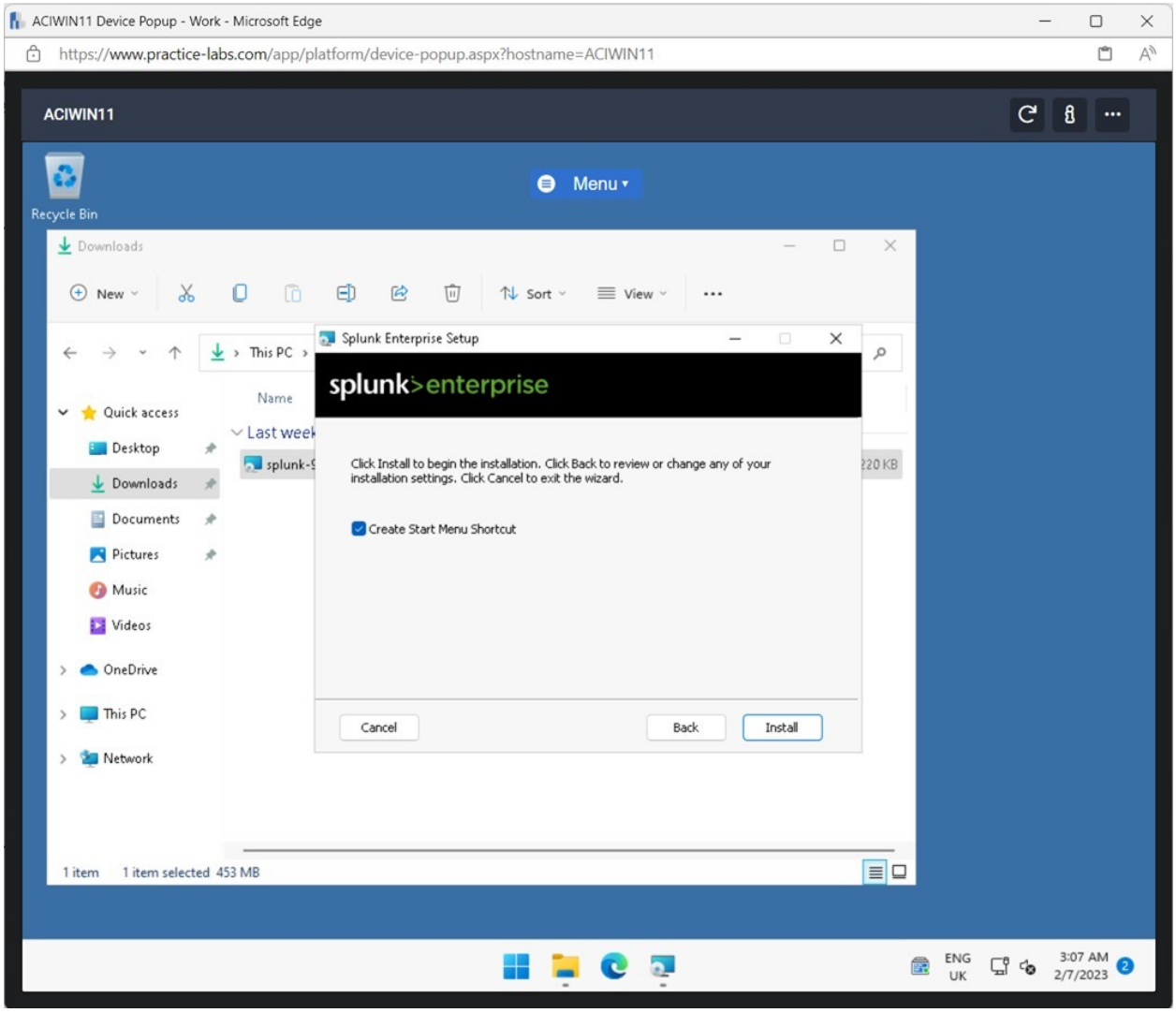
- Entered the following details on the **Splunk Enterprise Setup** screen:
- **Username: aciplab\administrator**
- **Password: Passw0rd**
- **Confirm password: Passw0rd**
- Clicked **Next**.



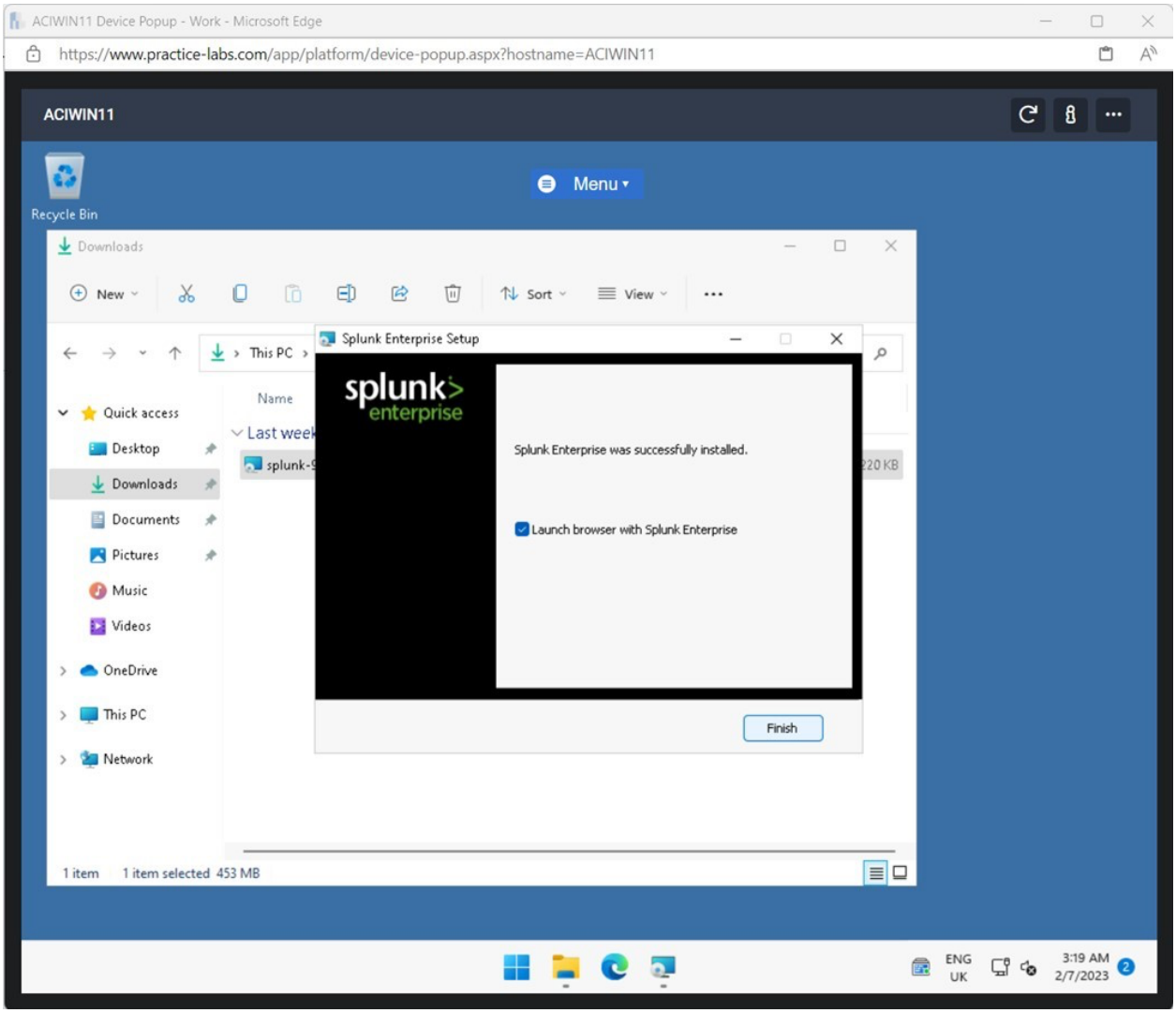
-
- Entered the following details on the **Splunk Enterprise Setup** screen:
- **Username: splunkadmin**
- **Password: Passw0rd**
- **Confirm password: Passw0rd**
- Clicked **Next**.



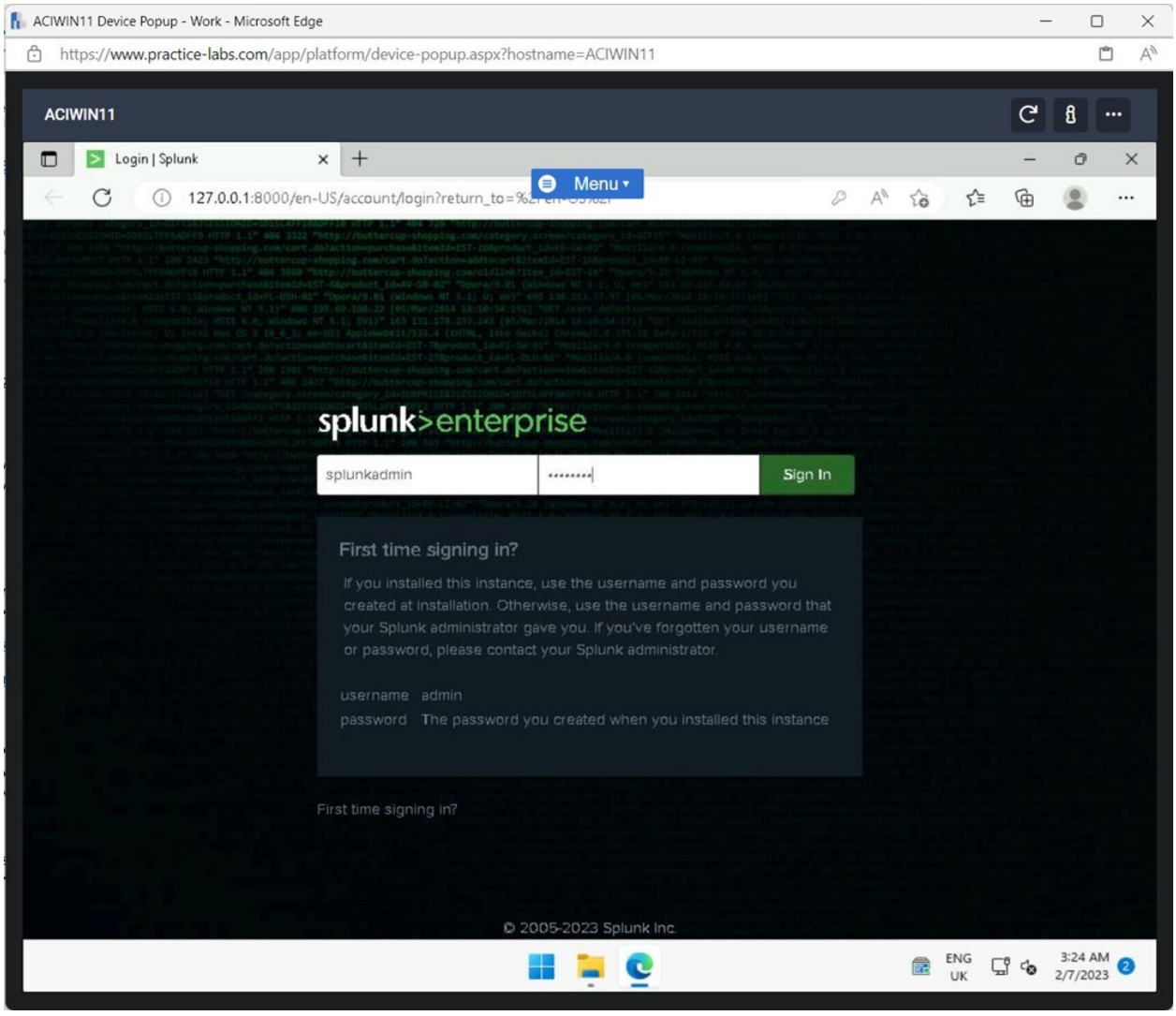
- Screenshot: Displaying entering the credentials and password on the installation screen.
- I created a local account with a password since it was used to log into the Splunk Enterprise web app.
- Clicked **Install** on the **Splunk Enterprise Setup** screen.



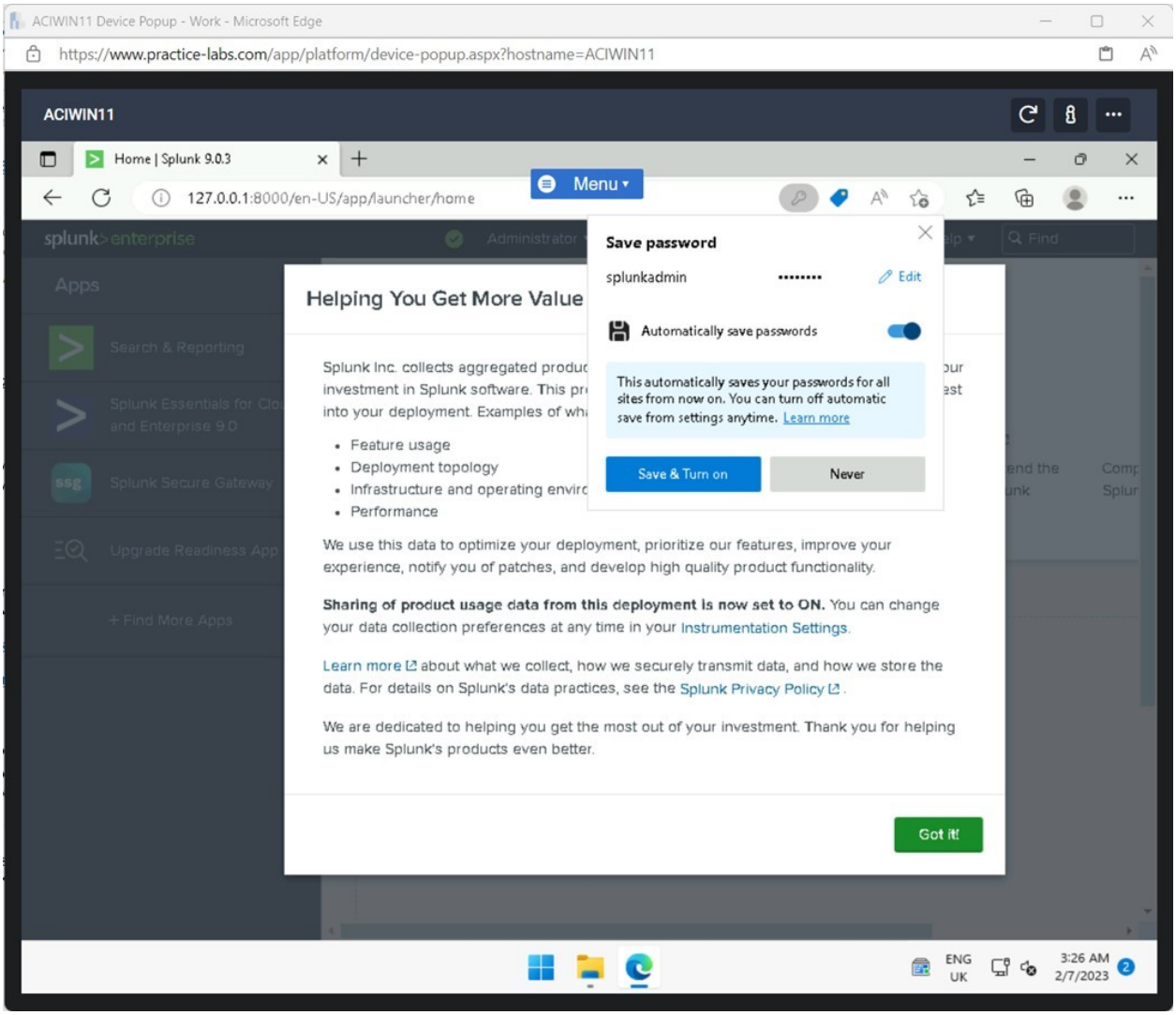
-
- Installation took a couple of minutes to load.
- Clicked **Finish** on the **Splunk Enterprise Setup** screen.



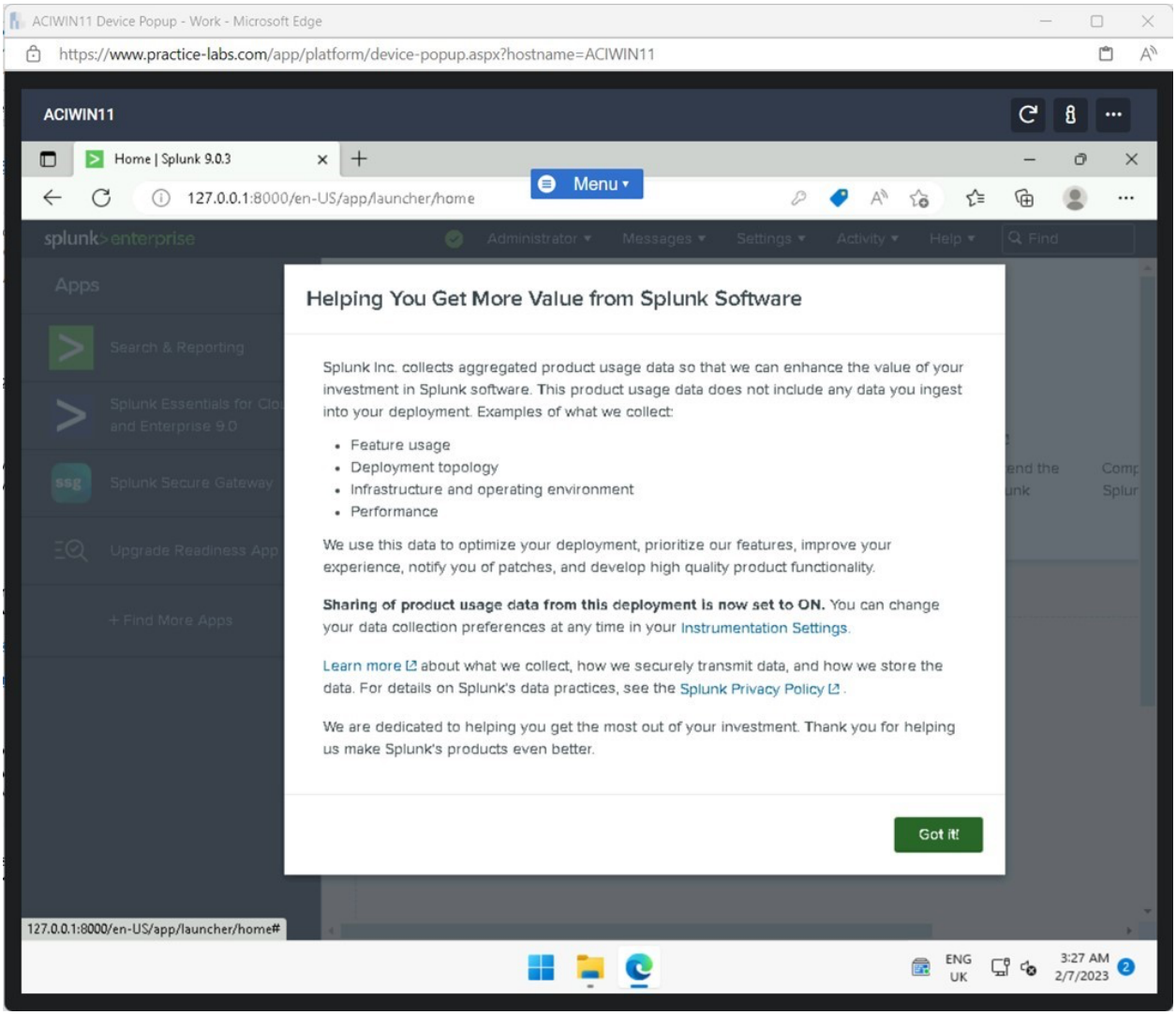
- Splunk opened automatically in the MS Edge browser.
- In the **Microsoft Edge** browser window, I entered the following credentials:
- **Username: splunkadmin**
- **Password: Passw0rd**
- Clicked **Sign In**.

- 

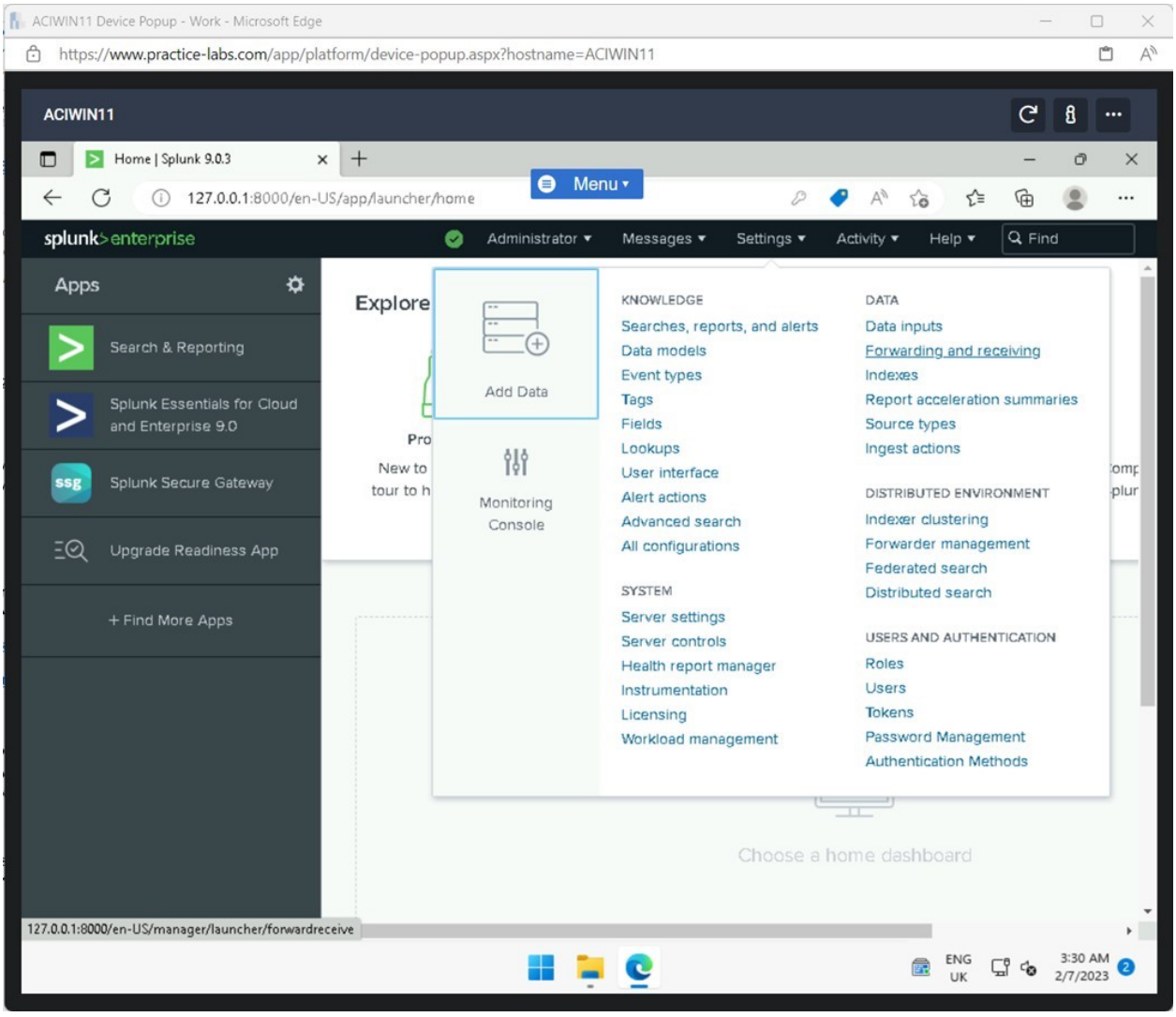
  Screenshot: Displaying signing into the Splunk Enterprise web application.
- Clicked **Never** on the **Save password** pop-up window.

- 

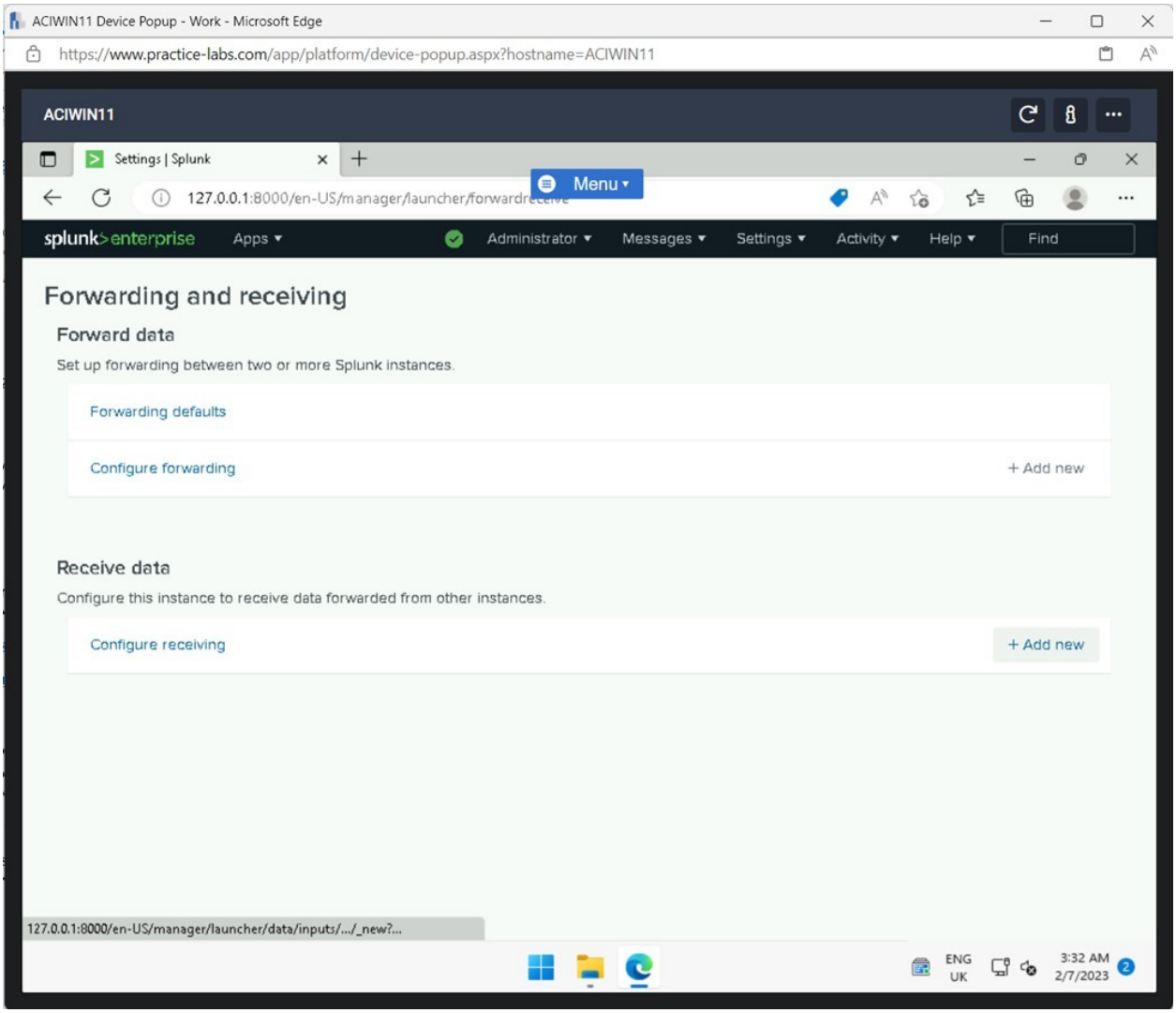
  Screenshot: Displaying clicking Never on the pop-up window.
- Clicked **Got it** on the **Helping You Get More Value from Splunk Software** pop-up window.



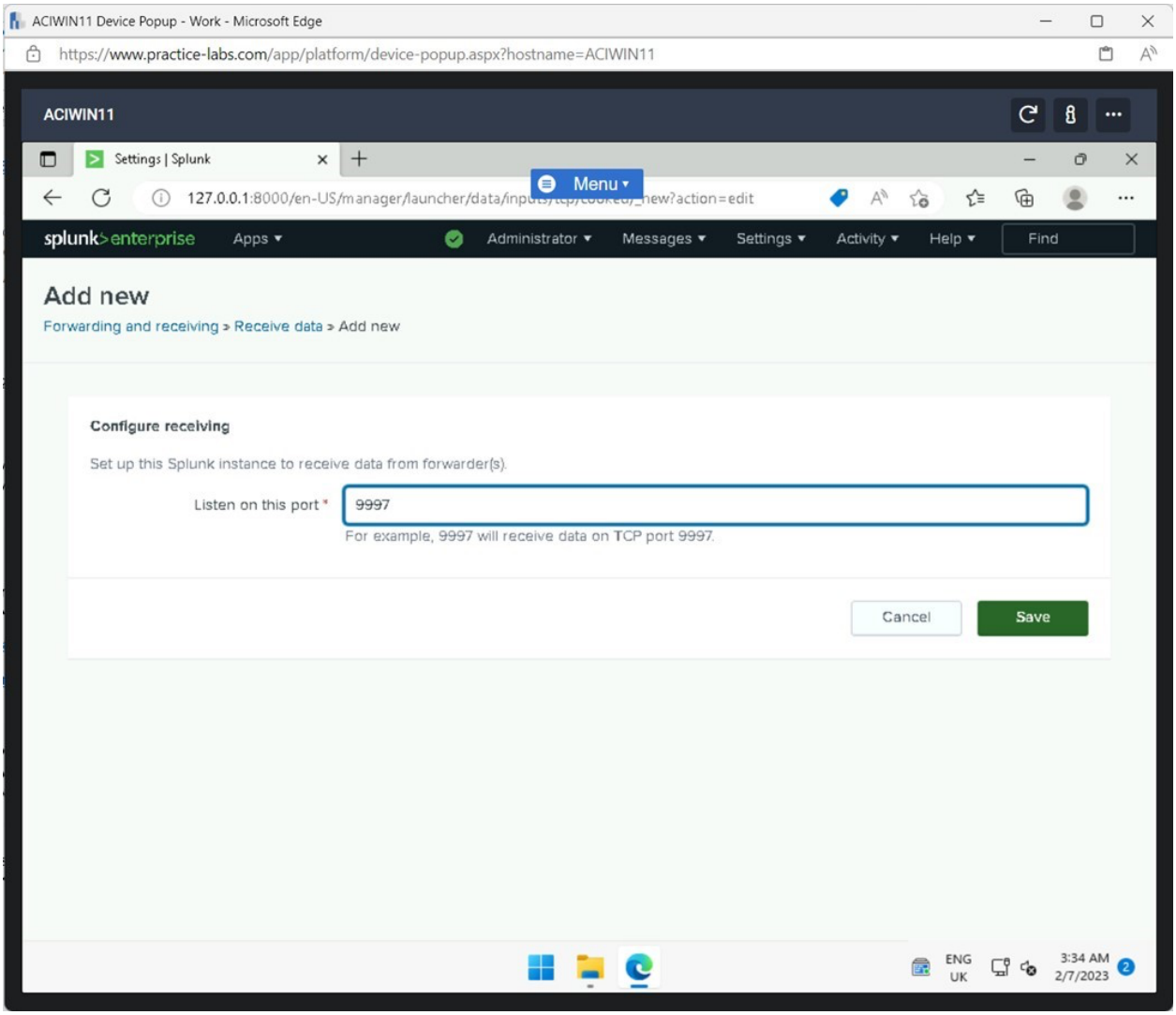
- Screenshot: Displaying clicking Got it on the pop-up window.
- In the **Splunk Enterprise** web application, I clicked **Settings**.
- In the fly-out window, in the **DATA** pane, I selected **Forwarding and receiving**.



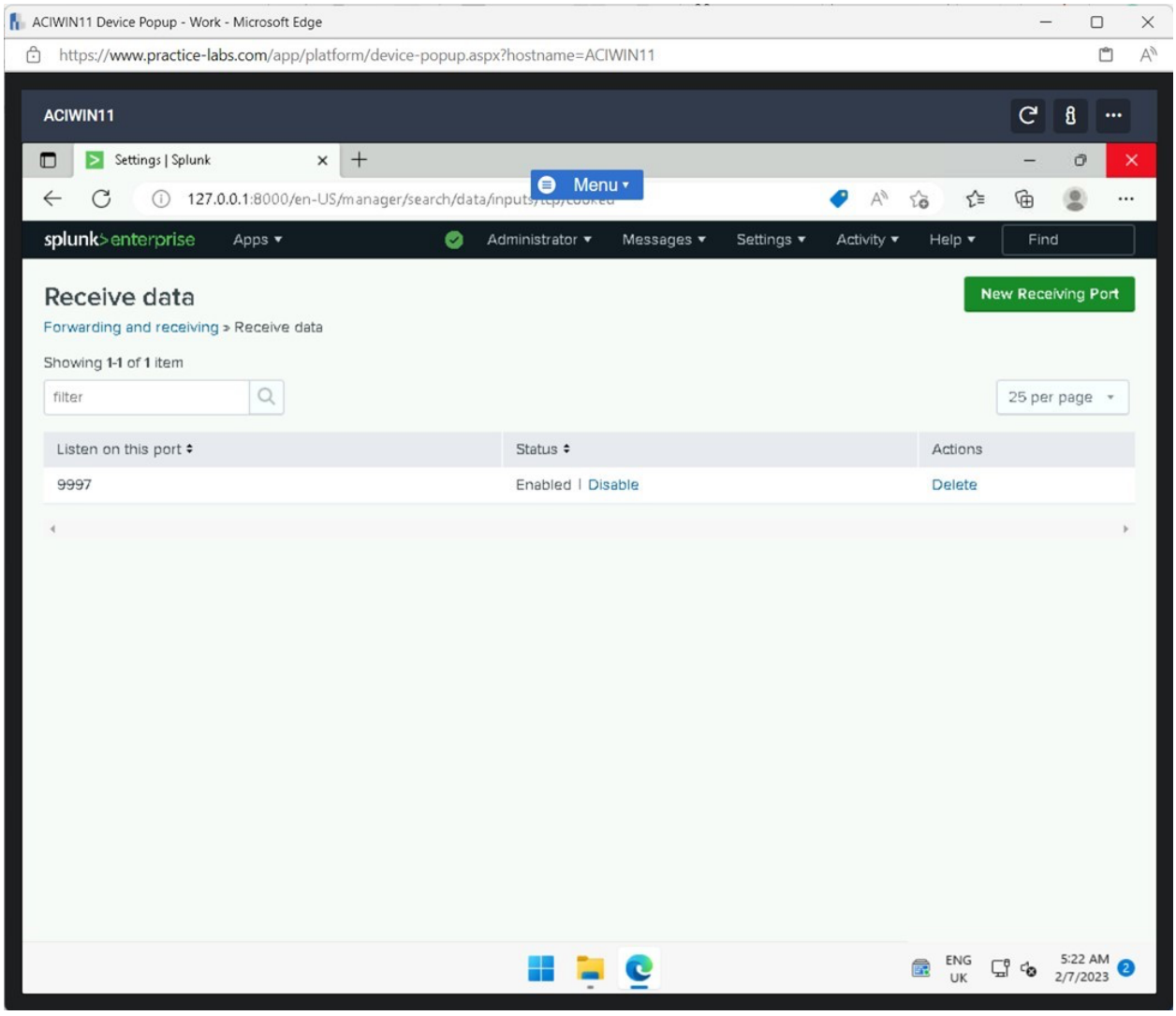
- Screenshot: Displaying clicking Settings and selecting Forwarding and receiving in the Data pane.
- On the **Forwarding and receiving** window, I clicked the **+ADD new** in the **Receive data** pane.



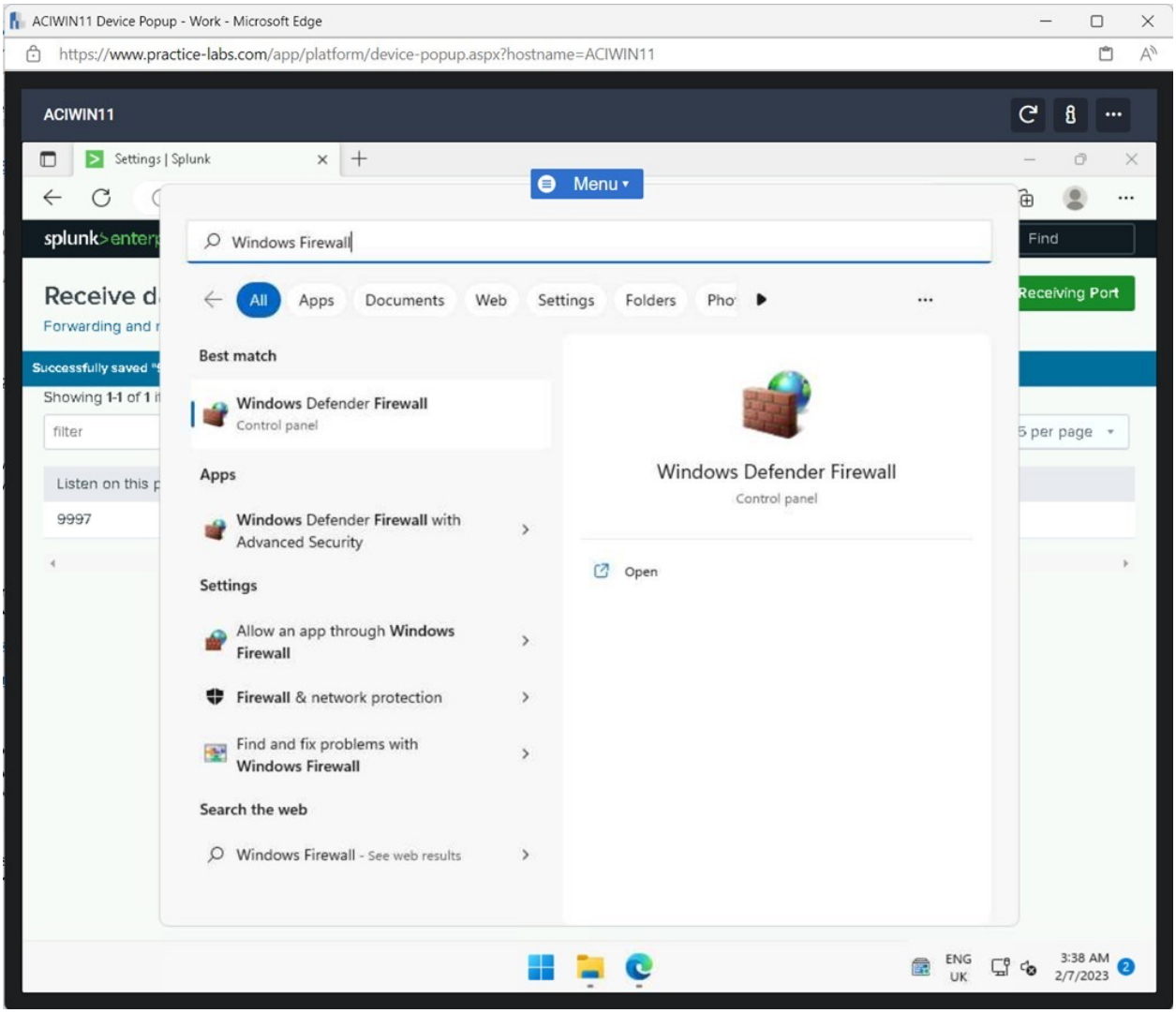
-
- On the **Add new** window, I entered the following in the **Listen on this port** field:
- **9997**
- Clicked **Save**.



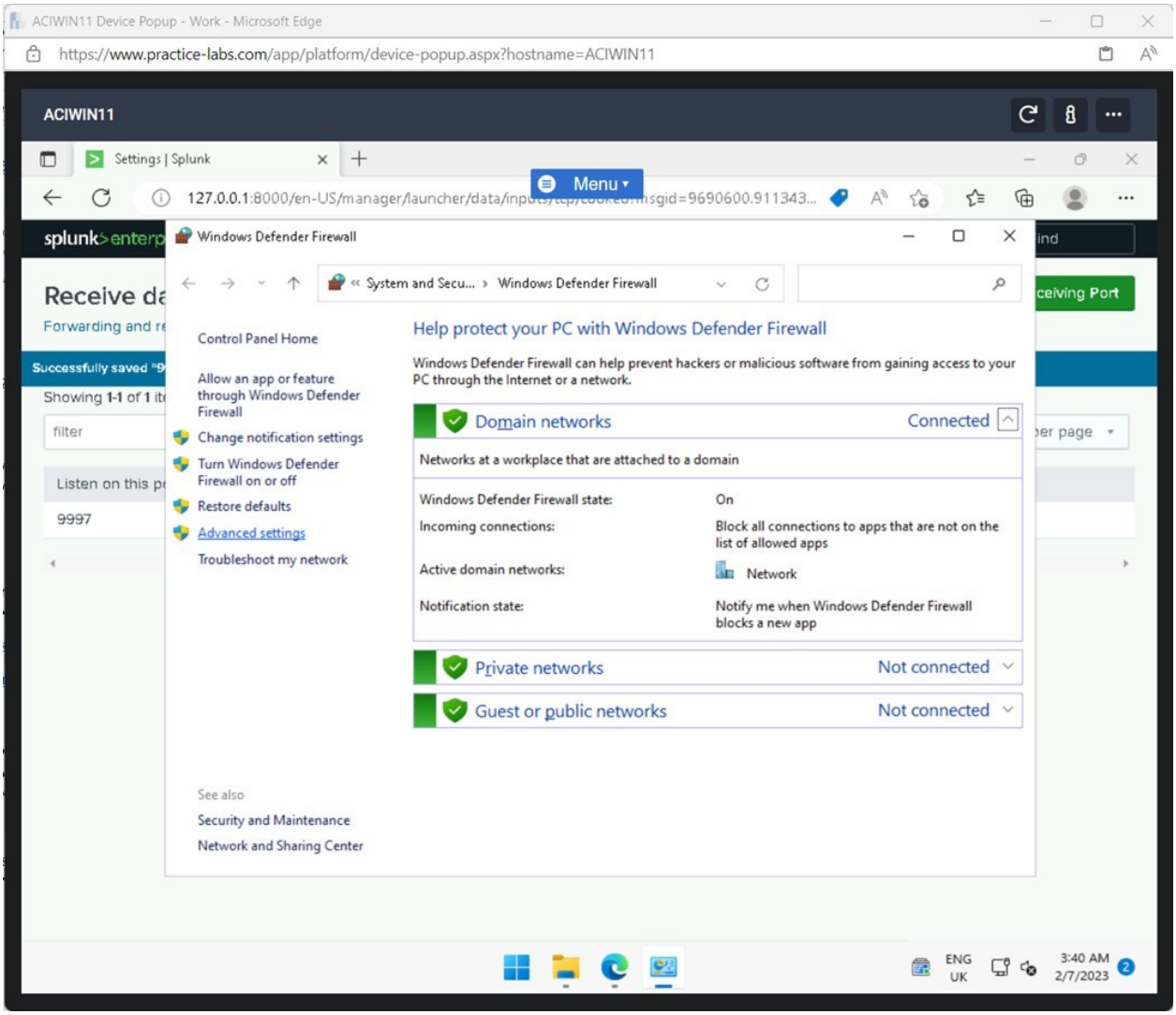
- Screenshot: Displaying entering the listening port and clicking Save.
- Kept in mind that Splunk was designed to listen for network traffic and the Windows Firewall needed to be set up to ensure the traffic could be accepted on the port.
- Closed the **Microsoft Edge** browser.



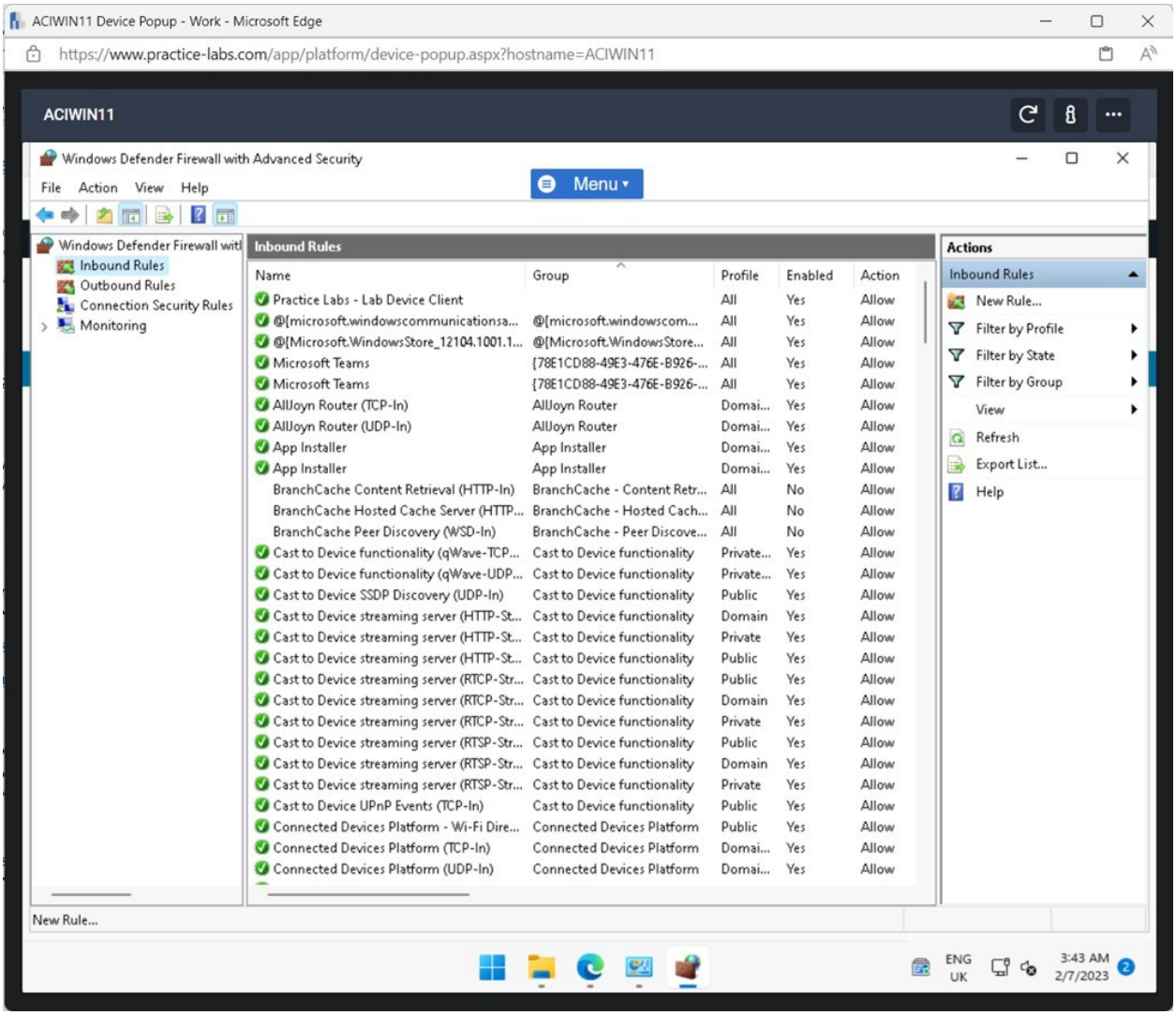
- Clicked **Start**, type the following, and press **Enter**:
- **Windows Firewall**



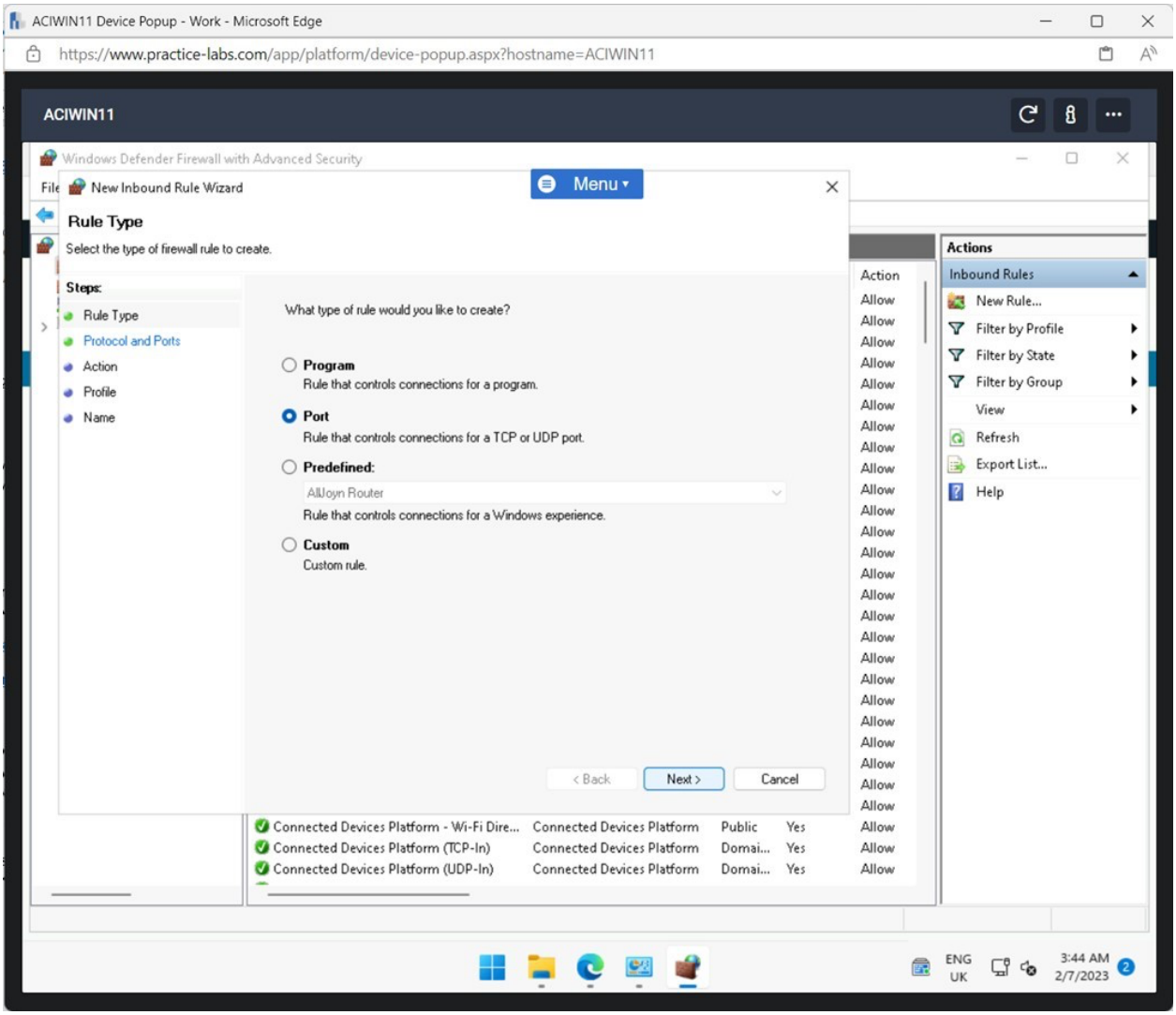
- On the **Windows Defender Firewall** window, I clicked **Advanced settings.**



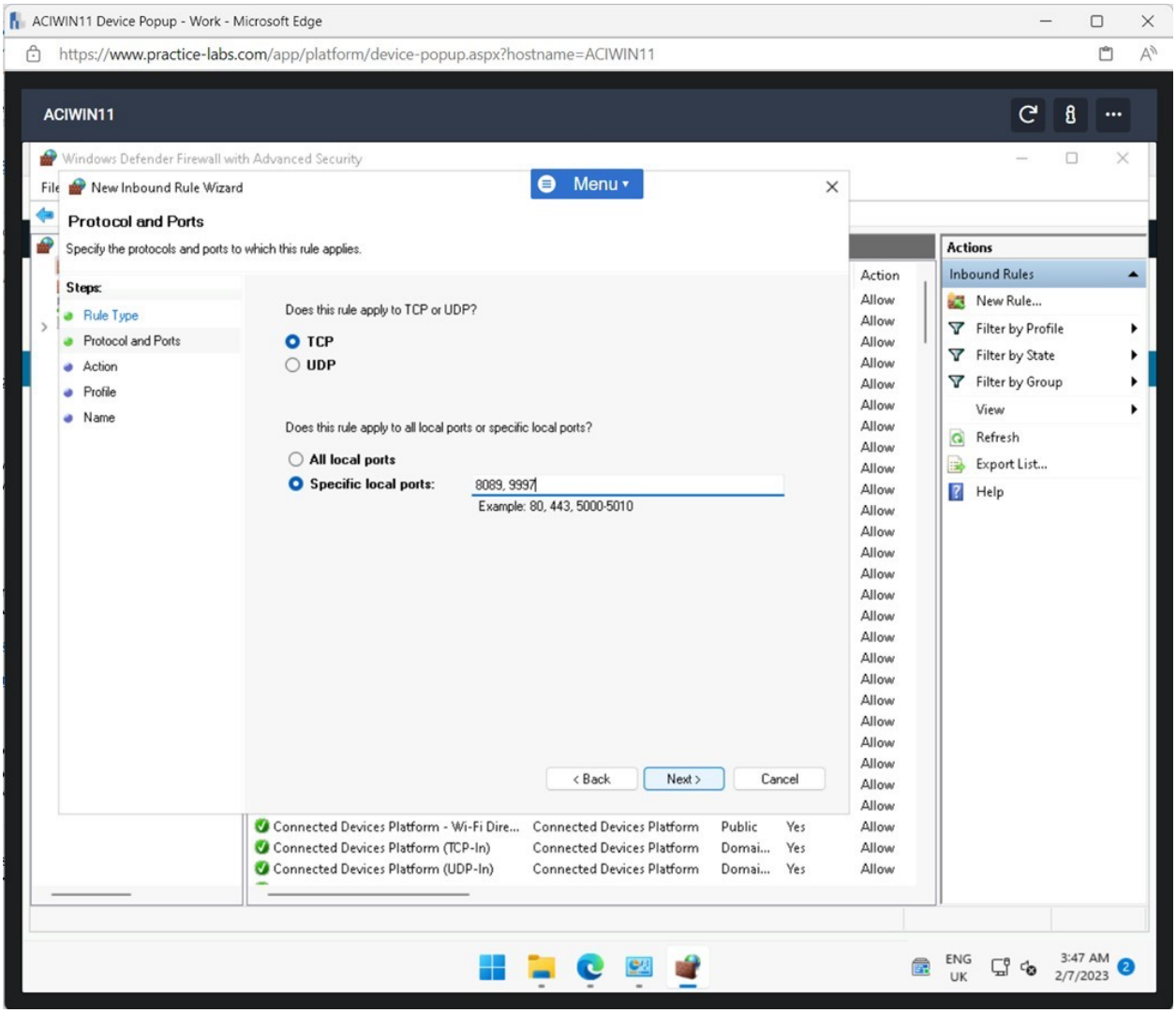
- Screenshot: Displaying clicking Advanced settings in the Windows Defender Firewall window.
- On **Windows Defender Firewall with Advanced Security**, selected **Inbound Rules** and clicked **New Rule** in the right pane.



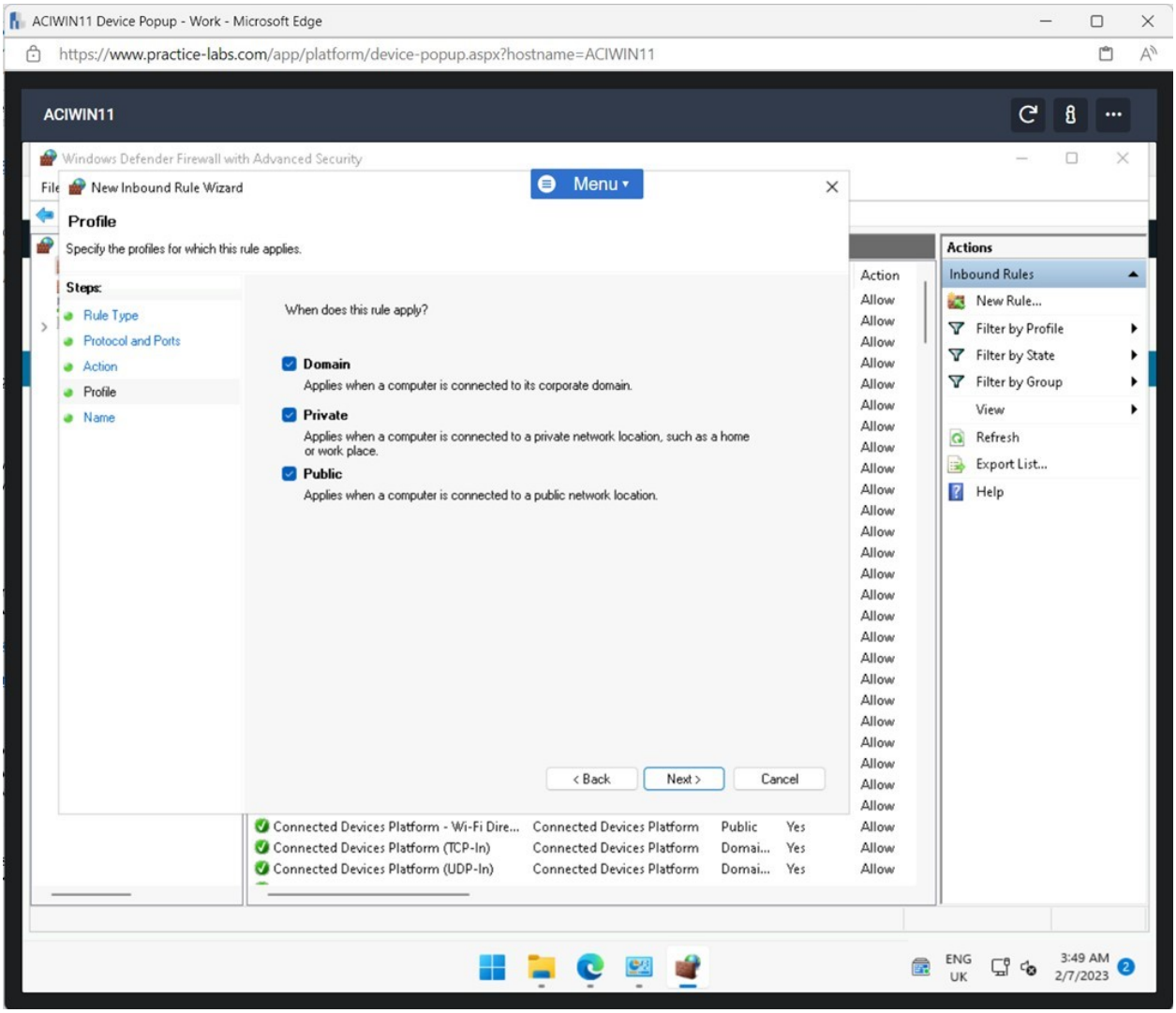
- Screenshot: Displaying creating a new inbound rule.
- Selected **Port** on the **Rule Type** window.
- Clicked **Next**.



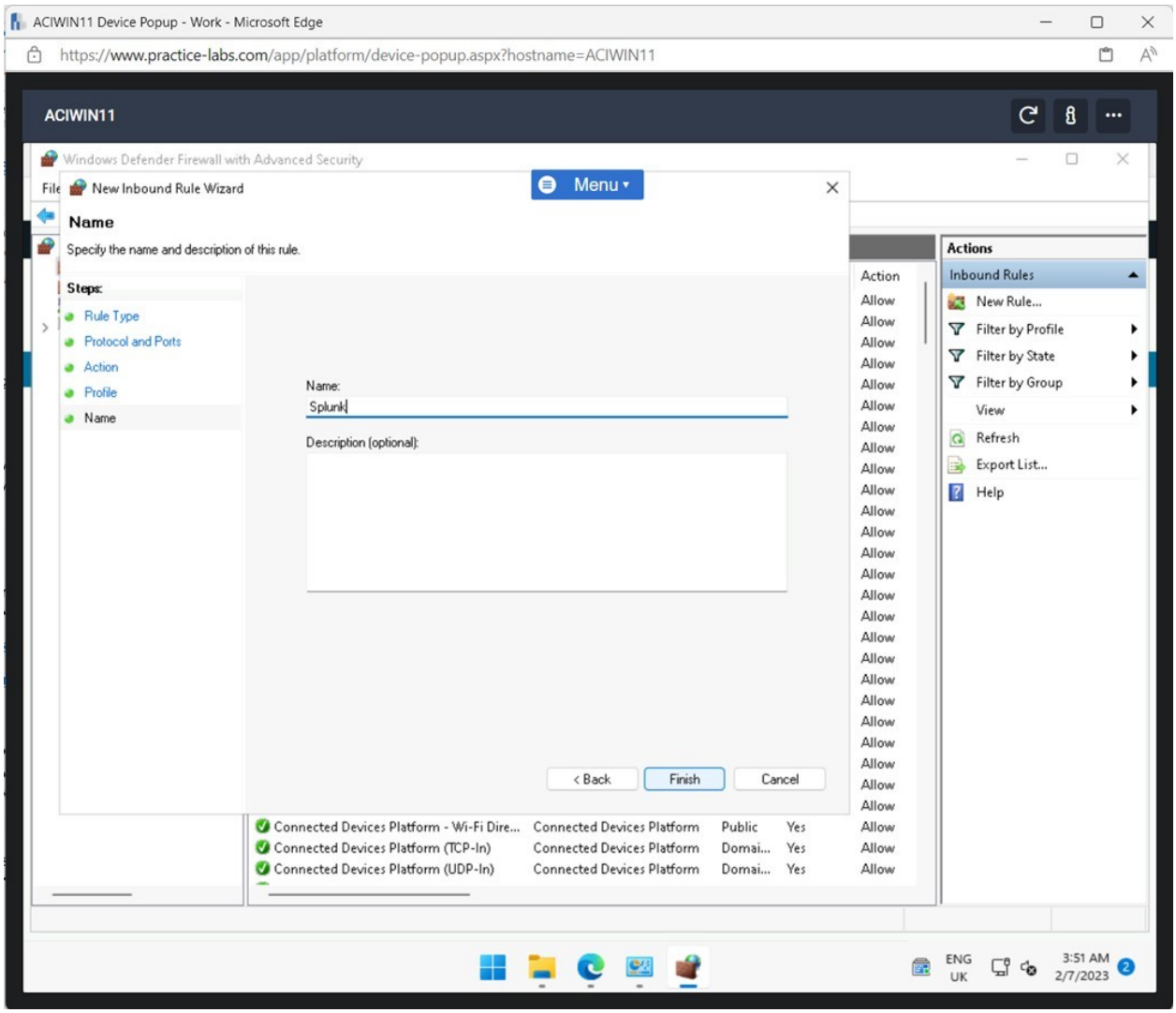
- Screenshot: Displaying selecting Port and clicking Next.
- Entered the following in the **Specific local ports** field:
- **8089, 9997**
- Clicked **Next**.



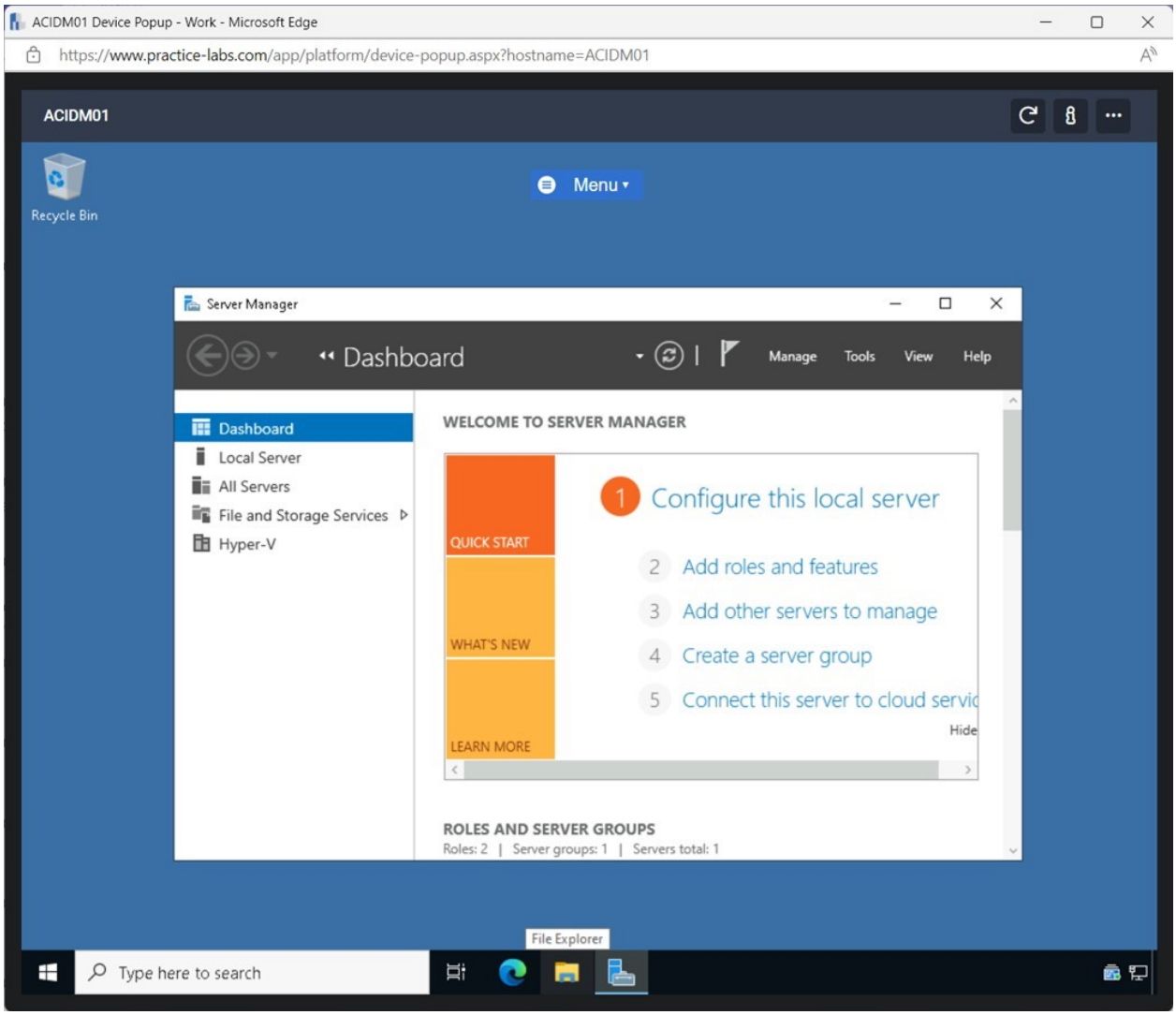
- Clicked **Next** on the **Action** and **Profile** windows.



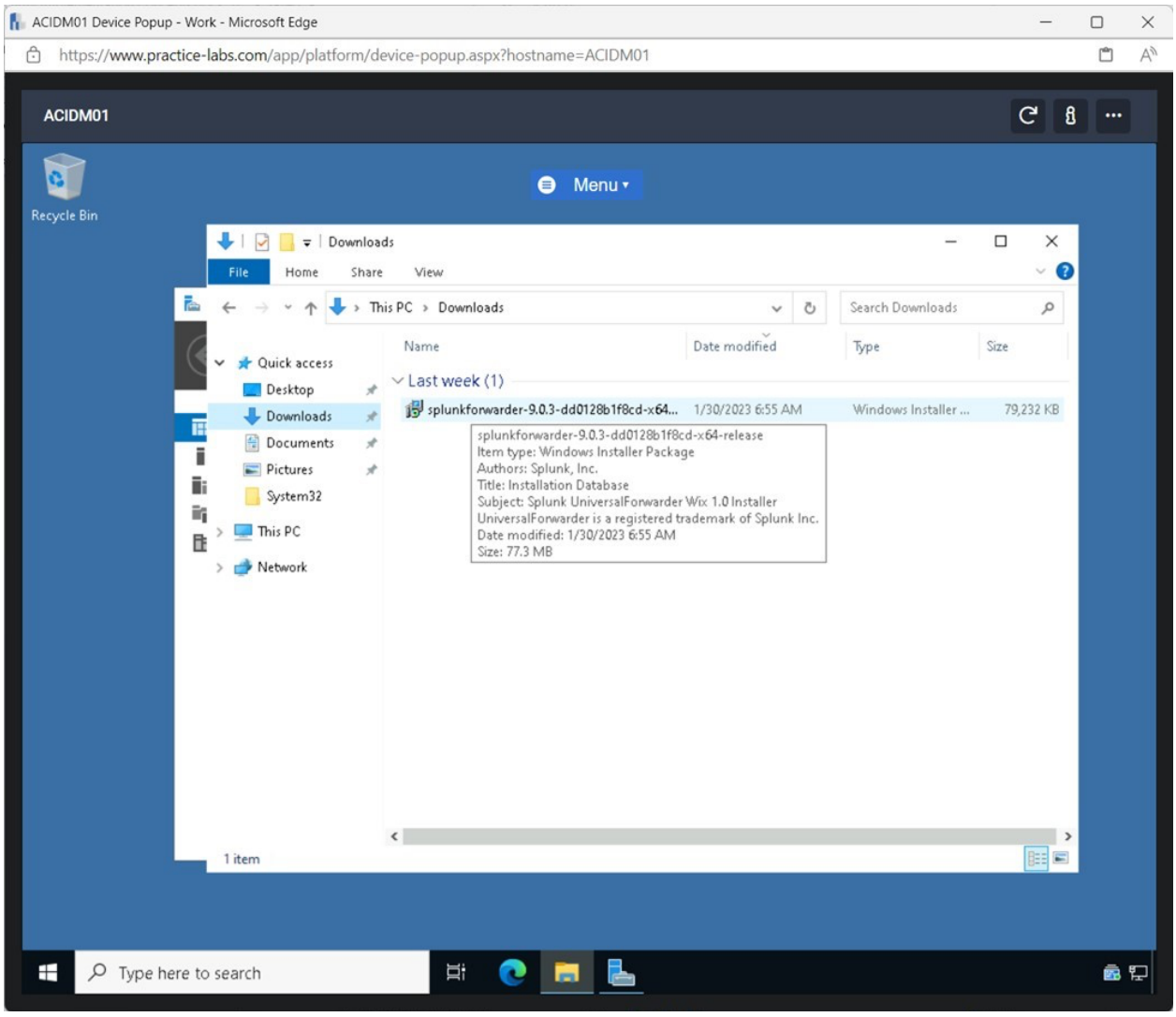
- Entered the following in the **Name** field and click **Finish**.
- **Splunk**

- 

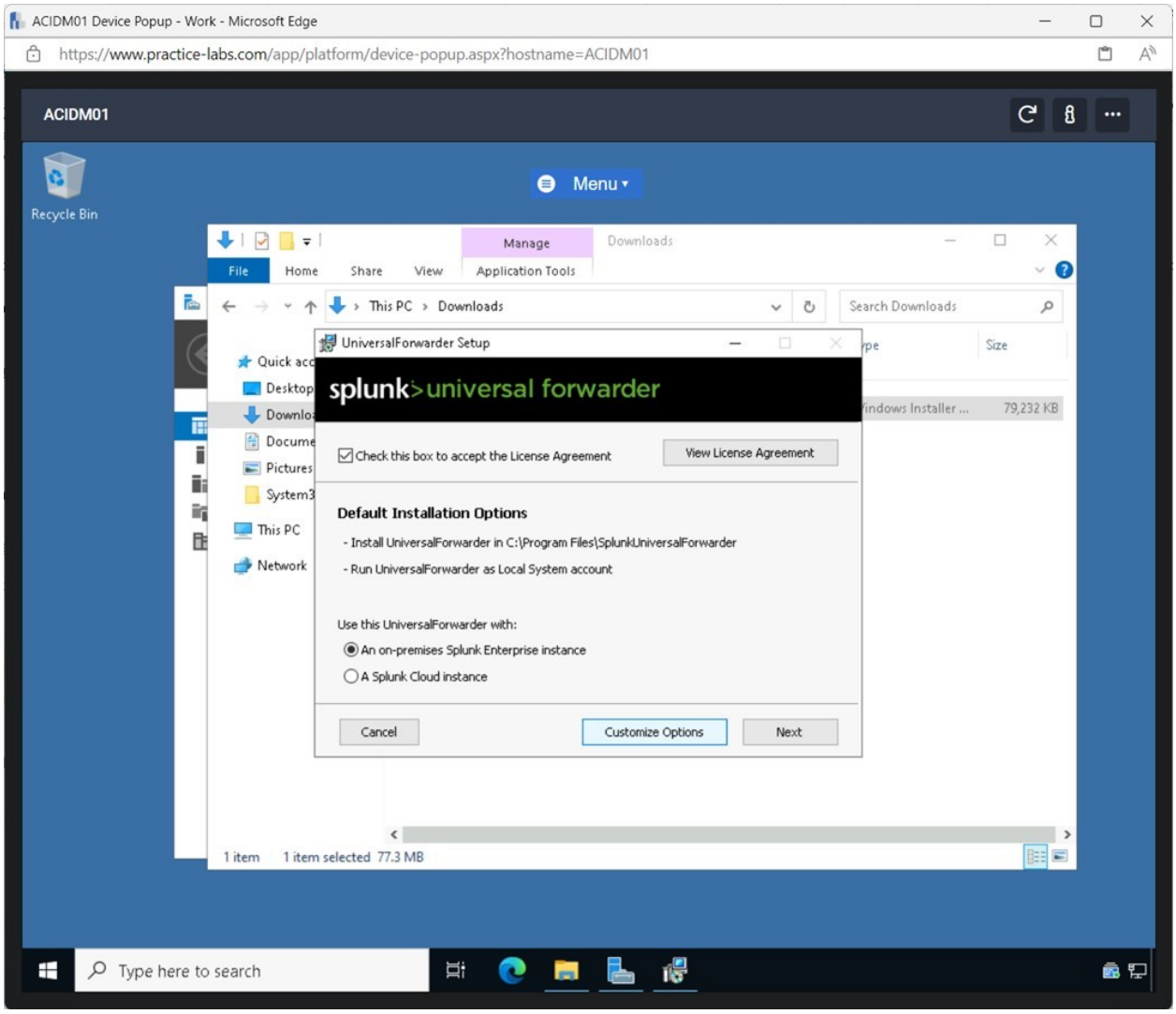
- **Action 2 - Configuring a Splunk Client**
- To ensure the devices on the network can send log activity, the device needed to be configured to facilitate this.
- I configured a client device to forward its logs to the Splunk Enterprise application.
- Connected to **VM.**
- Opened **File Explorer** from the **Taskbar.**



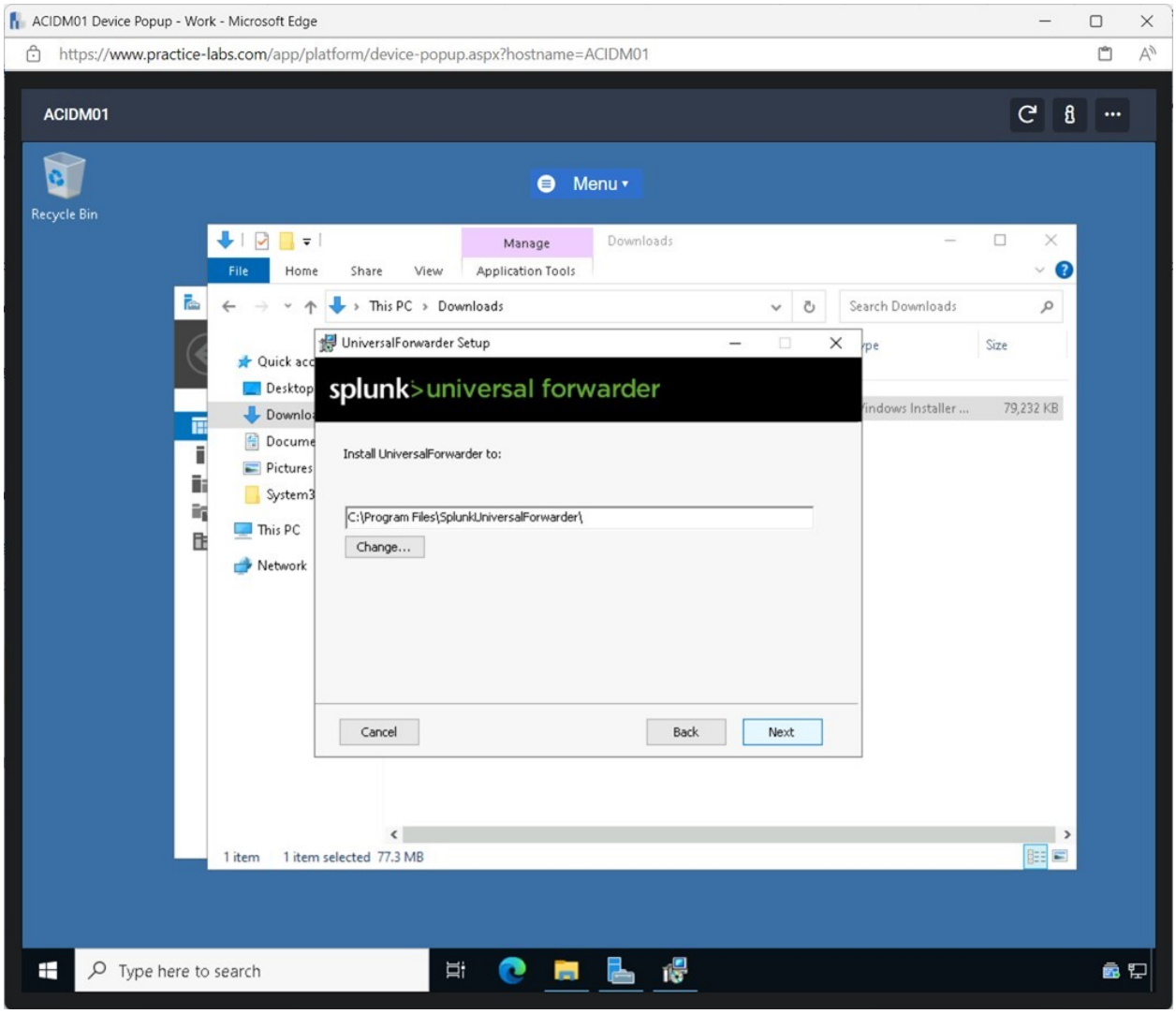
- In **File Explorer**, I selected the **Downloads** folder and double clicked the **splunk-forwarder-9.0.3** installation file.



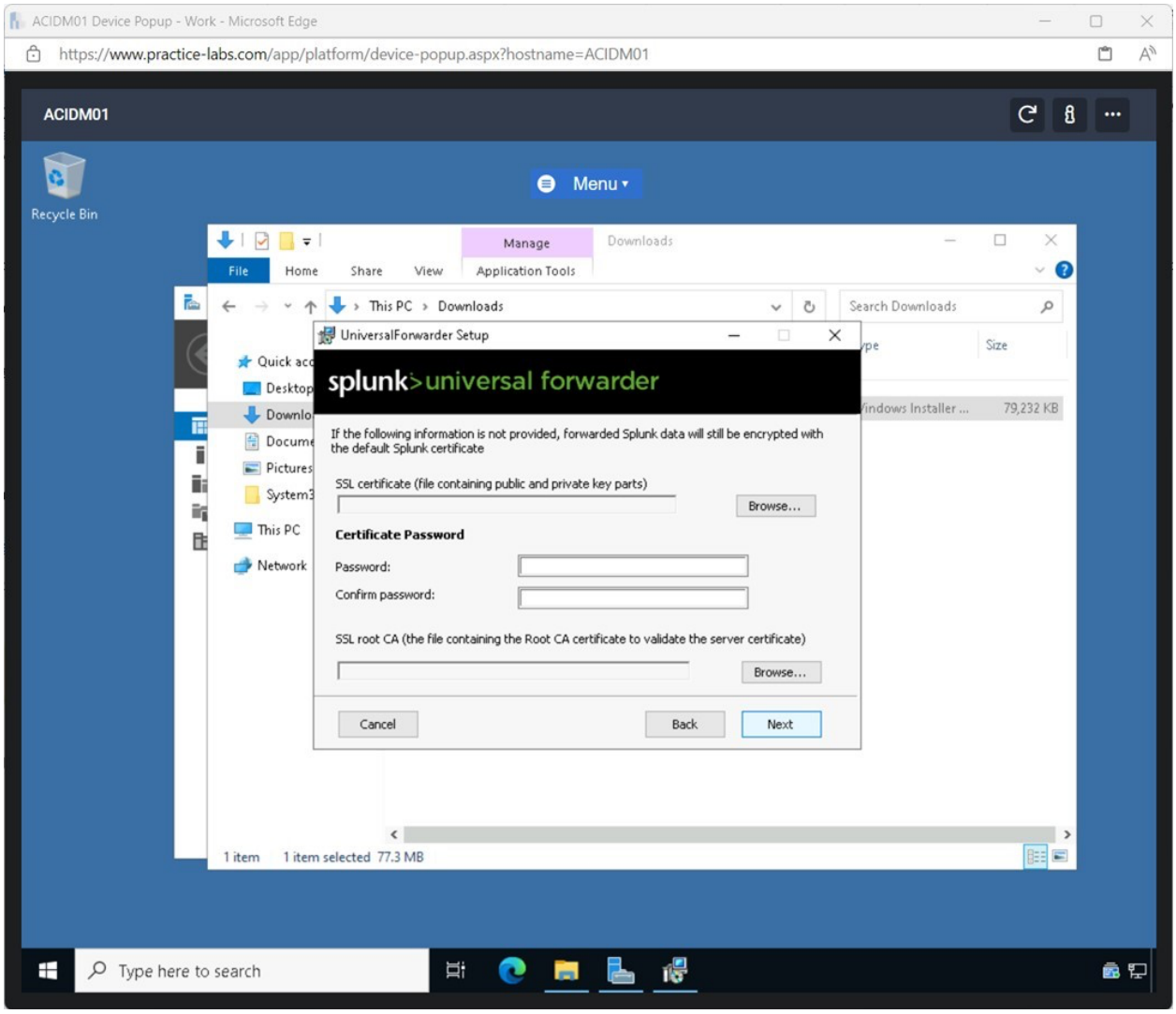
- Checked the **Check this box to accept the License Agreement** tick box and clicked **Customize Options**.



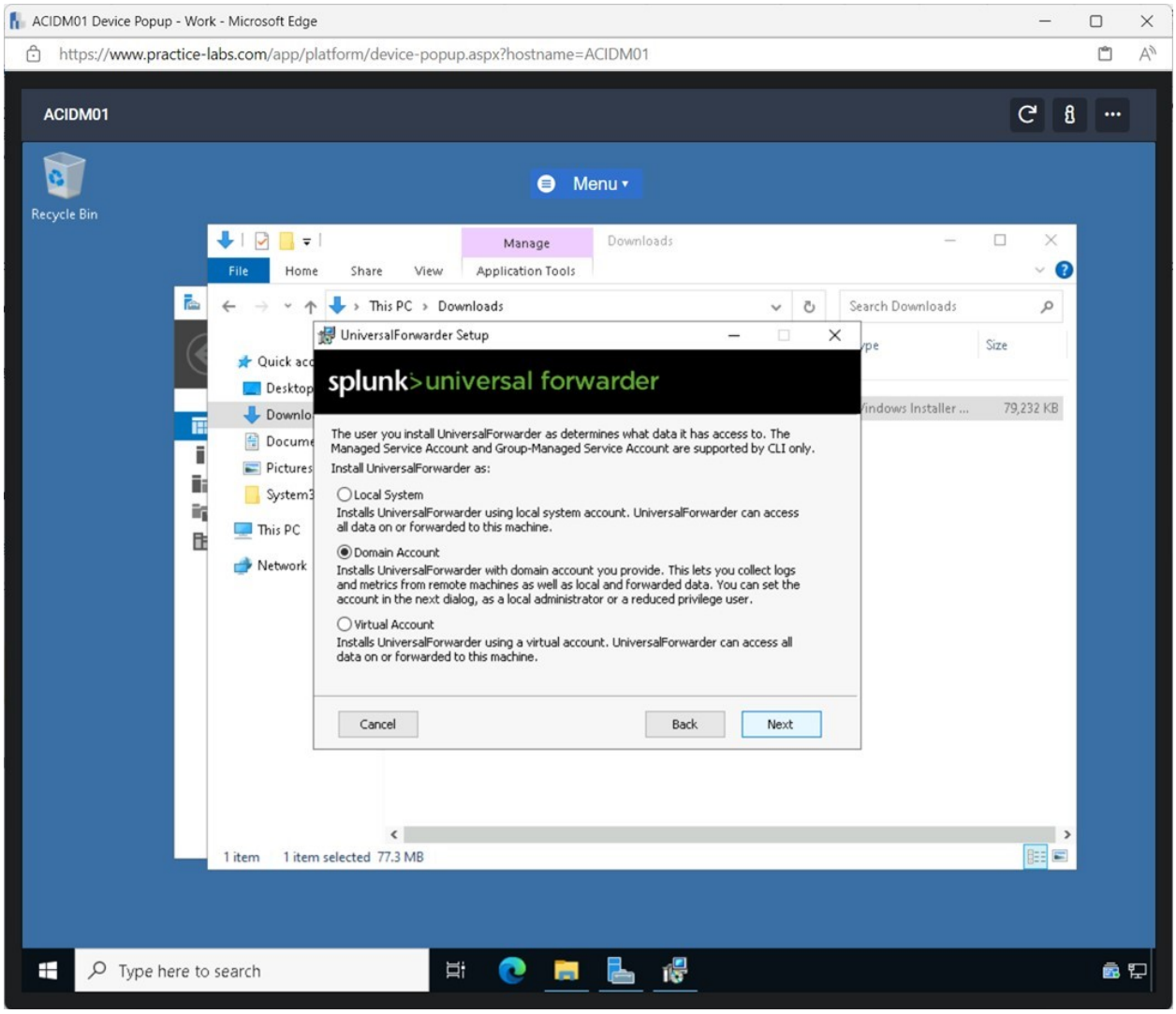
- Clicked **Next** on the **UniversalForwarder Setup** window.

- 

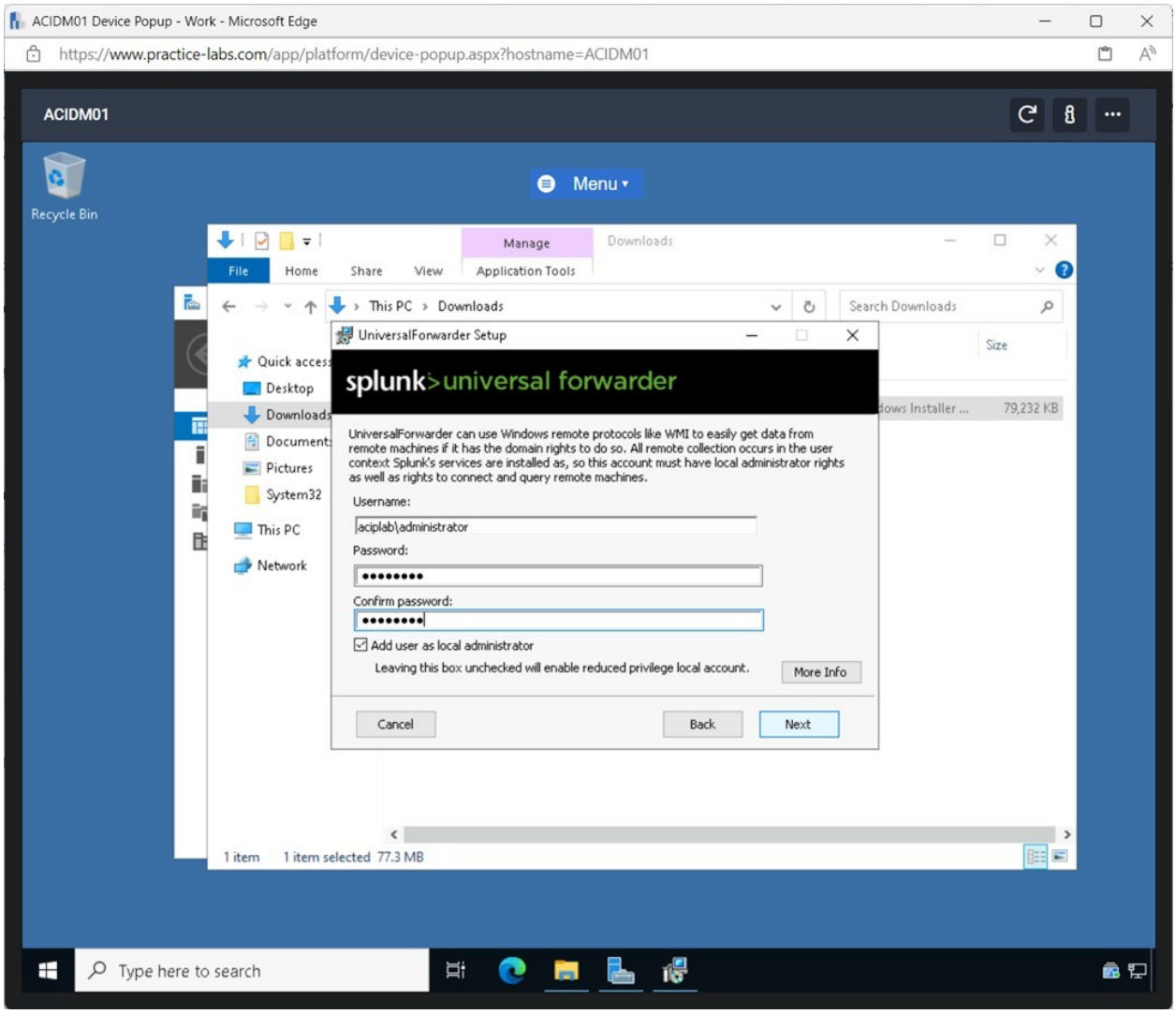
- Clicked **Next** on the next installation screen.



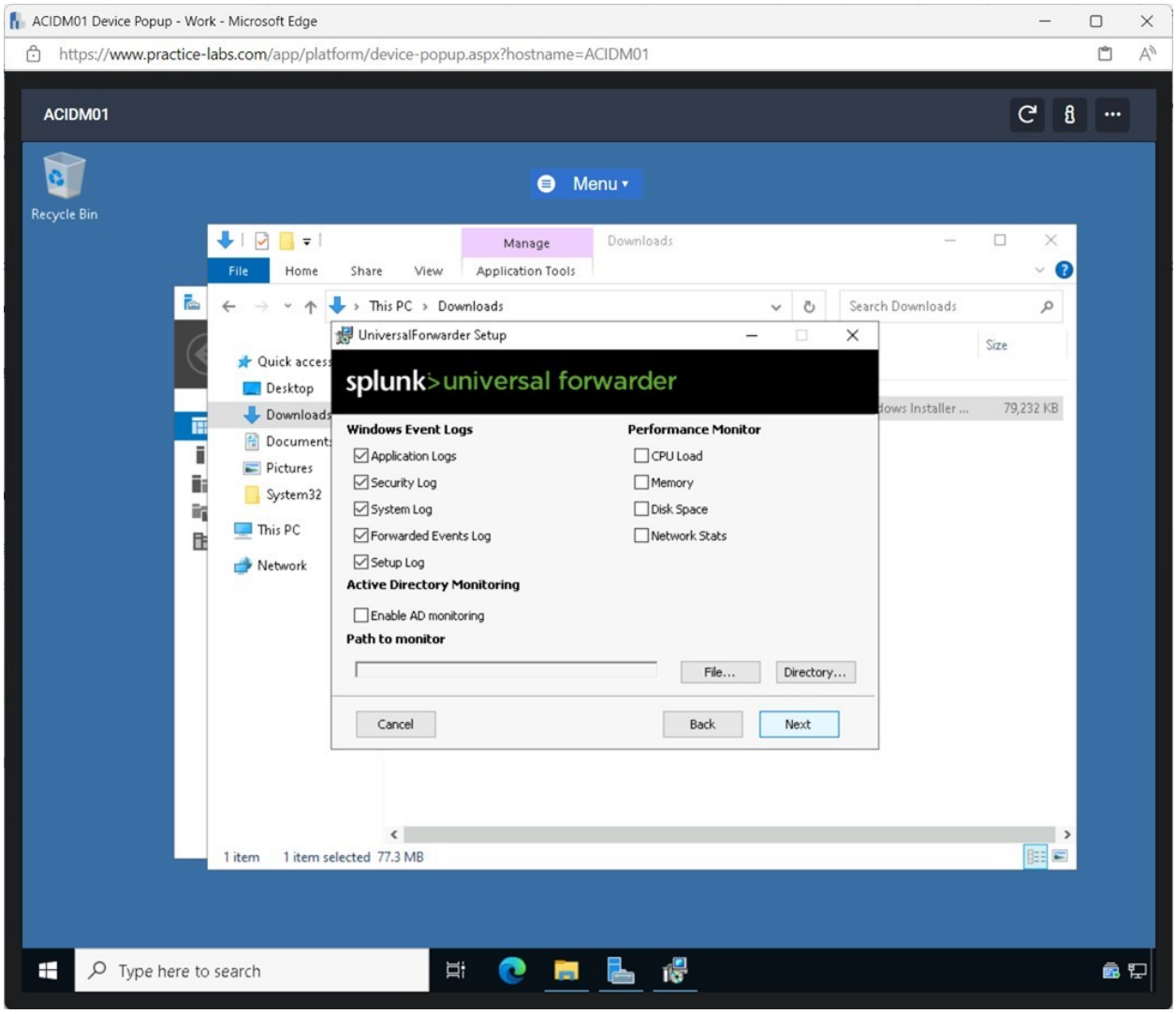
- Selected the **Domain Account** radio button and click **Next**.



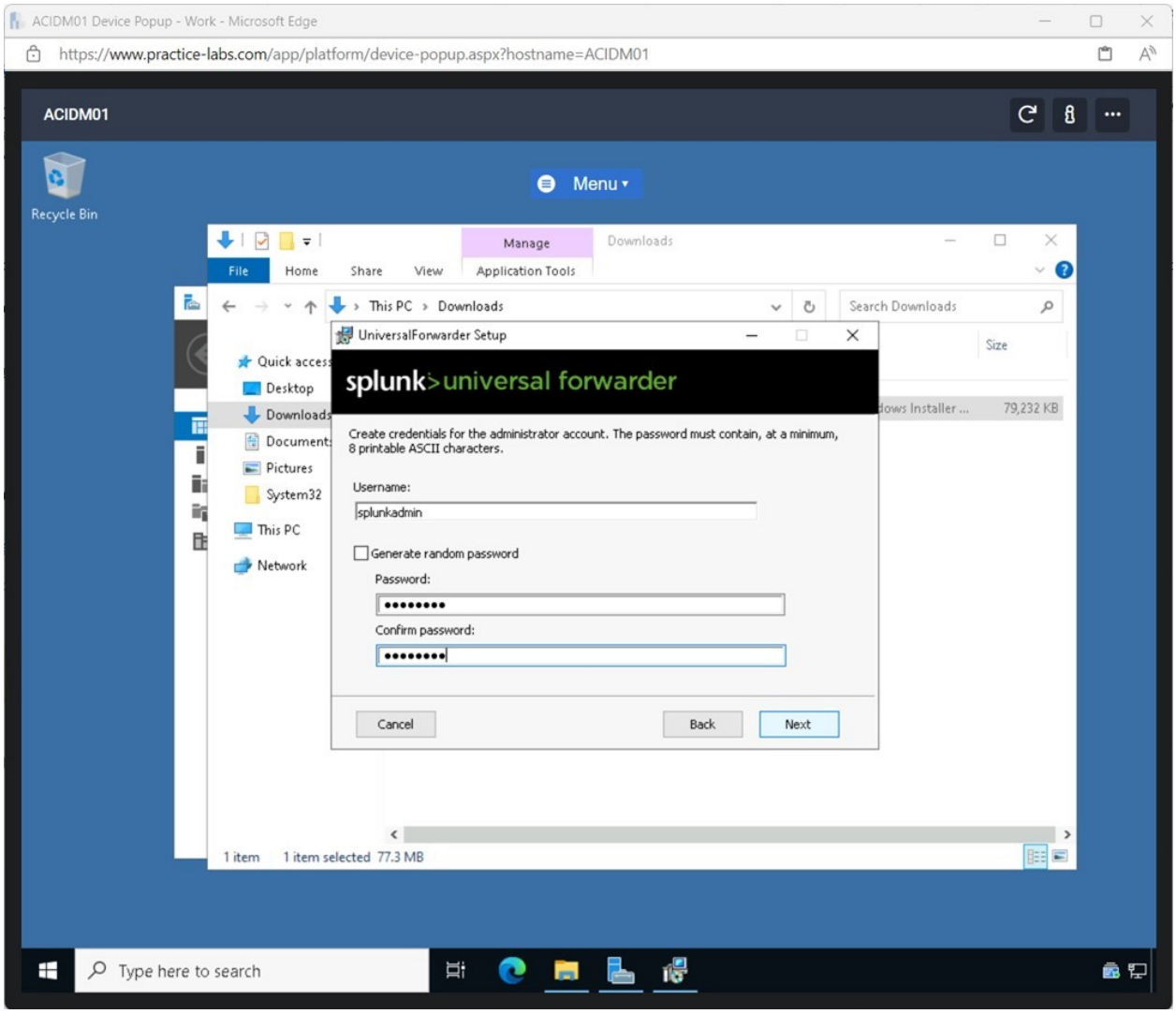
-
- Entered the following details on the **UniversalForwader Setup** screen:
- Username: aciplab\administrator
- Password: Passw0rd
- Confirm password: Passw0rd
- Clicked **Next**.



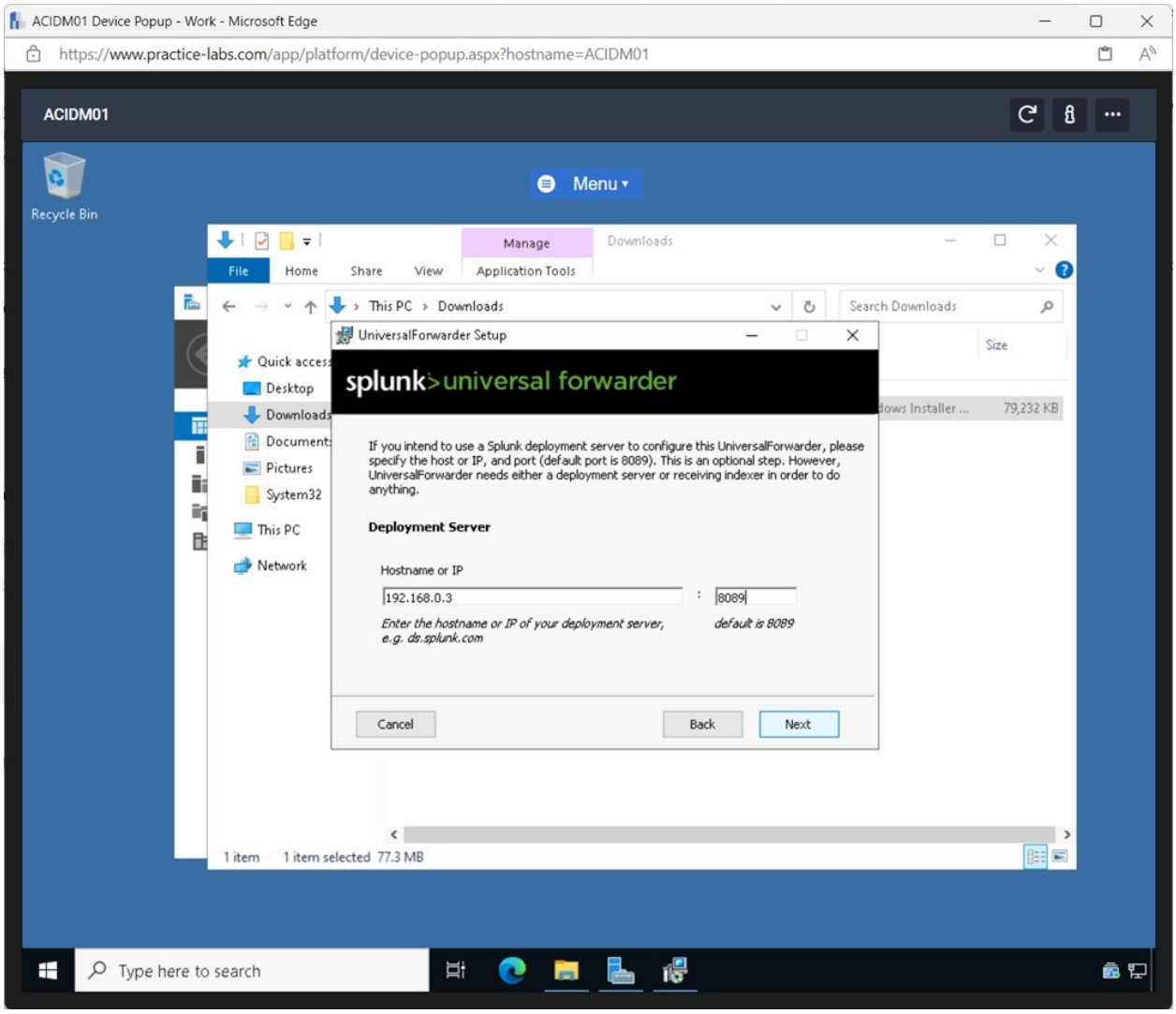
- On the **UniversalForwarder Setup** screen, I clicked all the boxes in the **Windows Event Logs** pane.
- Clicked **Next**.



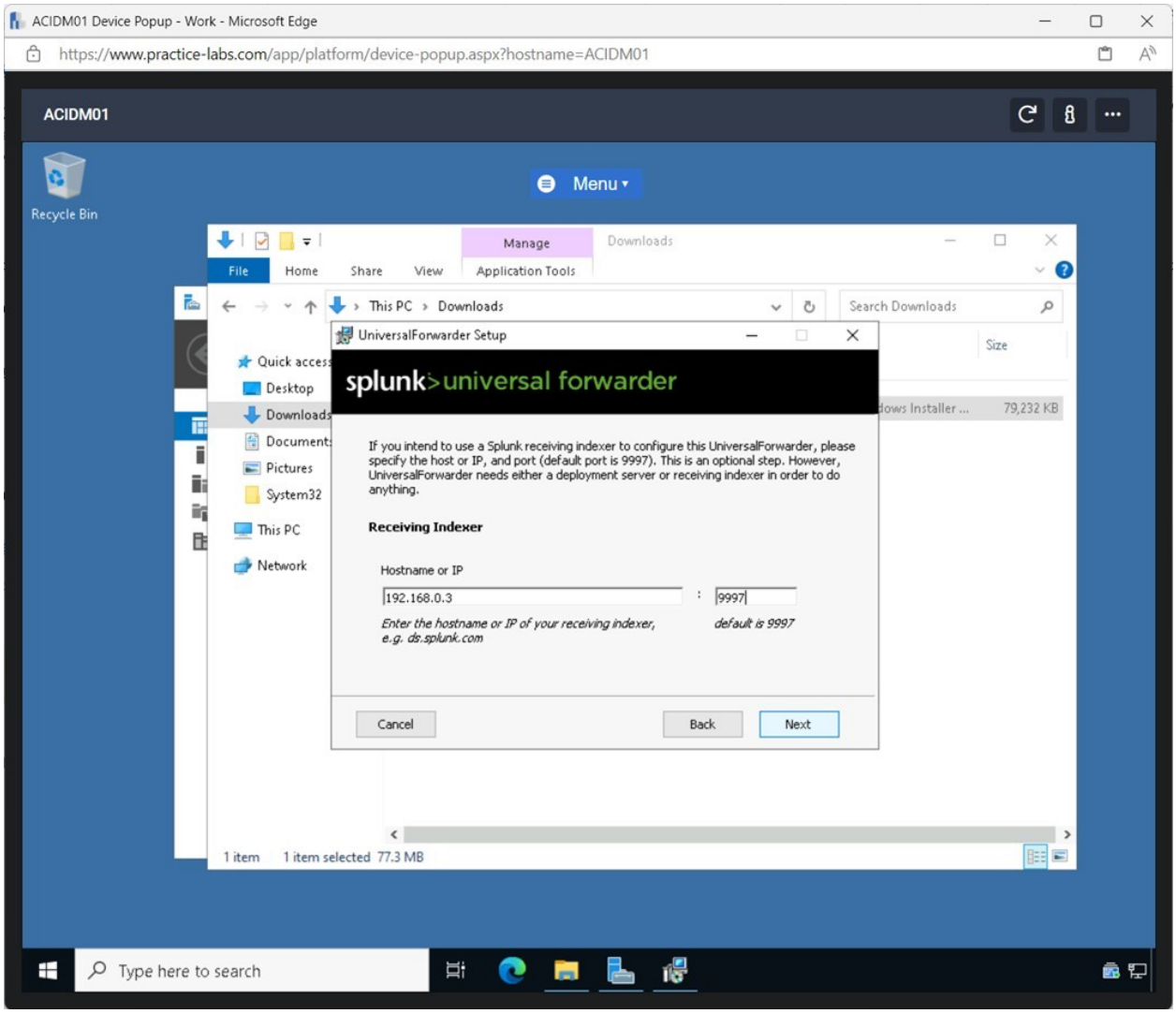
- Unchecked the **Generate random password** tick box.
- Entered the following details on the **UniversalForwader Setup** screen:
- Username: splunkadmin
- Password: Passw0rd
- Confirm password: Passw0rd
- Clicked **Next**.



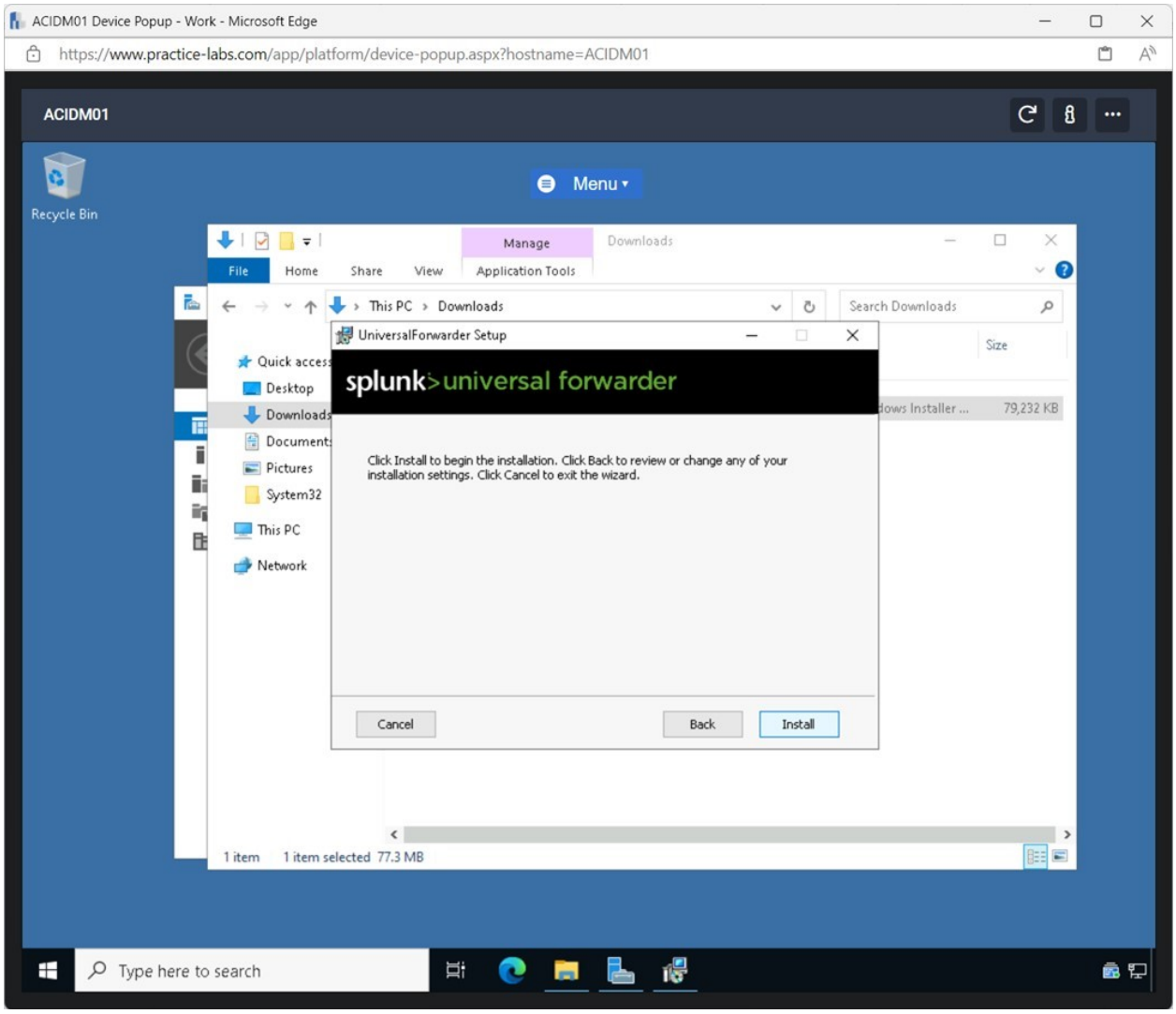
- In the **Hostname or IP** field, entered the following:
- **192.168.0.3**
- In the port field, entered the following:
- **8089**
- Clicked **Next**.



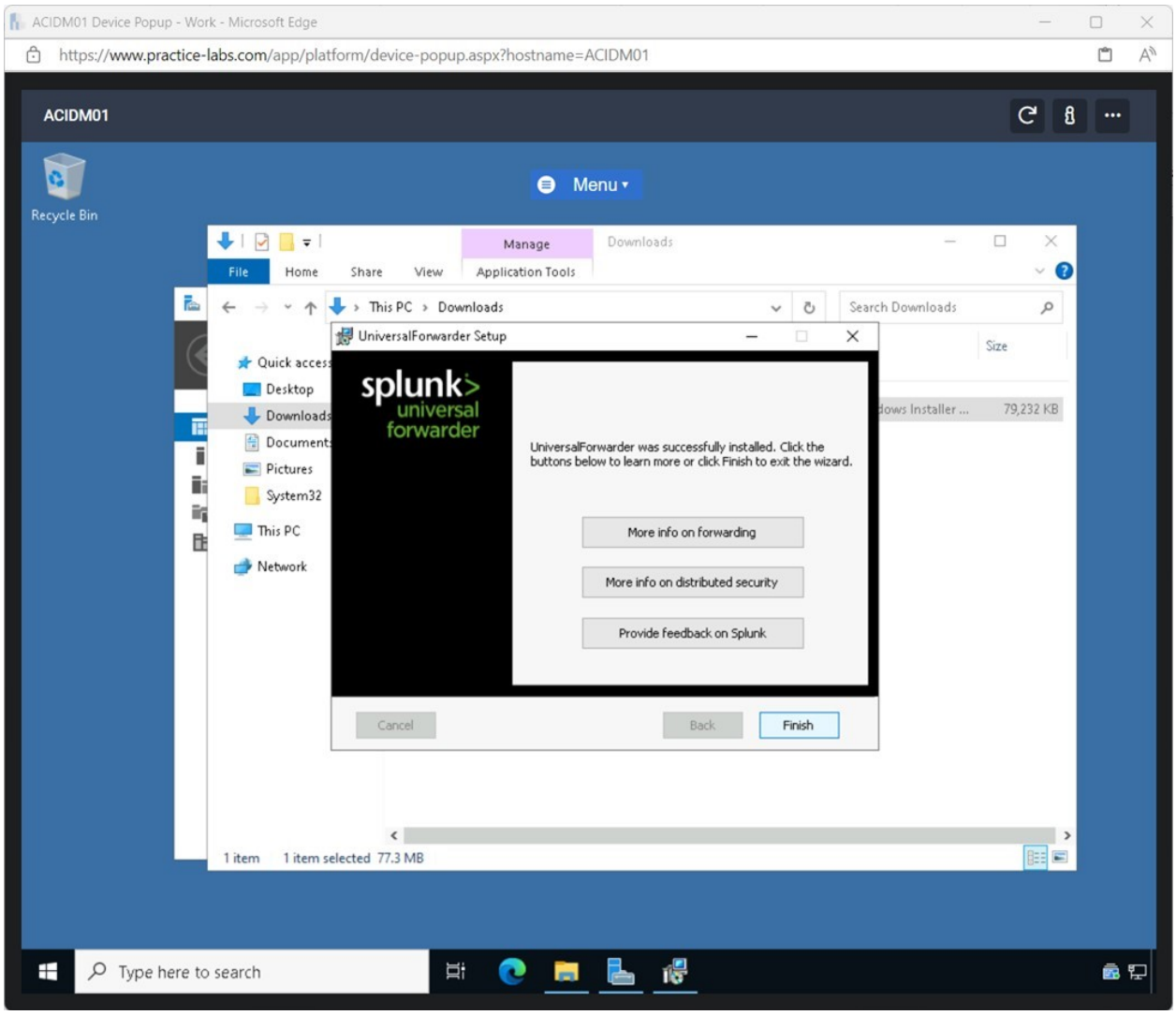
-
- In the **Hostname or IP** field, entered the following:
- **192.168.0.3**
- In the port field, entered the following:
- **9997**
- Clicked **Next**.



- Clicked **Install** on the **UniversalForwarder Setup** window.

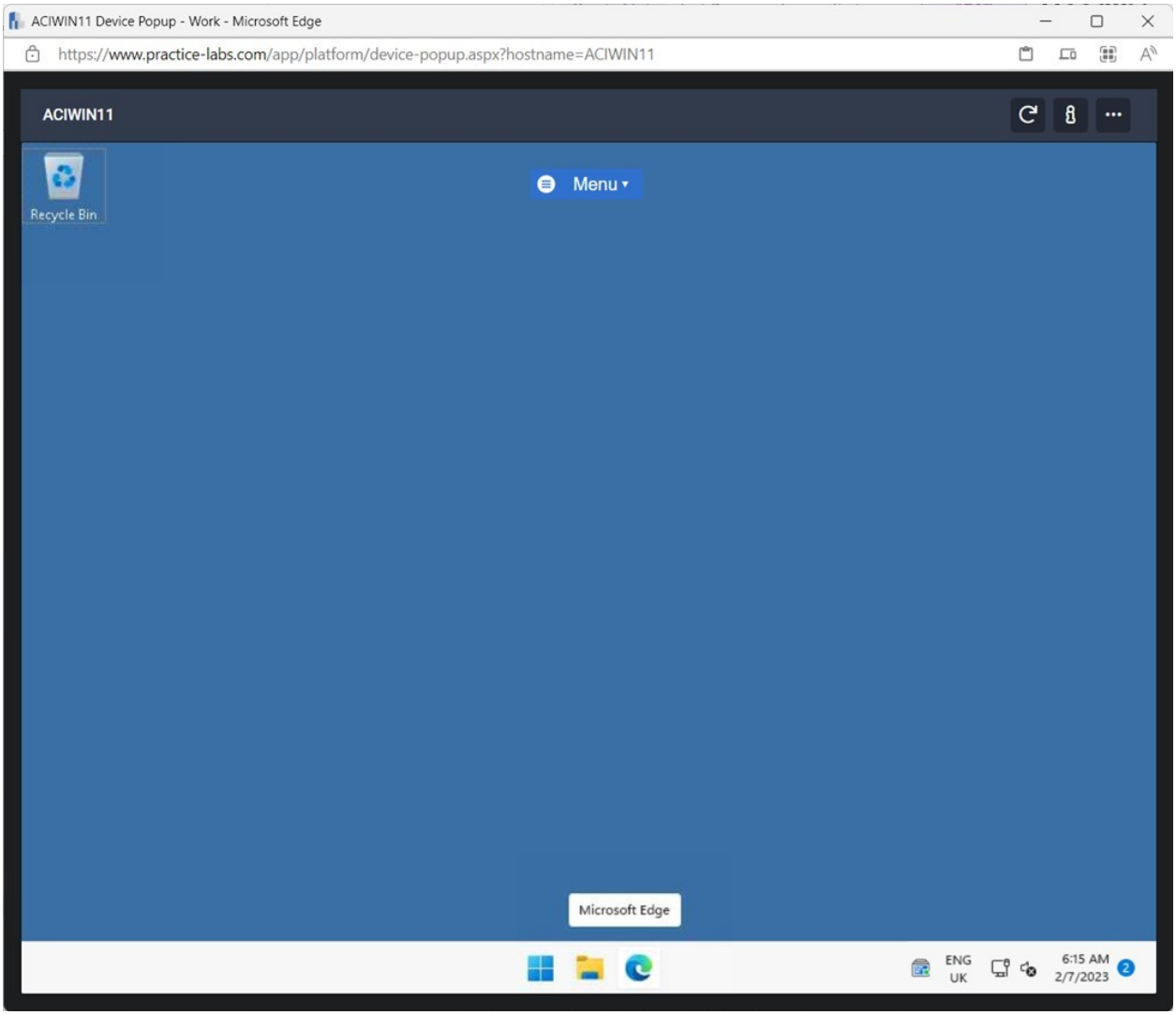


- After the installation has been completed, I clicked **Finish**.

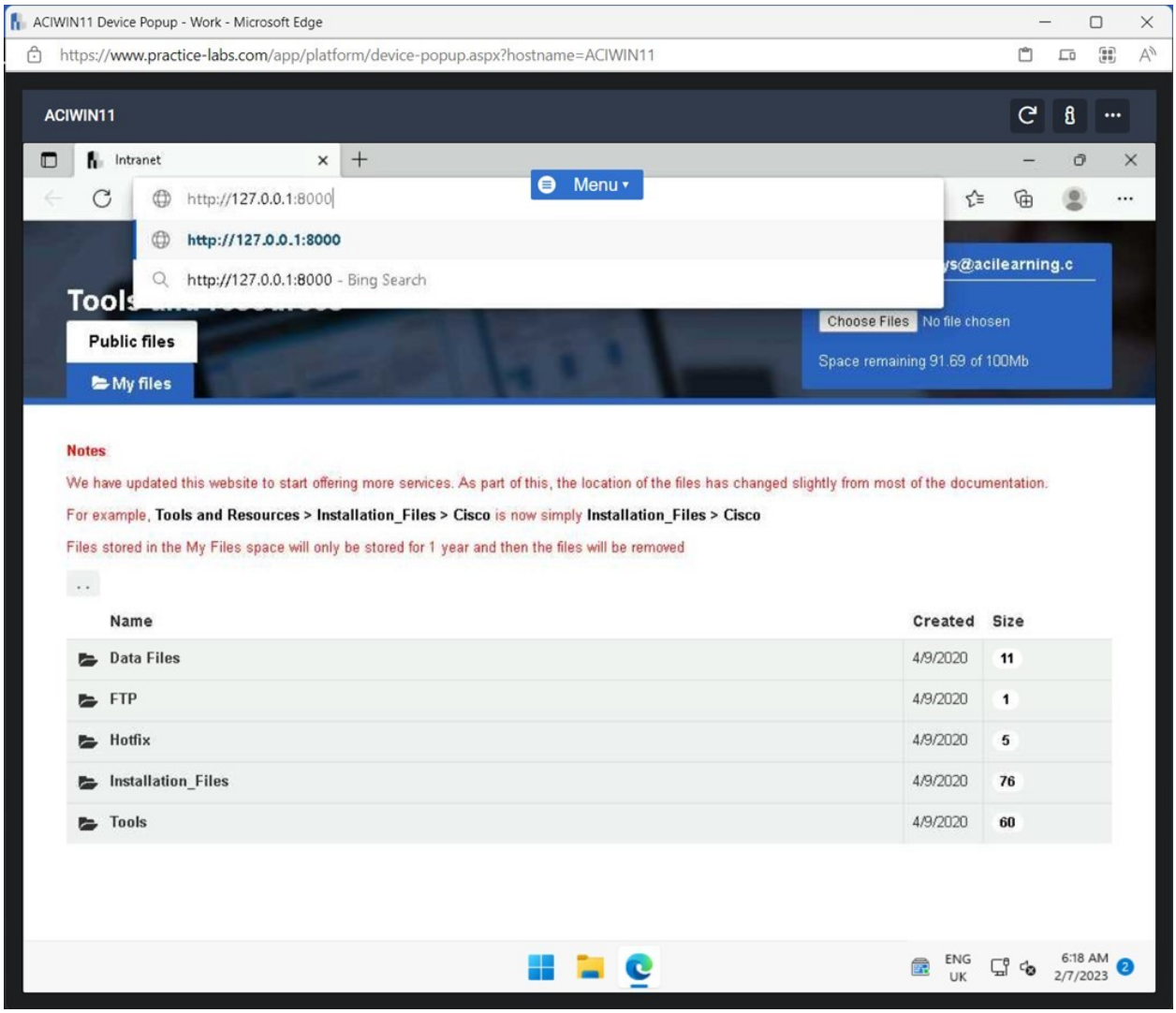
- 

Action 3 - Collect Logs using Splunk Enterprise

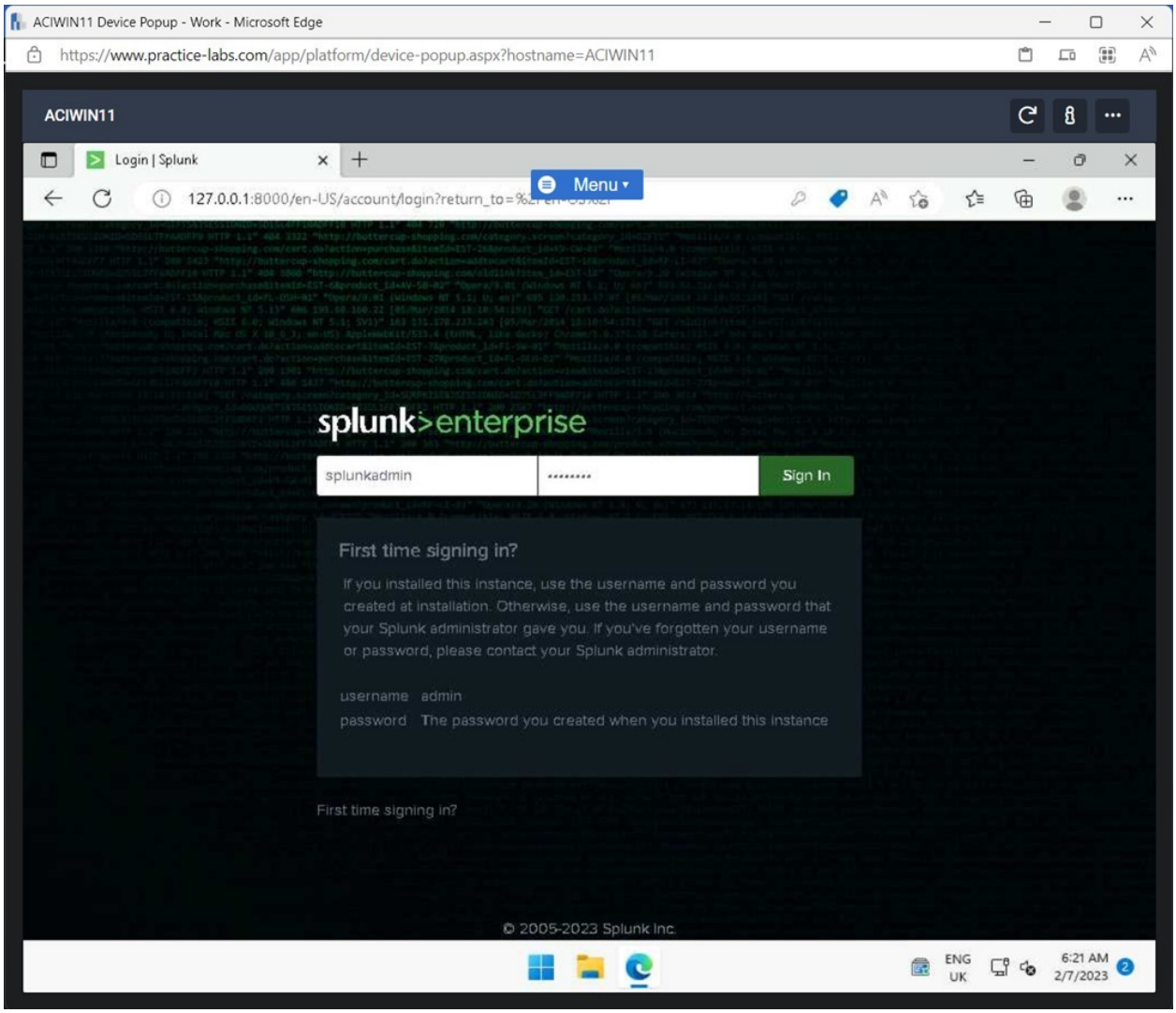
- I collected logs from a VM using the Splunk Enterprise application.
- Connected to computer and opened **Microsoft Edge** from the **Taskbar**.



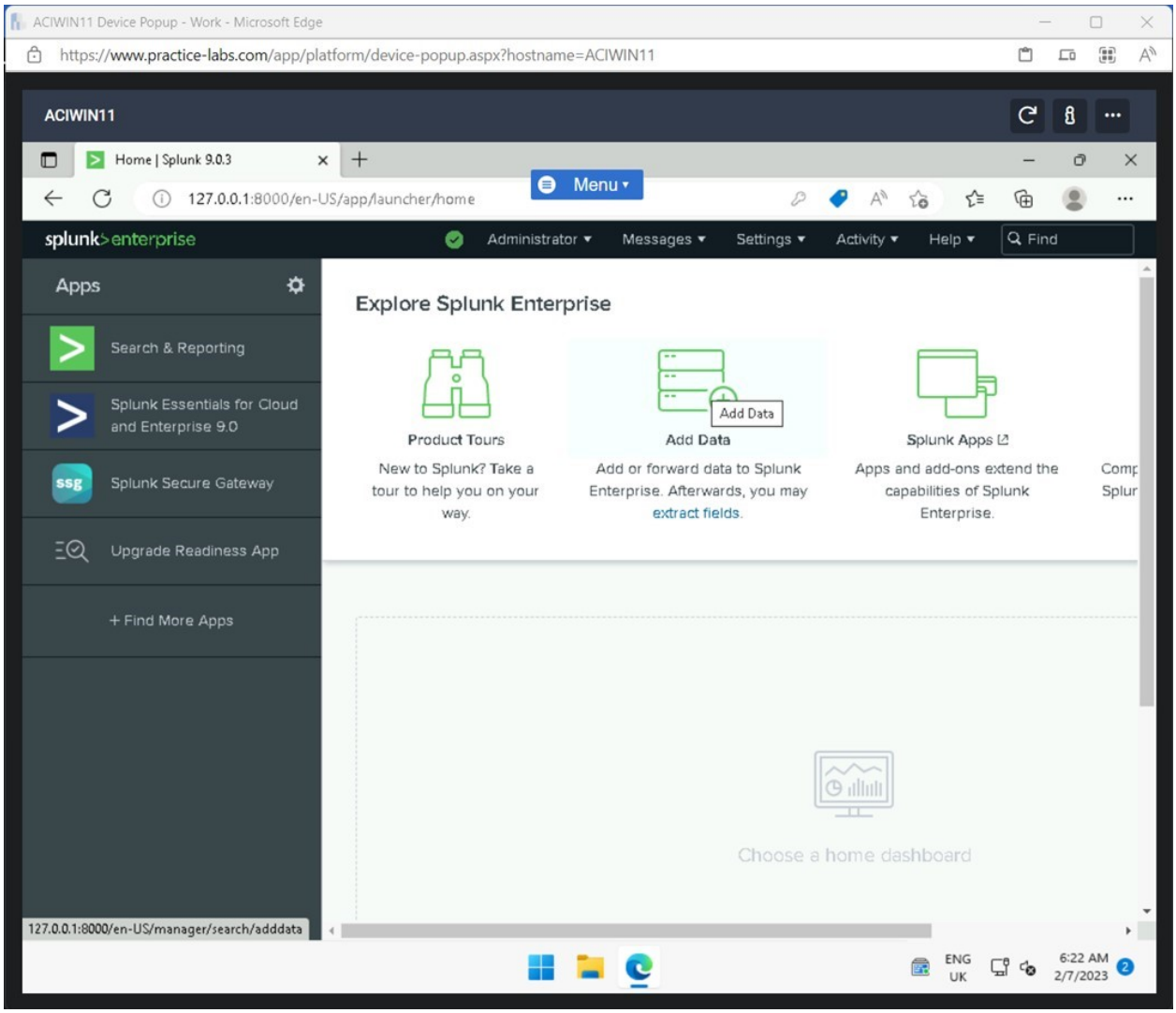
- In the **Microsoft Edge** browser, browsed to the following URL:
- **http://127.0.0.1:8000**



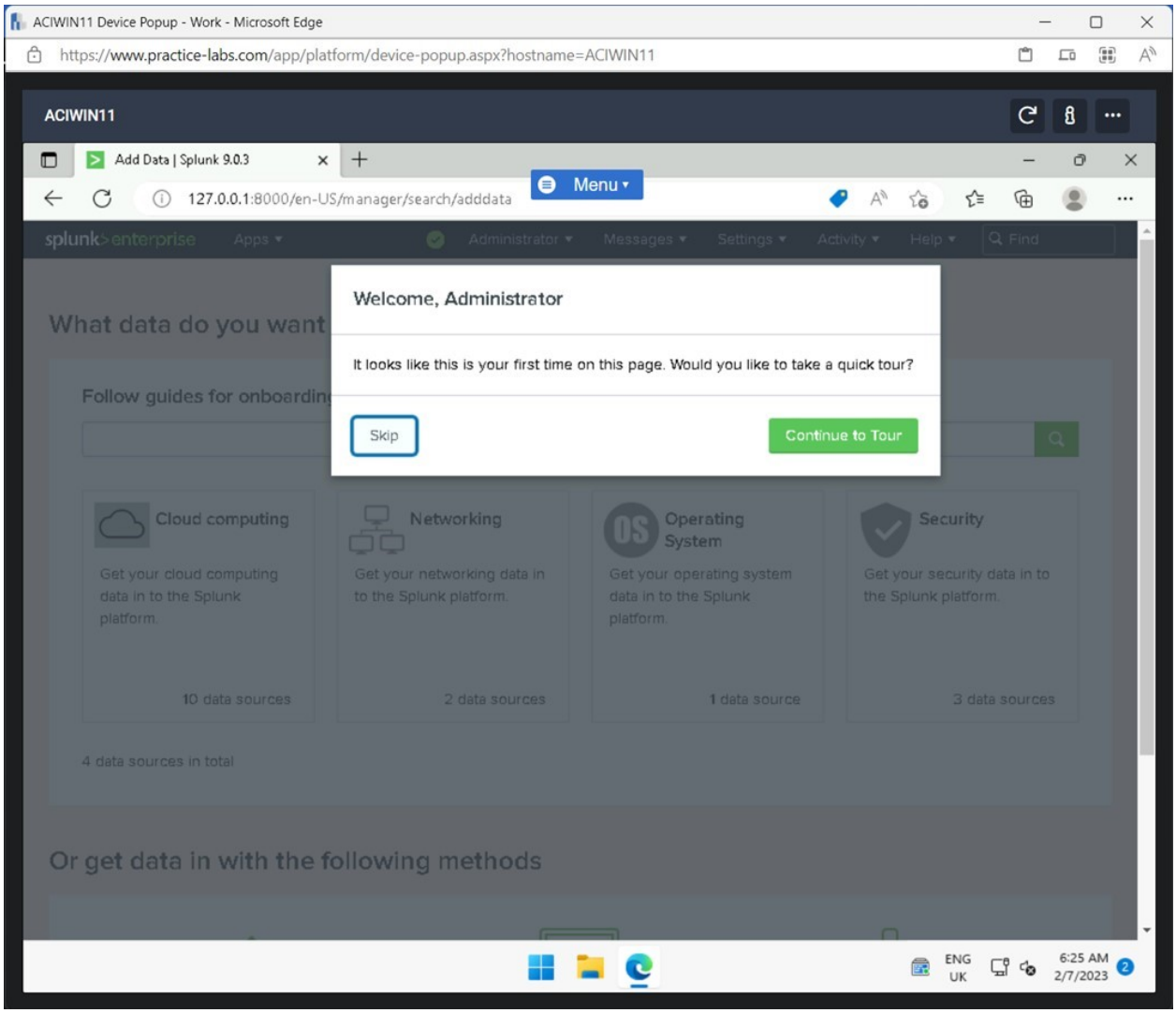
- When prompted, I entered the following credentials:
- **Username: splunkadmin**
- **Password: Passw0rd**
- Clicked **Sign In**.

- 

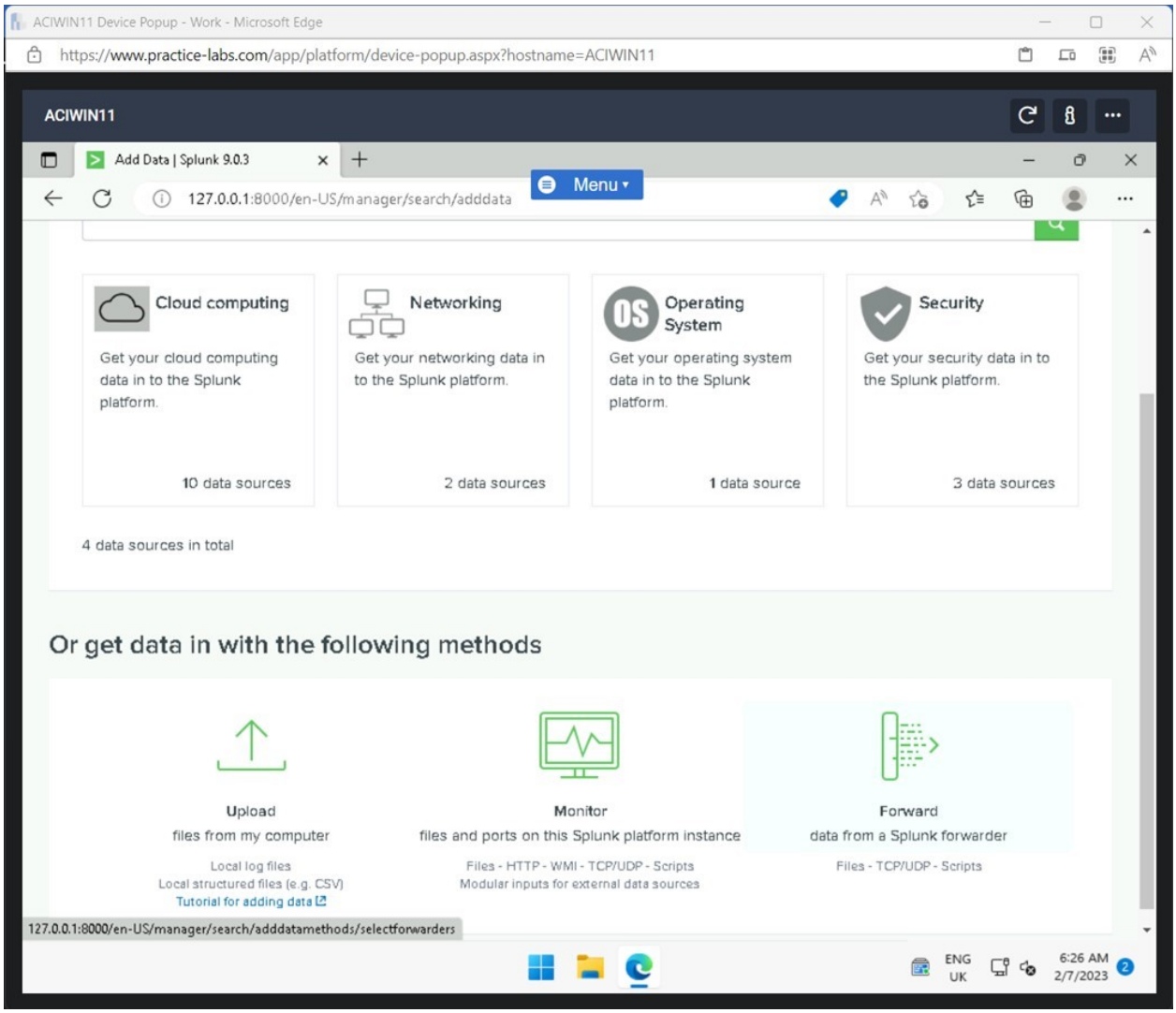
- Clicked **Add Data** in the **Explore Splunk Enterprise** pane.



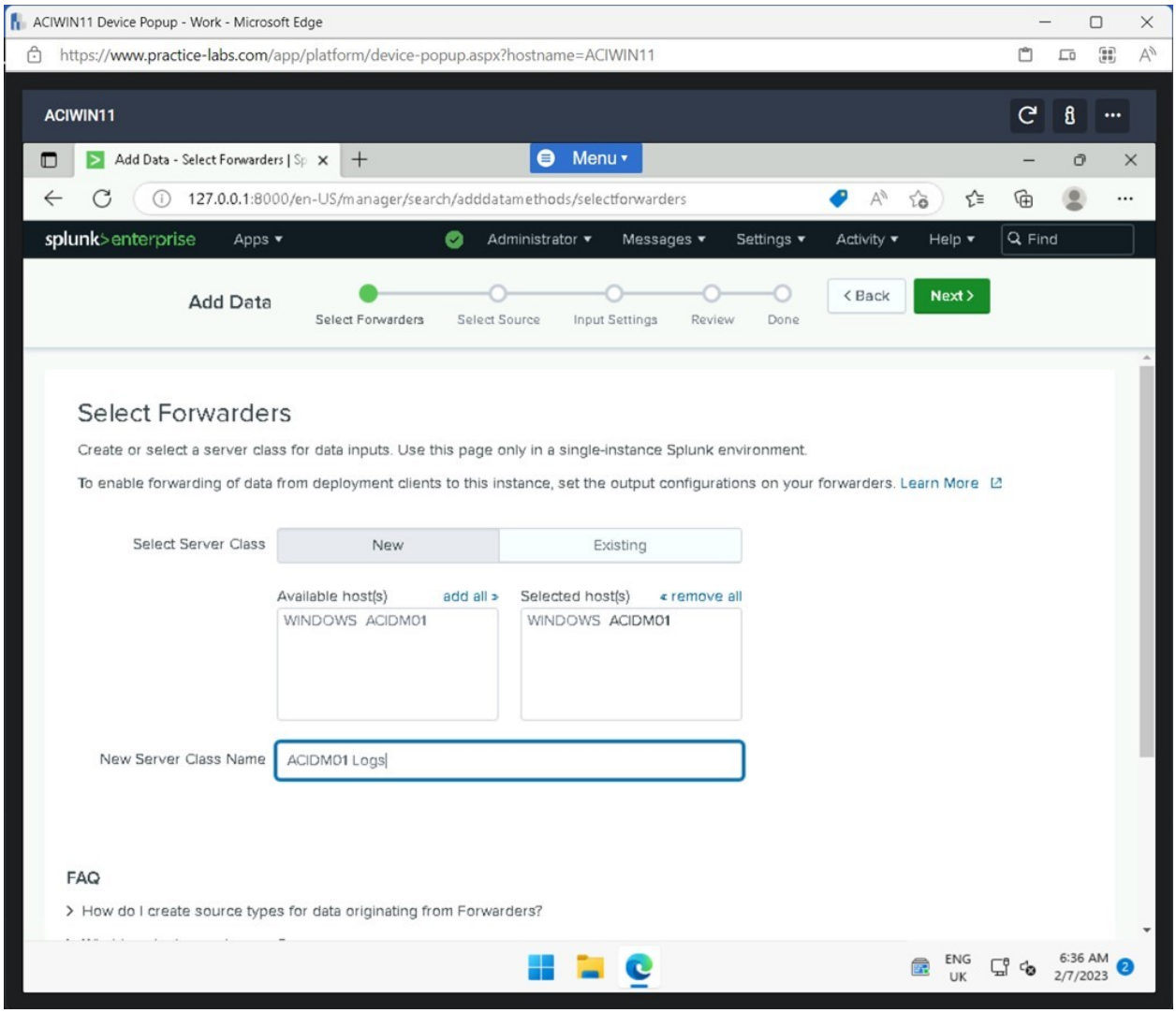
- When the **Welcome Administrator** window popped up, I clicked **Skip**.



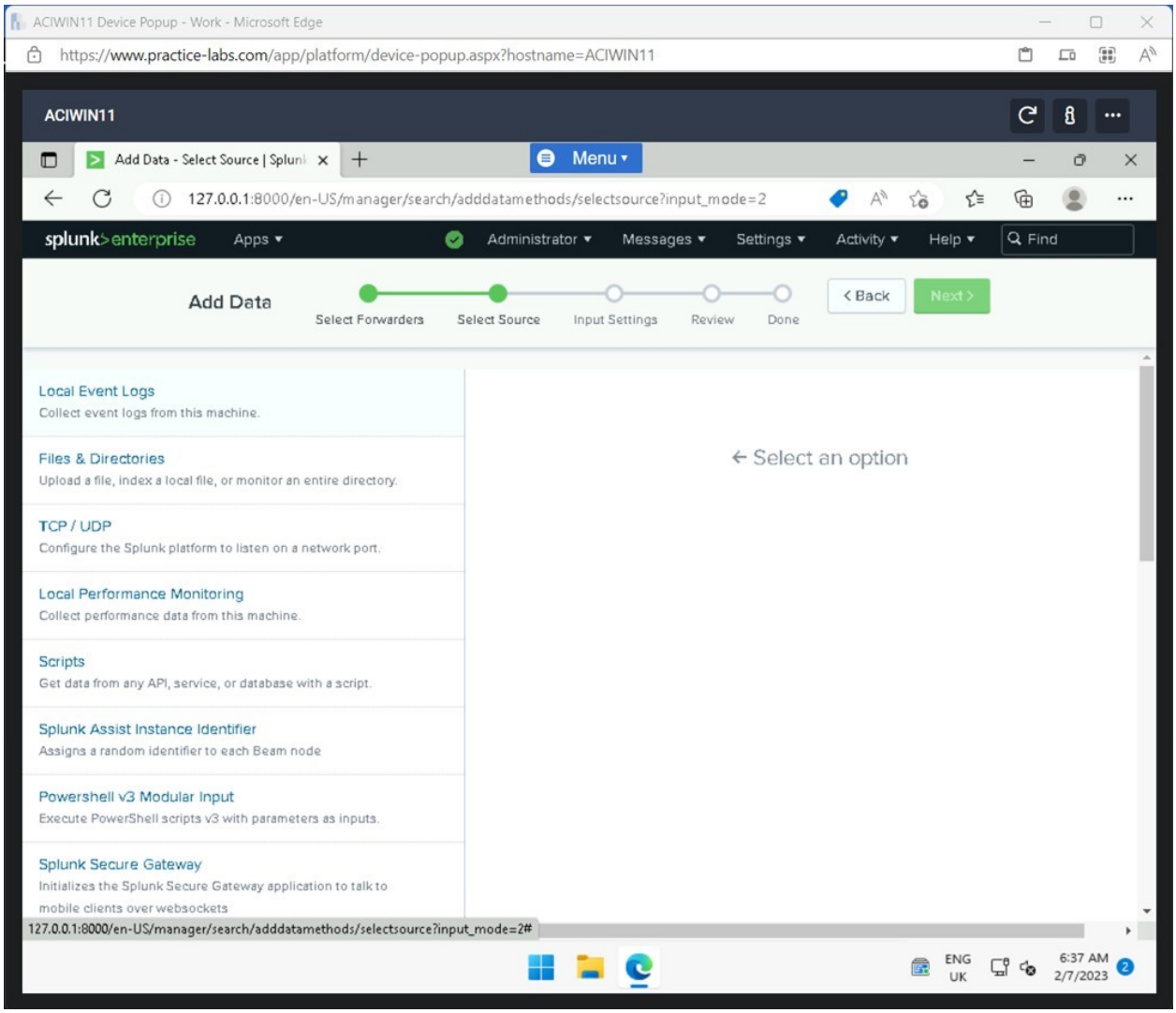
- I selected **Forward data from a Splunk forwarder**.



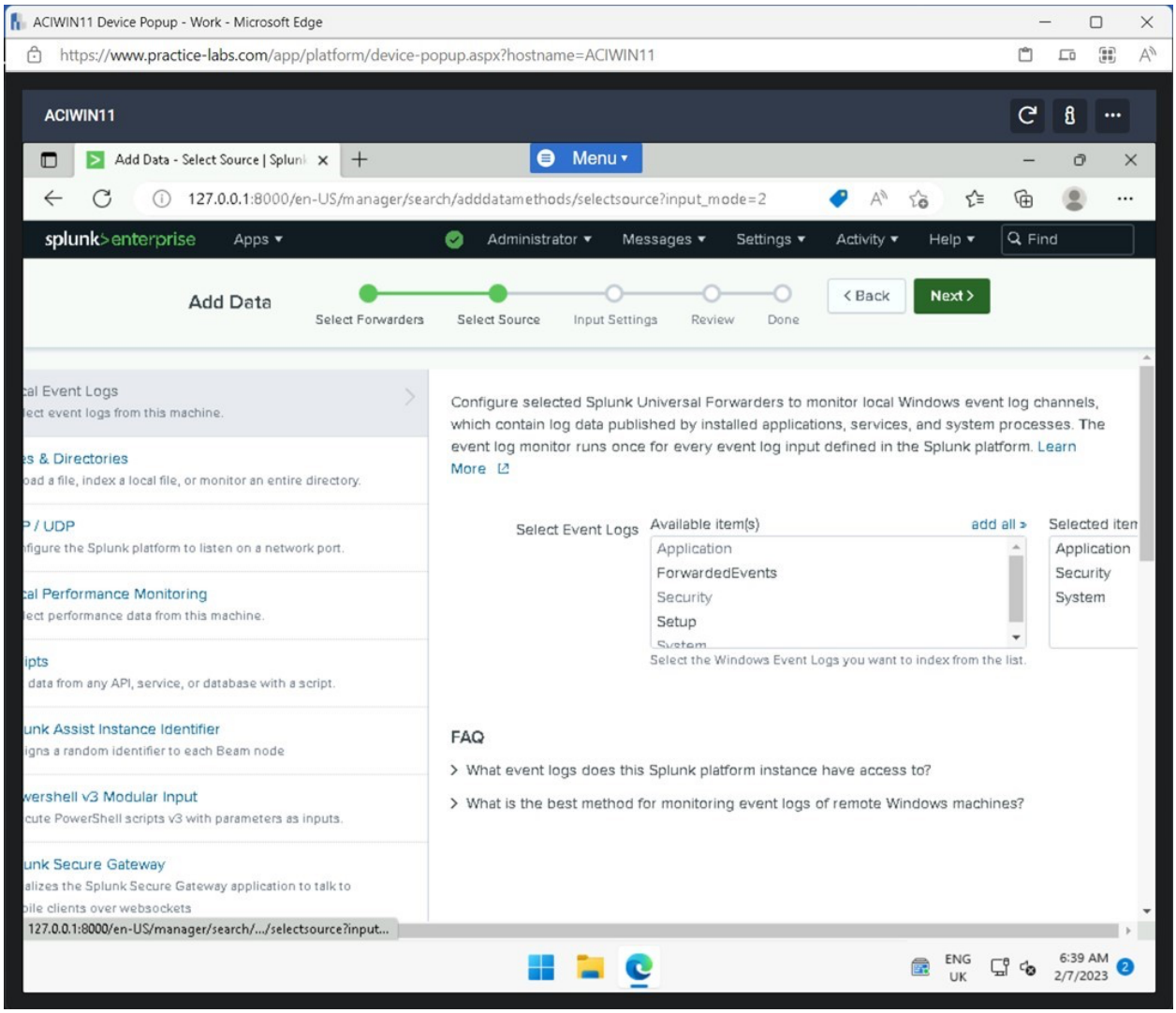
- On the **Add Data** window, I entered the following in the **New Server Class Name** field:
- **ACIDM01 Logs**
- Clicked **WINDOWS ACIDM01** in the **Available host(s)** pane.
- Clicked **Next**.



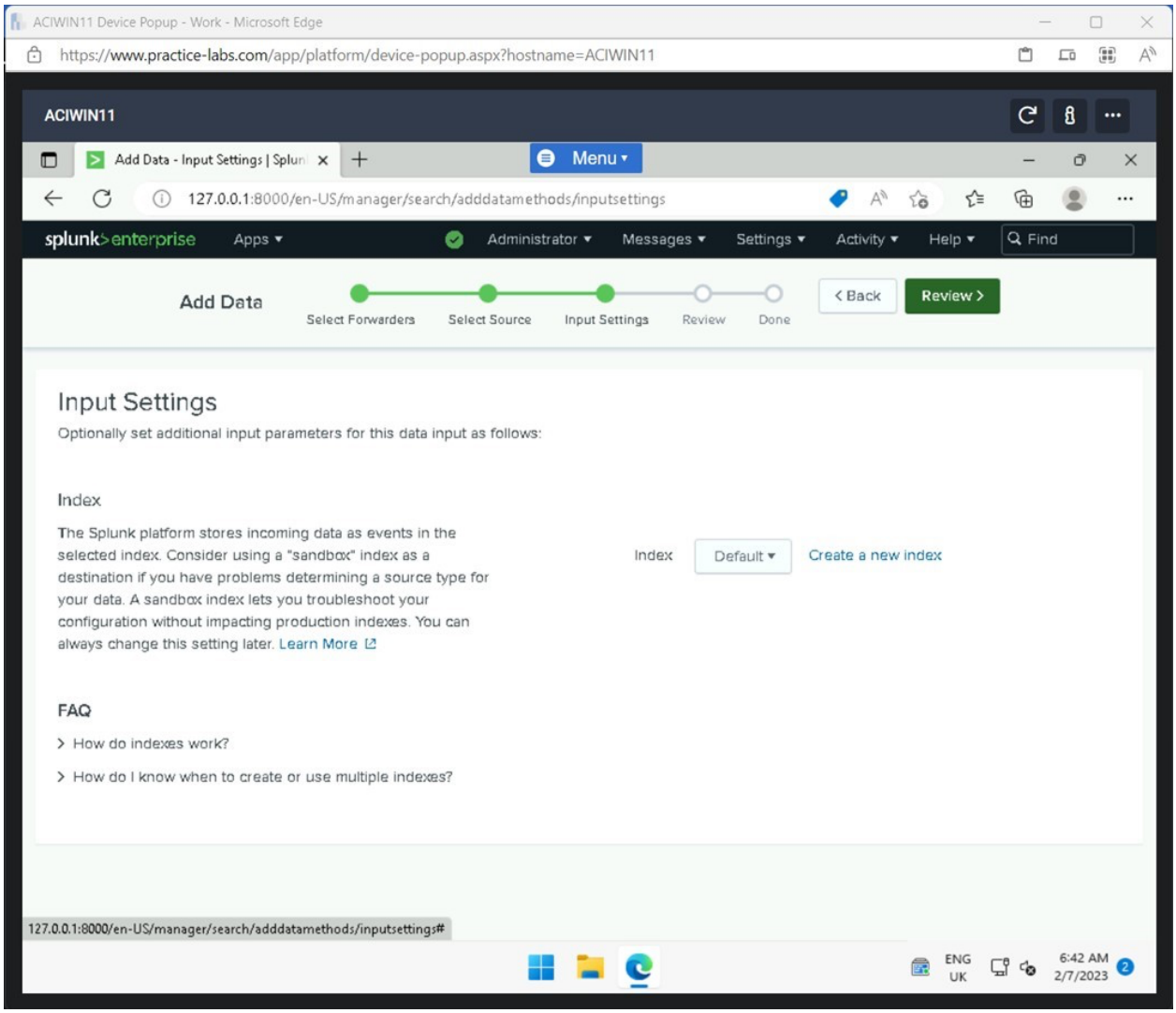
- Clicked **Local Event Logs** on the **Select Source** window.



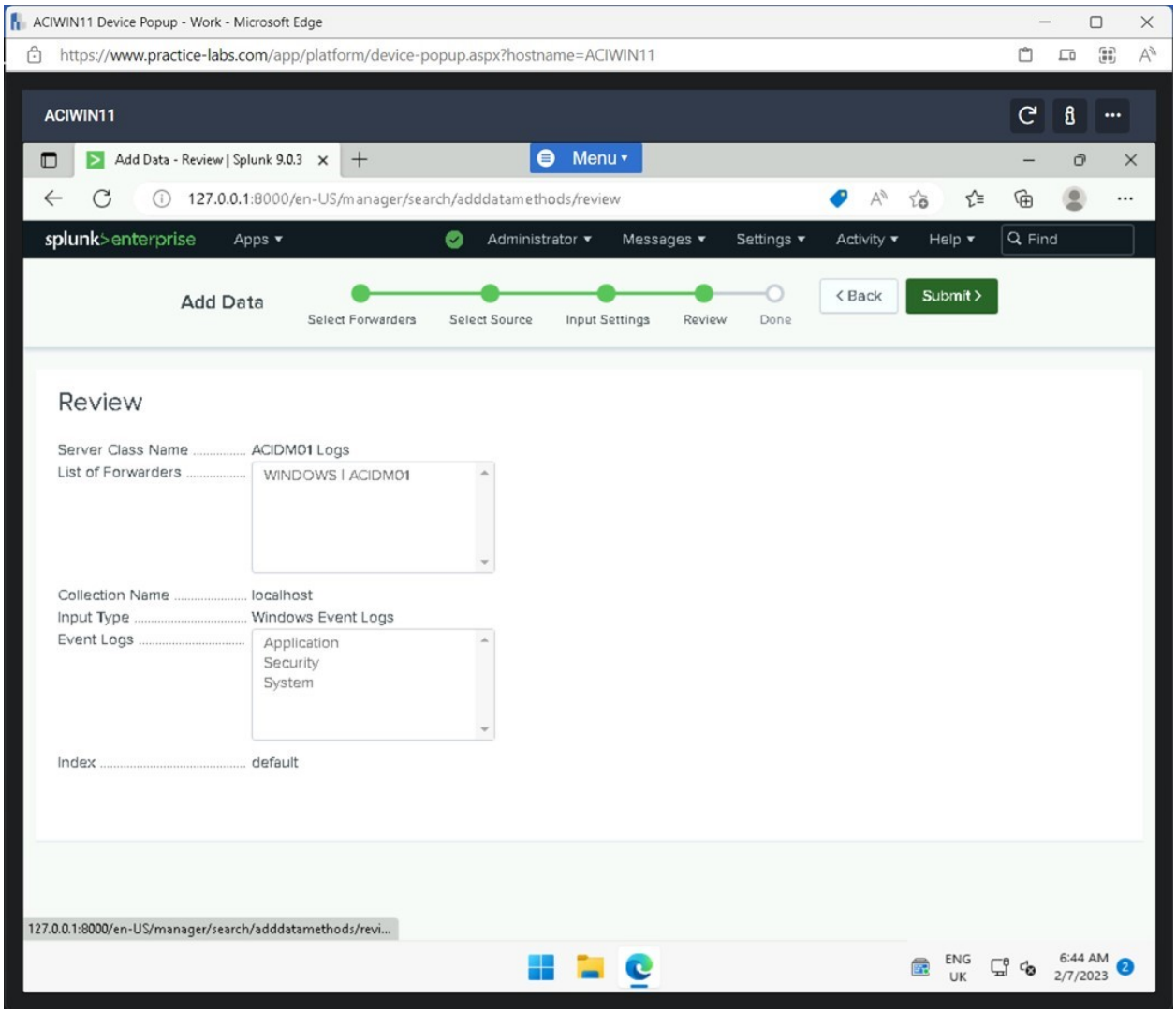
- In **Select Event Logs** pane, I clicked the following options:
- **Application**
- **Security**
- **System**
- Clicked **Next**.



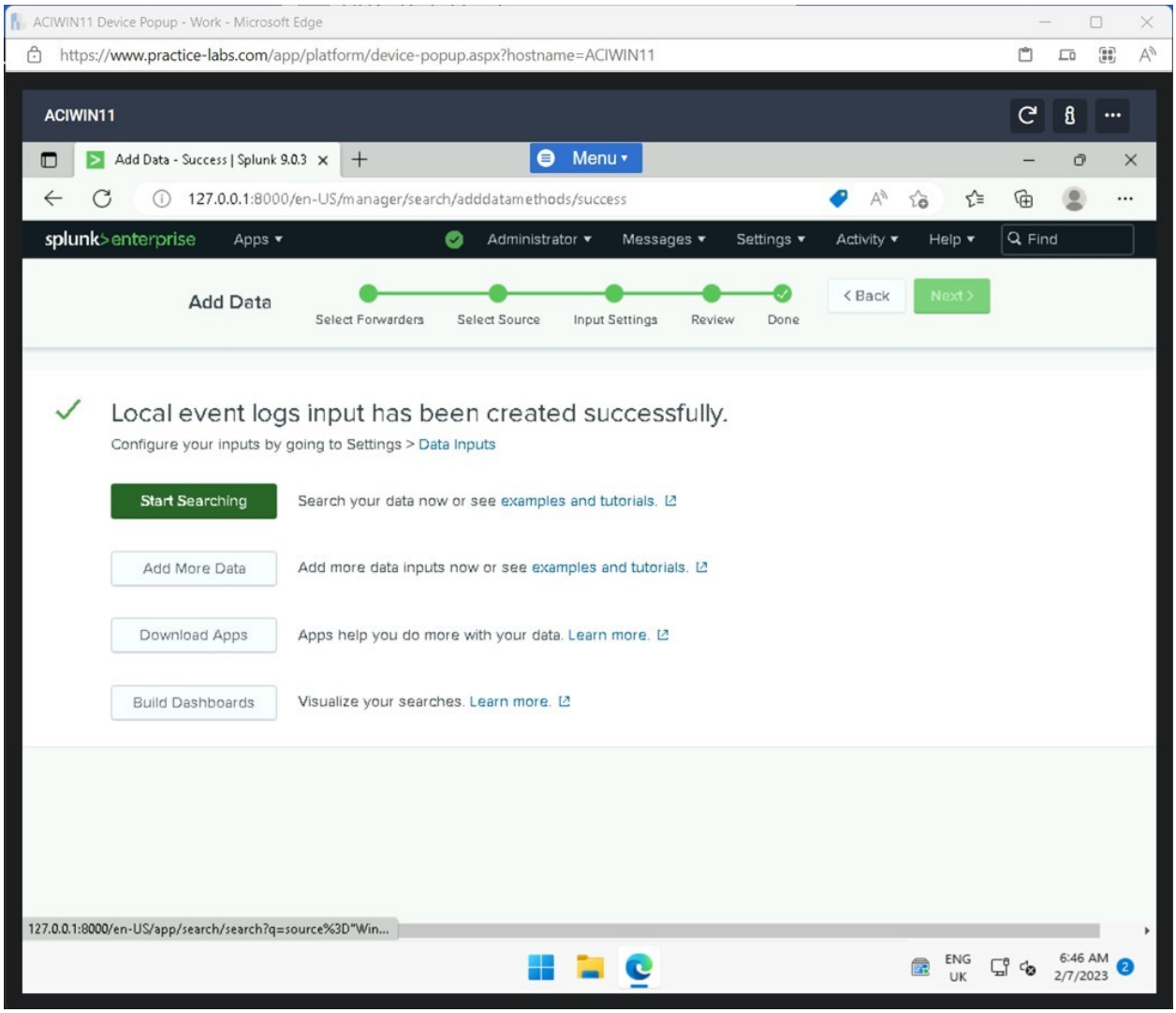
- Clicked the log events and moved them to the **Selected Items Window.**
- Clicked **Review** on the **Input Settings** window.



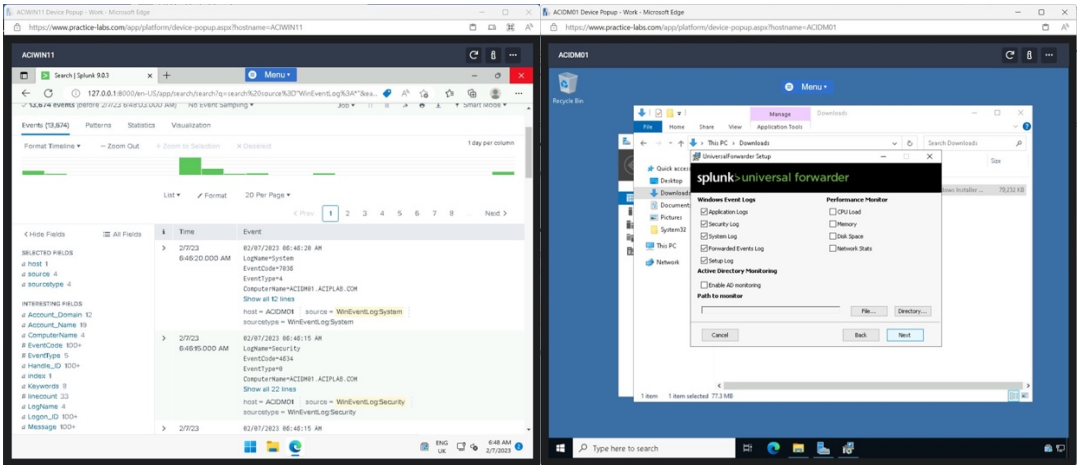
- Clicked **Submit** on the **Review** window.



- Clicked **Start Searching** on the **Local event logs input has been created successfully** window.

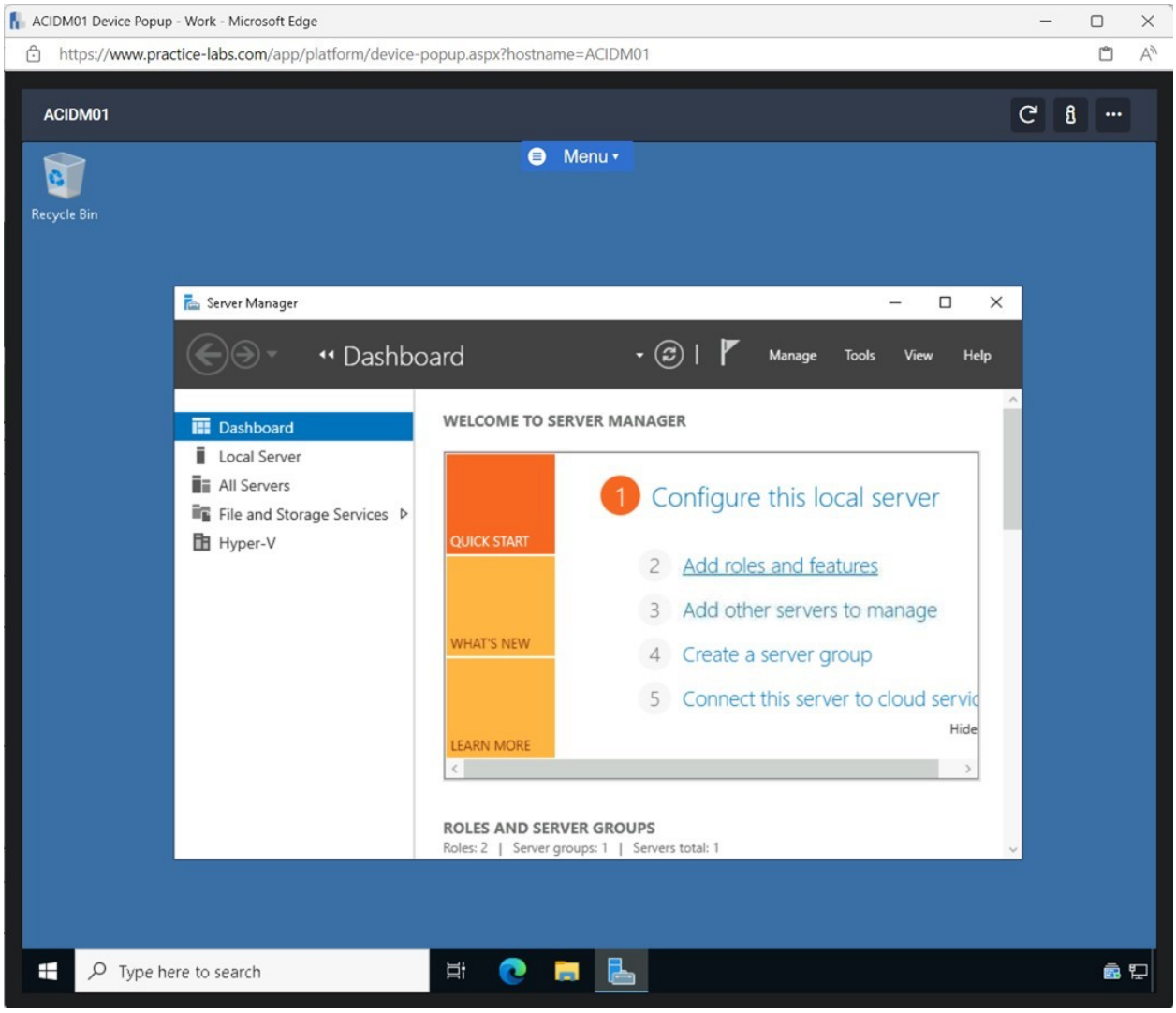


- Closed the **Microsoft Edge** browser window once you have viewed the event logs.

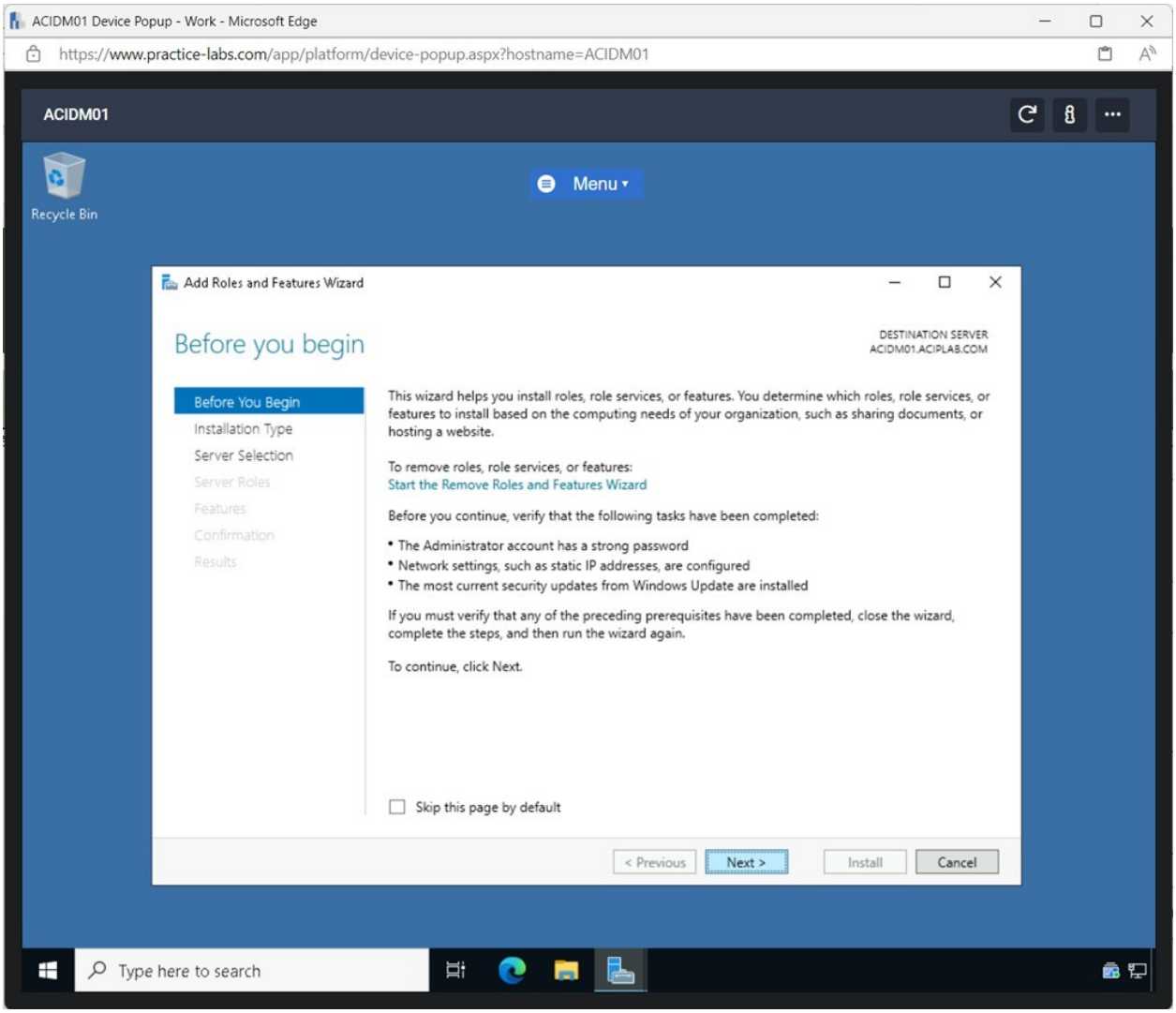


Exercise 2 - Encrypting Sensitive Data

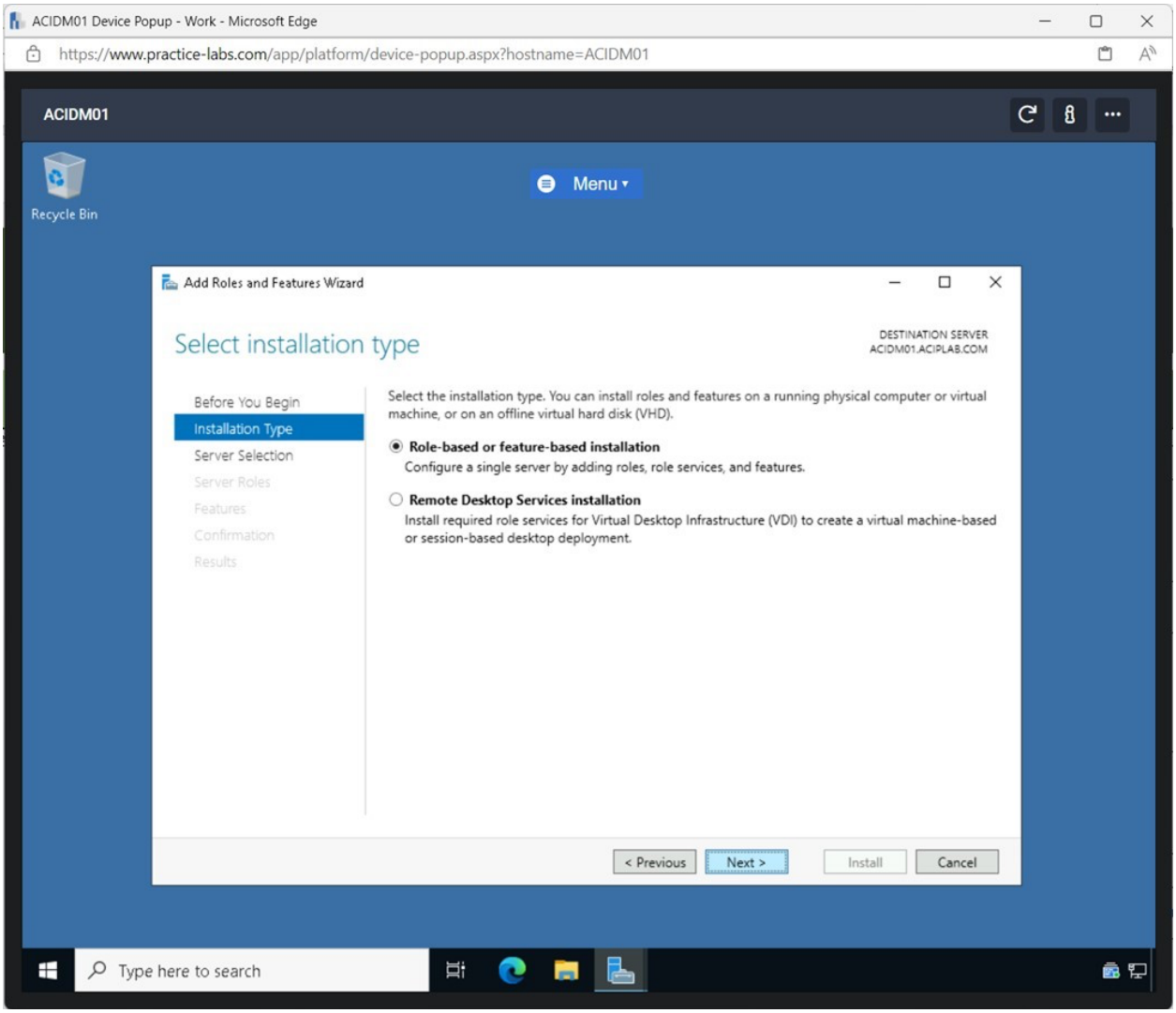
- As a Cyber Security Specialist, it is critical to protect sensitive data that is stored locally or in the cloud. Different types of sensitive data can be stored on the server, for example, Personally identifiable information (PII) or Cardholder Data (CHD)
- To protect locally stored data, the server's hard drives can be encrypted to protect the data on the drive.
- I installed the BitLocker Drive encryption feature and encrypted a local drive.
- **Task 1 - Install the BitLocker Drive Encryption Feature**
- **To be able to encrypt a local disk on a Windows Server, the BitLocker feature needs to be installed.**
- **Connected to the VM in Server Manager and clicked Add roles and features.**



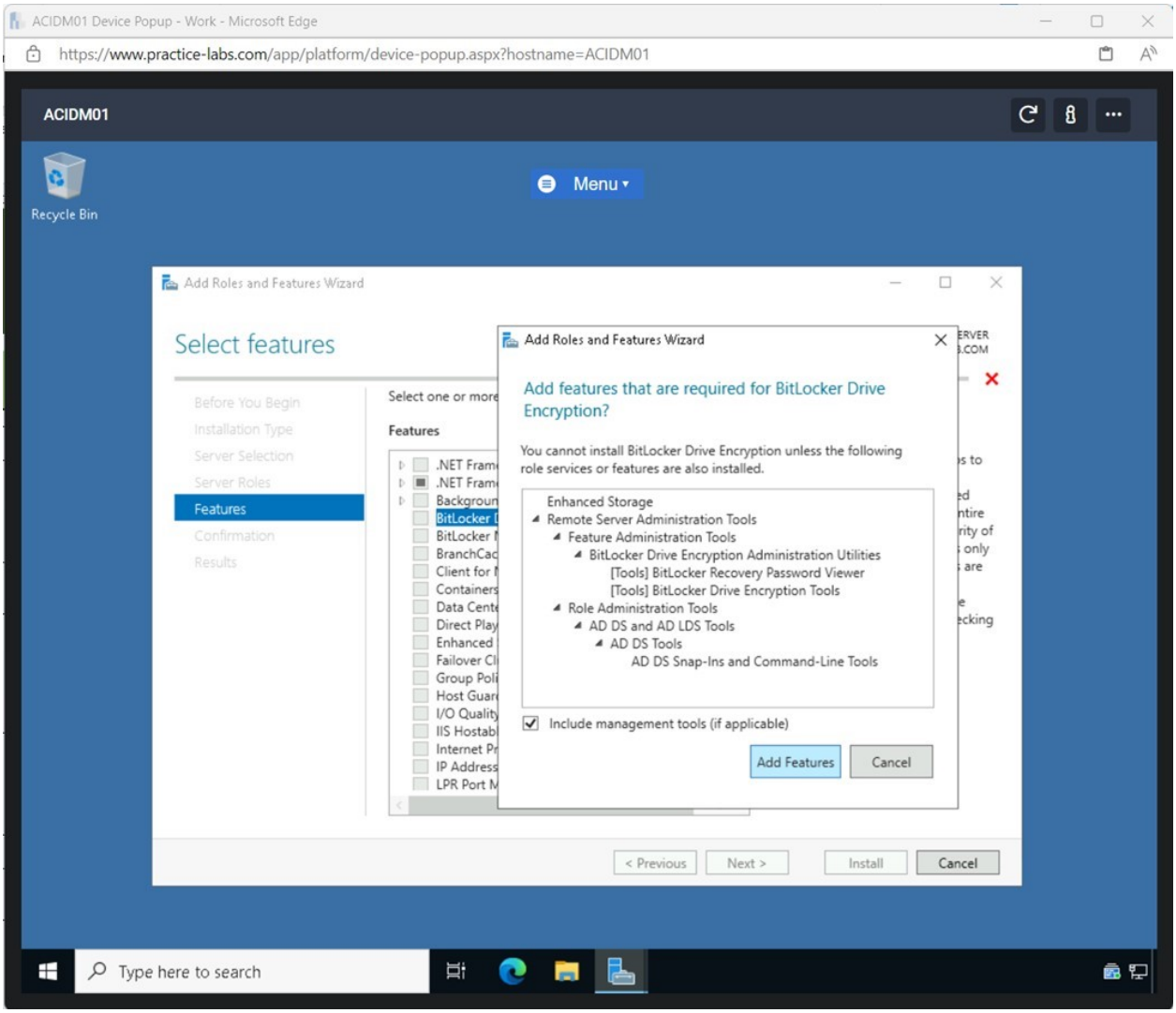
- **In the Add Roles and Features Wizard window, I clicked Next.**



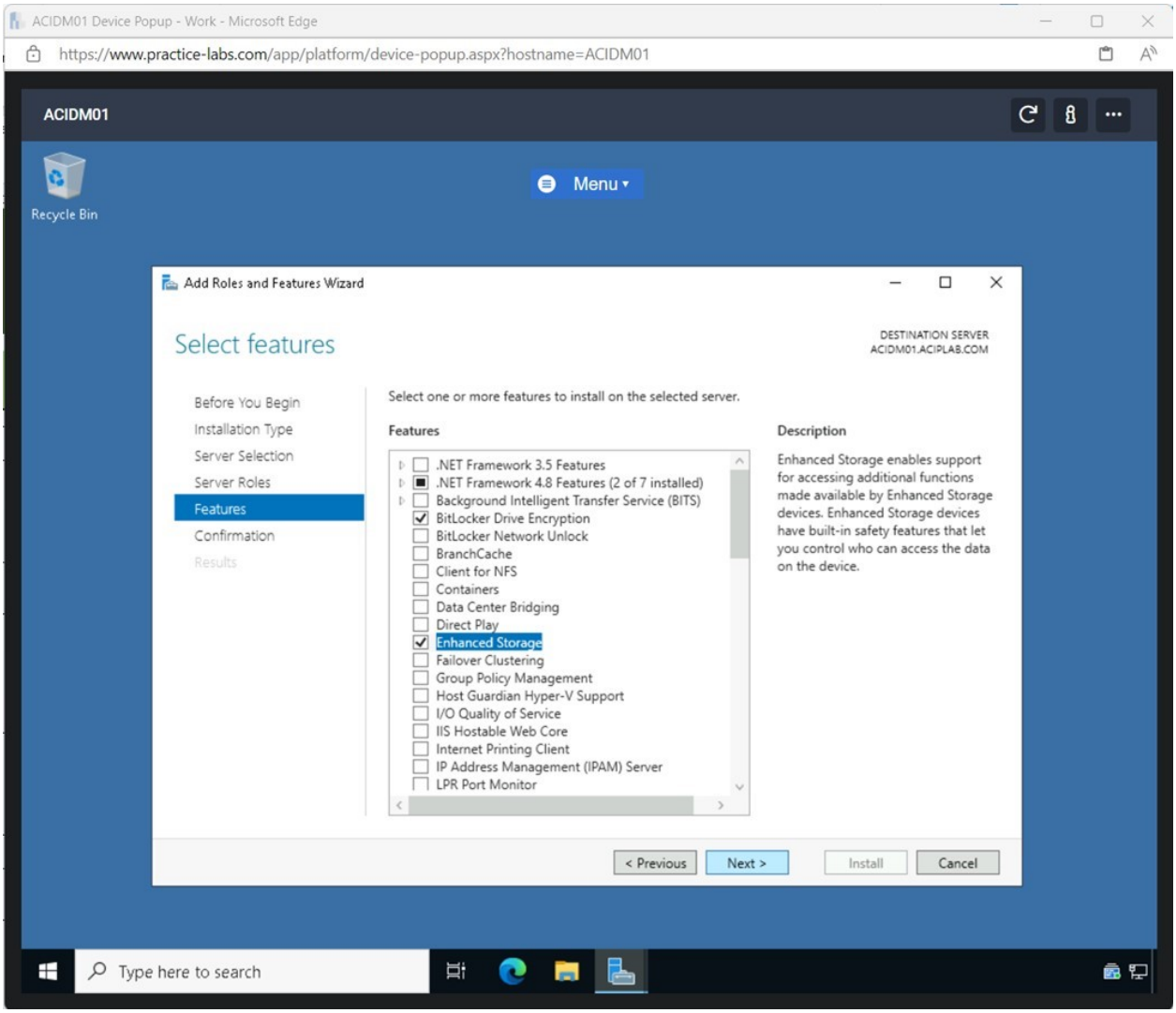
- **On the Select Installation type pane, I clicked Next until reaching the Select Features pane.**



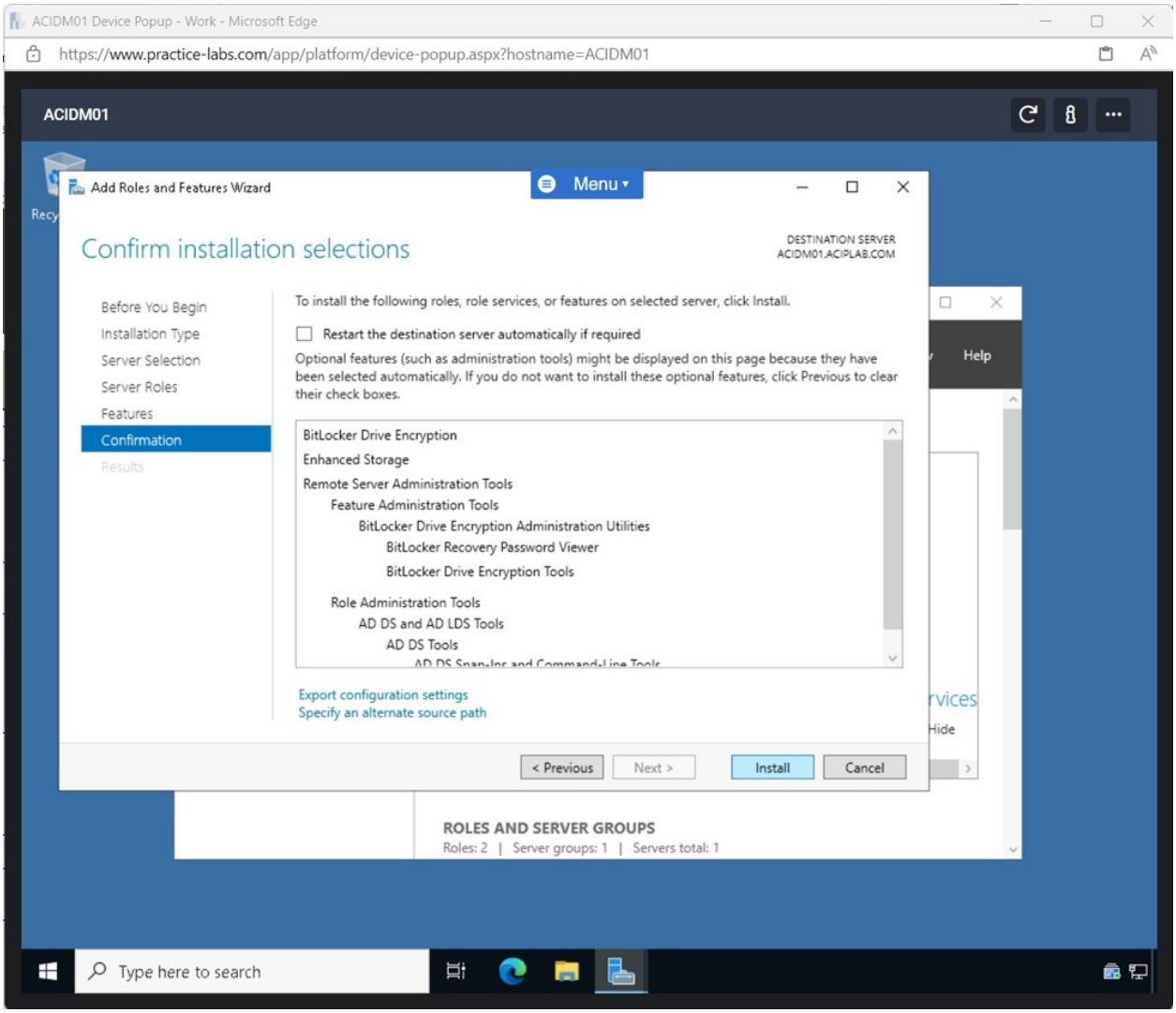
- **On the Select Features pane, I enabled the BitLocker Drive Encryption checkbox and clicked Add Features in the pop-up window.**



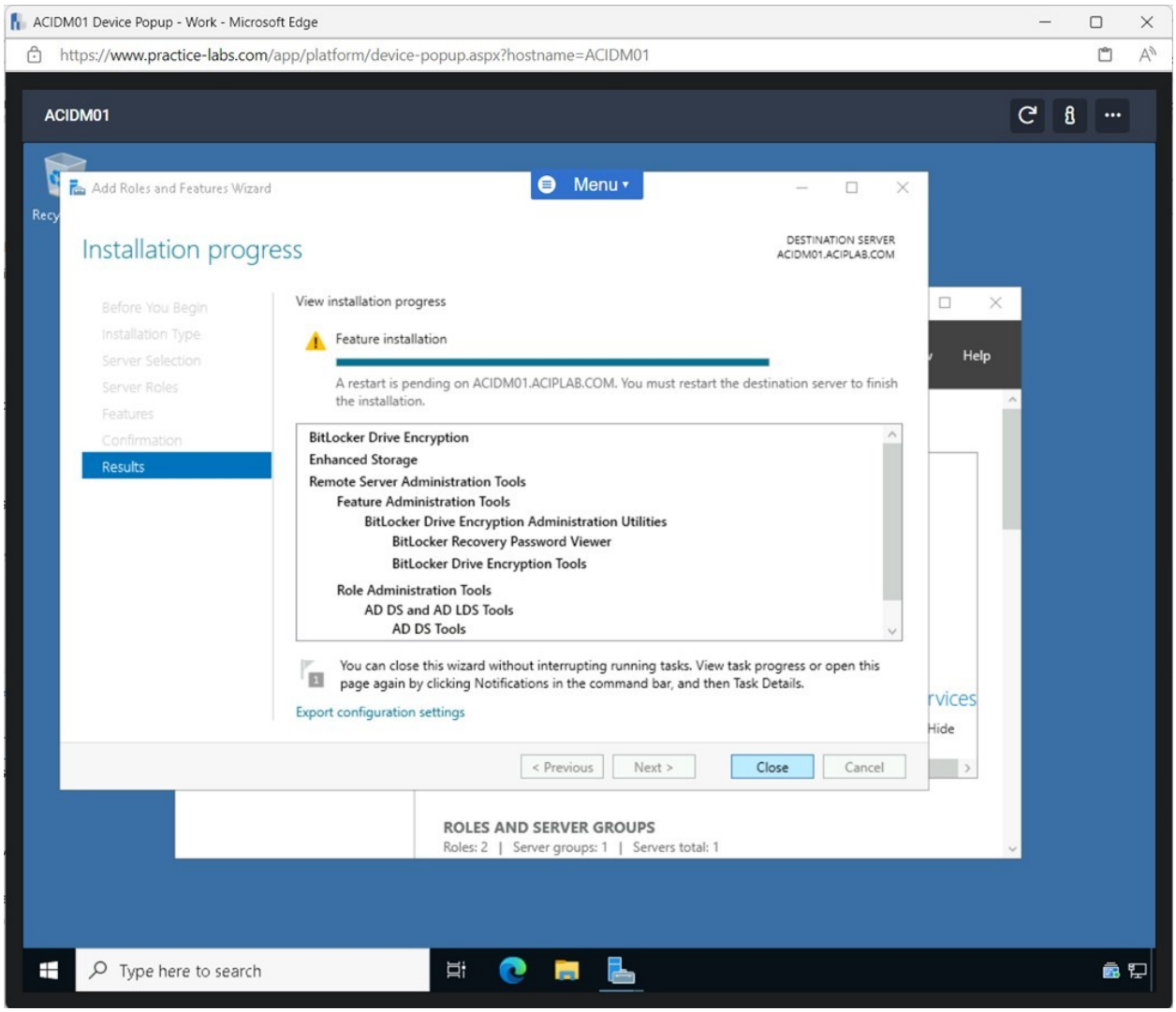
- **Clicked Next on the Select Features pane.**



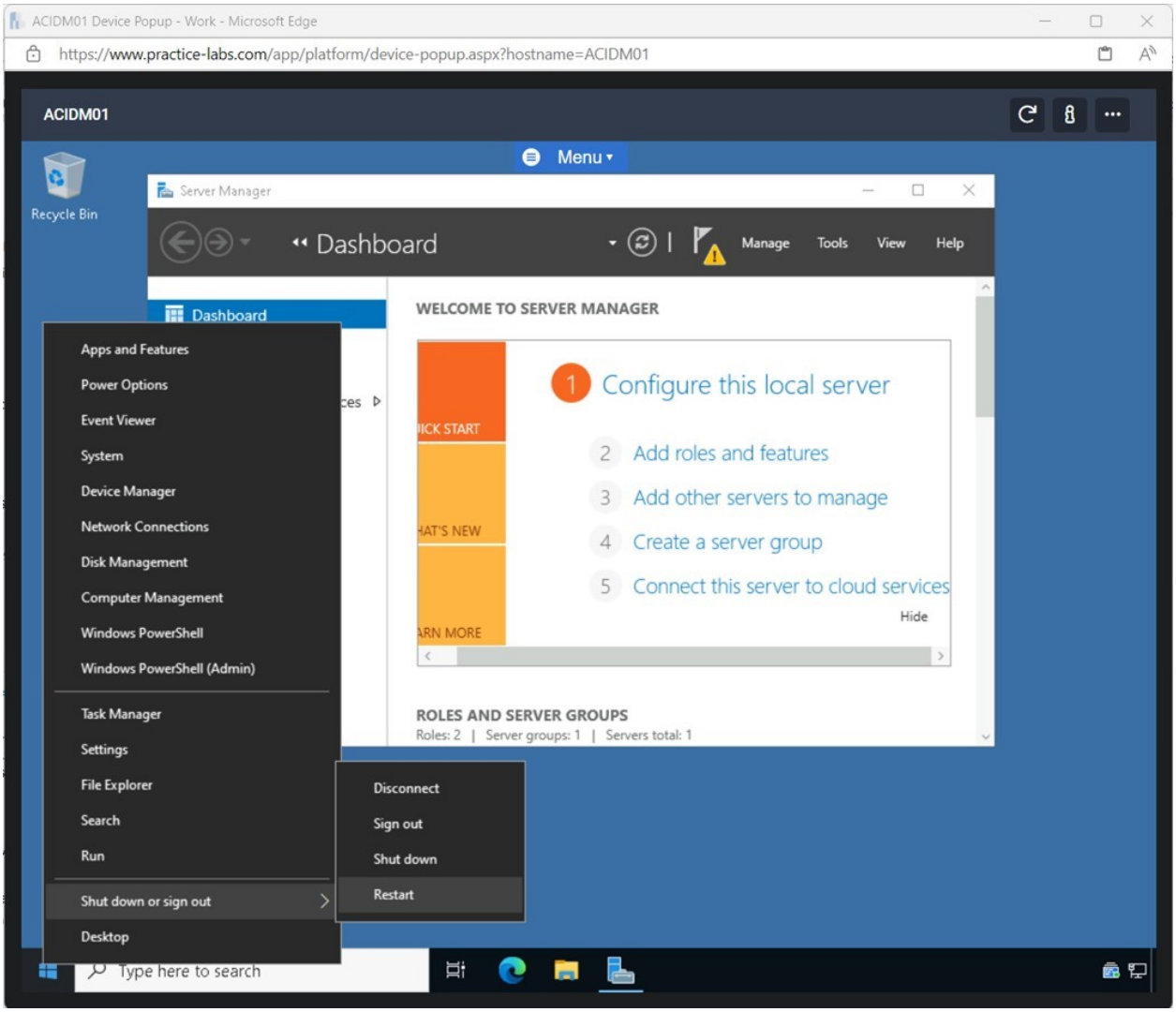
- **On the Confirm installation selections pane, I clicked Install.**



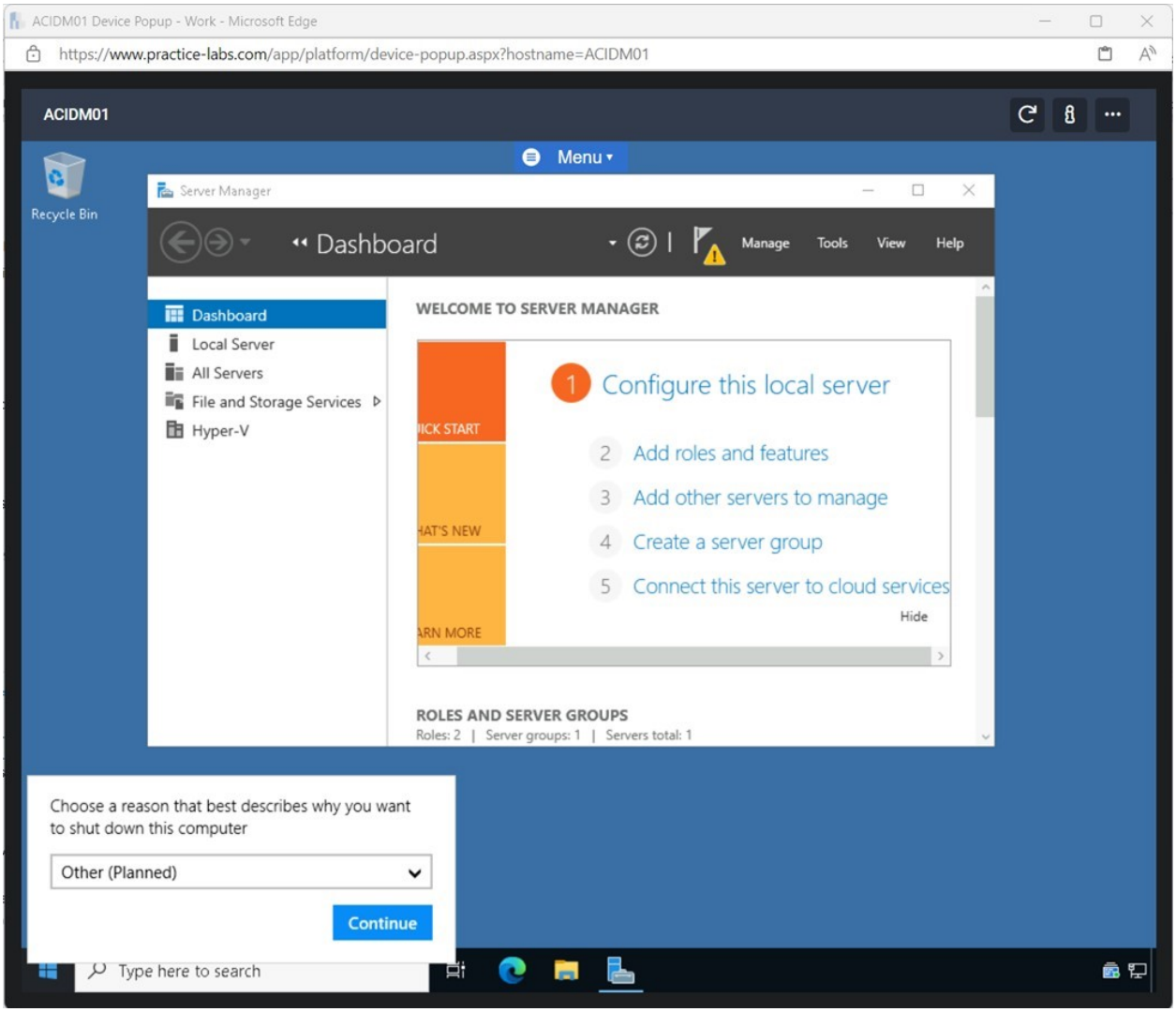
- BitLocker download took a few minutes.
- **Clicked Close after the installation has been completed.**

- 

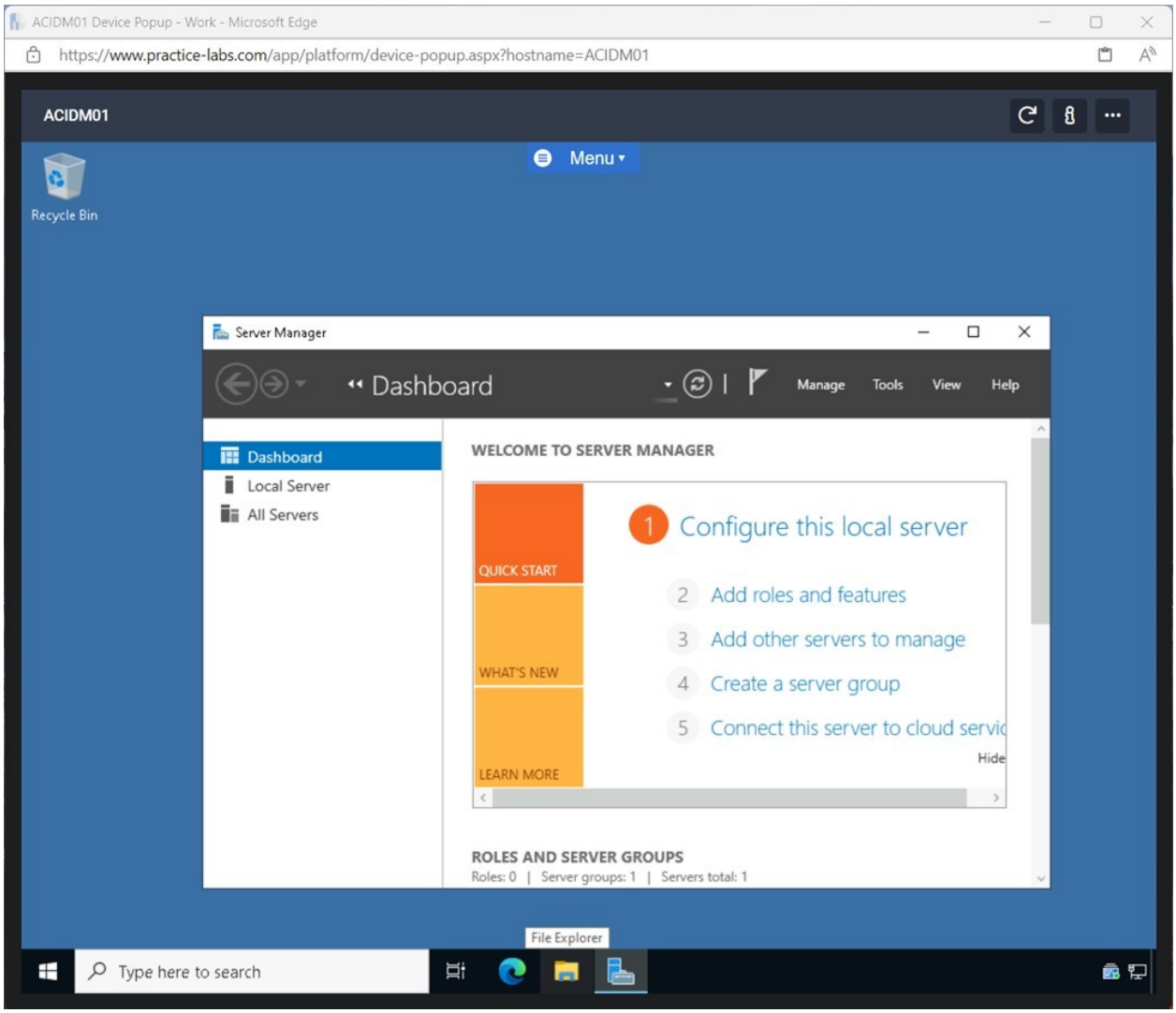
- **Restarted pc and logged back in.**
- **Right-clicked Start, selected Shut down and clicked Restart.**



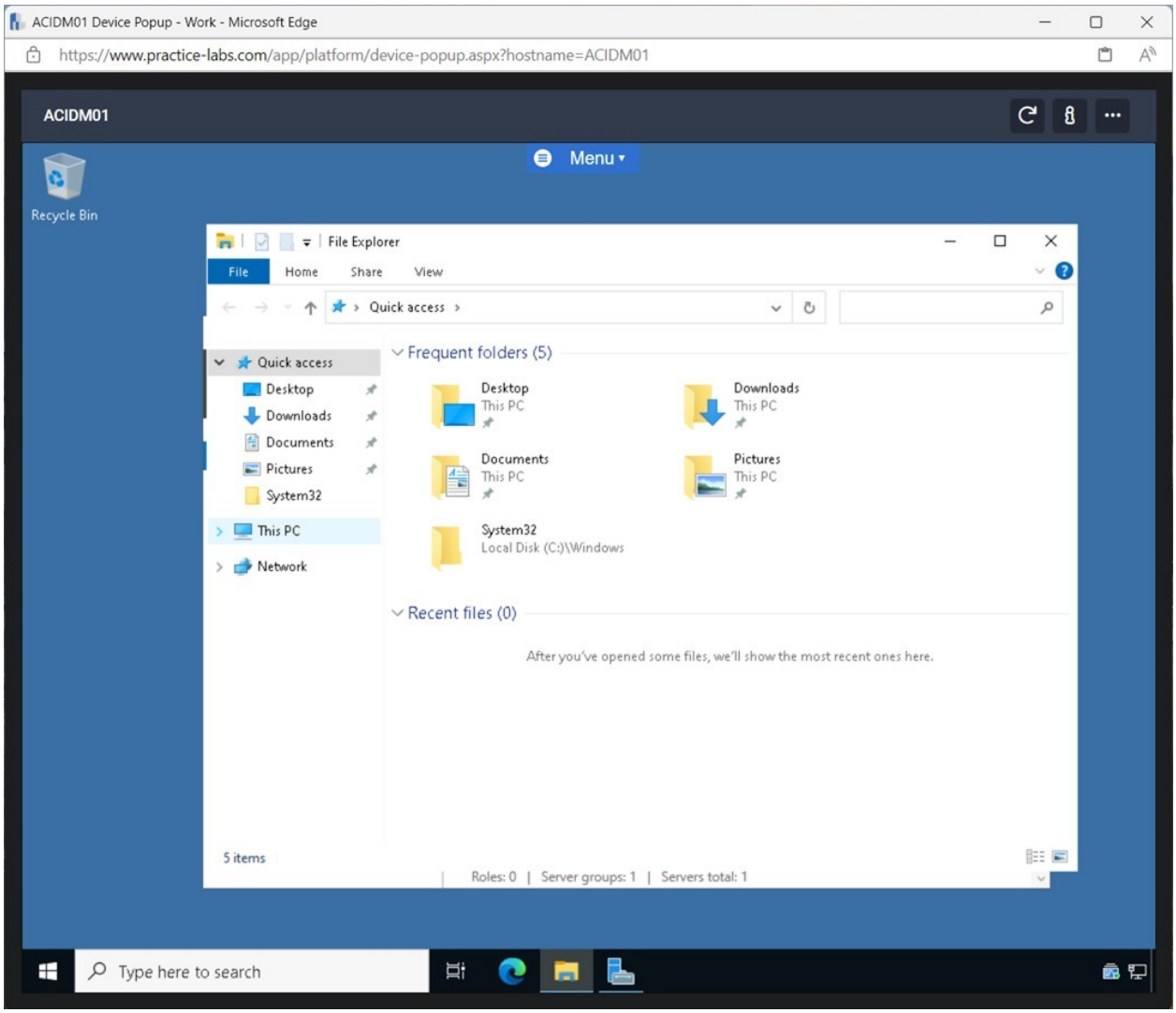
- **On the Choose a reason that best describes why you want to shut down this computer pop-up window in the drop-down menu, I selected the Other (Planned) and clicked Continue.**



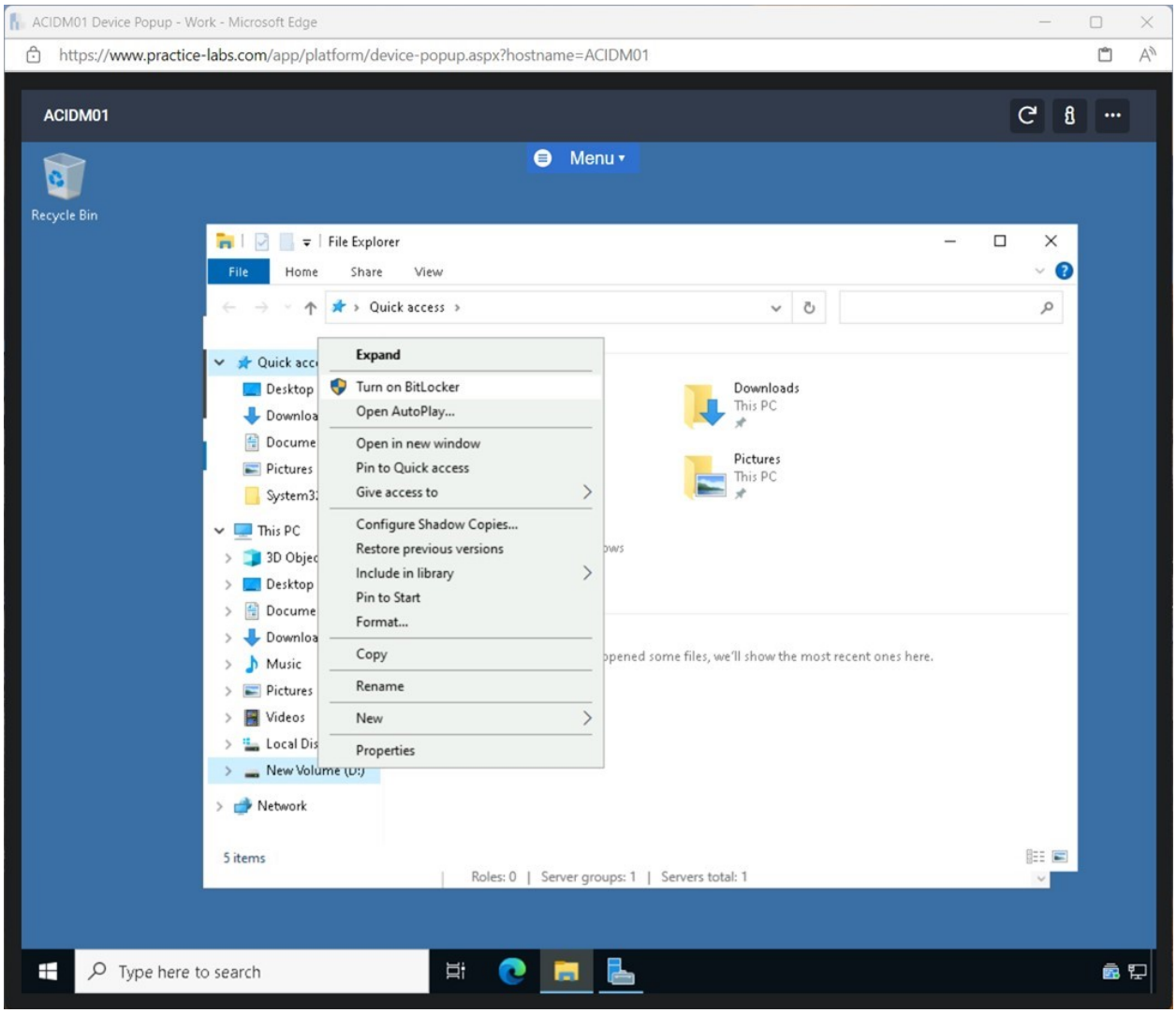
- **Task 2 - Encrypting a Local Drive on a Server**
- **After installing the BitLocker Drive Encryption feature, it can encrypt and secure a local drive.**
- **In this task, a local drive will be encrypted.**
- **Reconnected to pc and opened File Explorer from the Taskbar.**



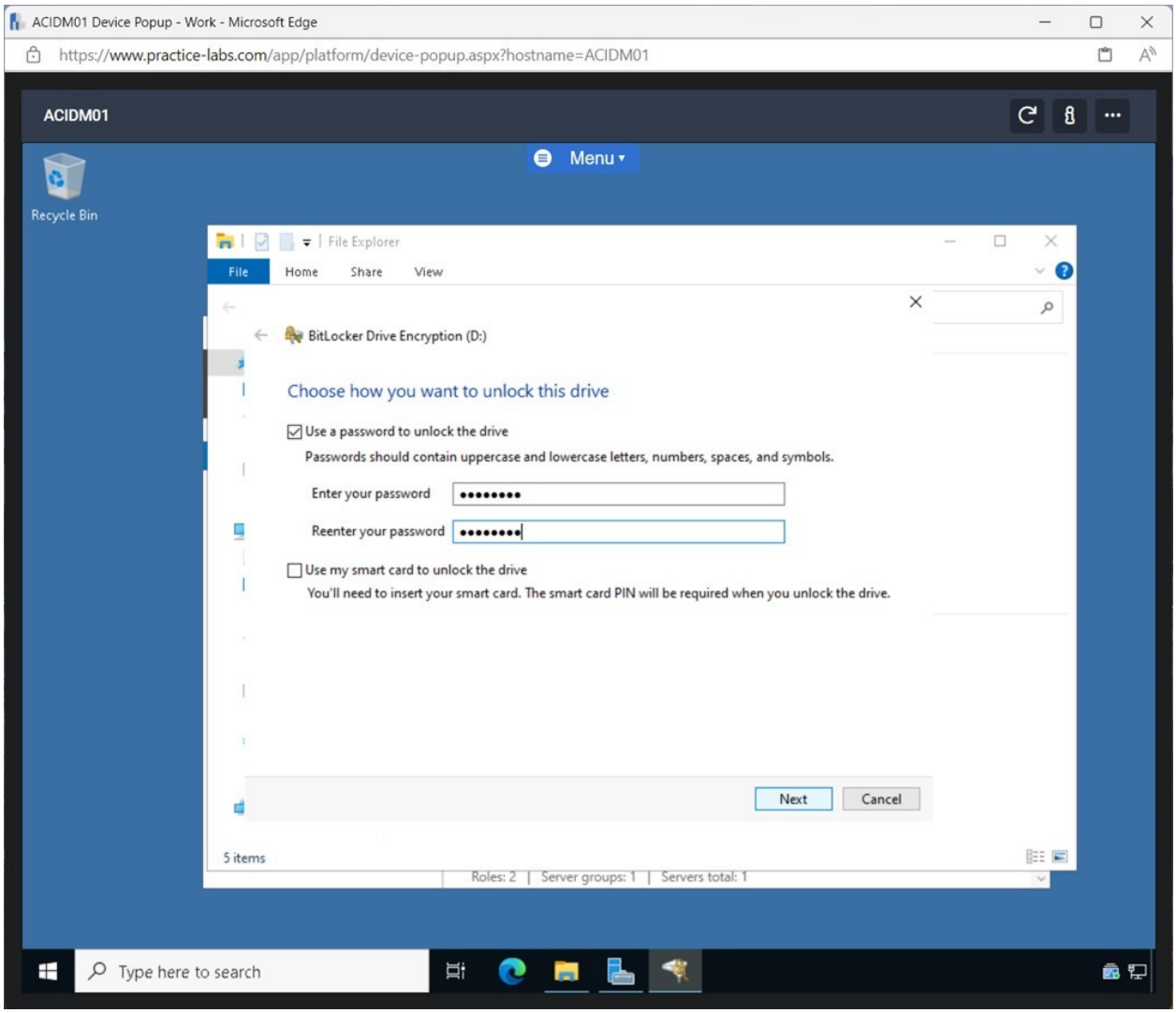
- **In File Explorer, expanded This PC**



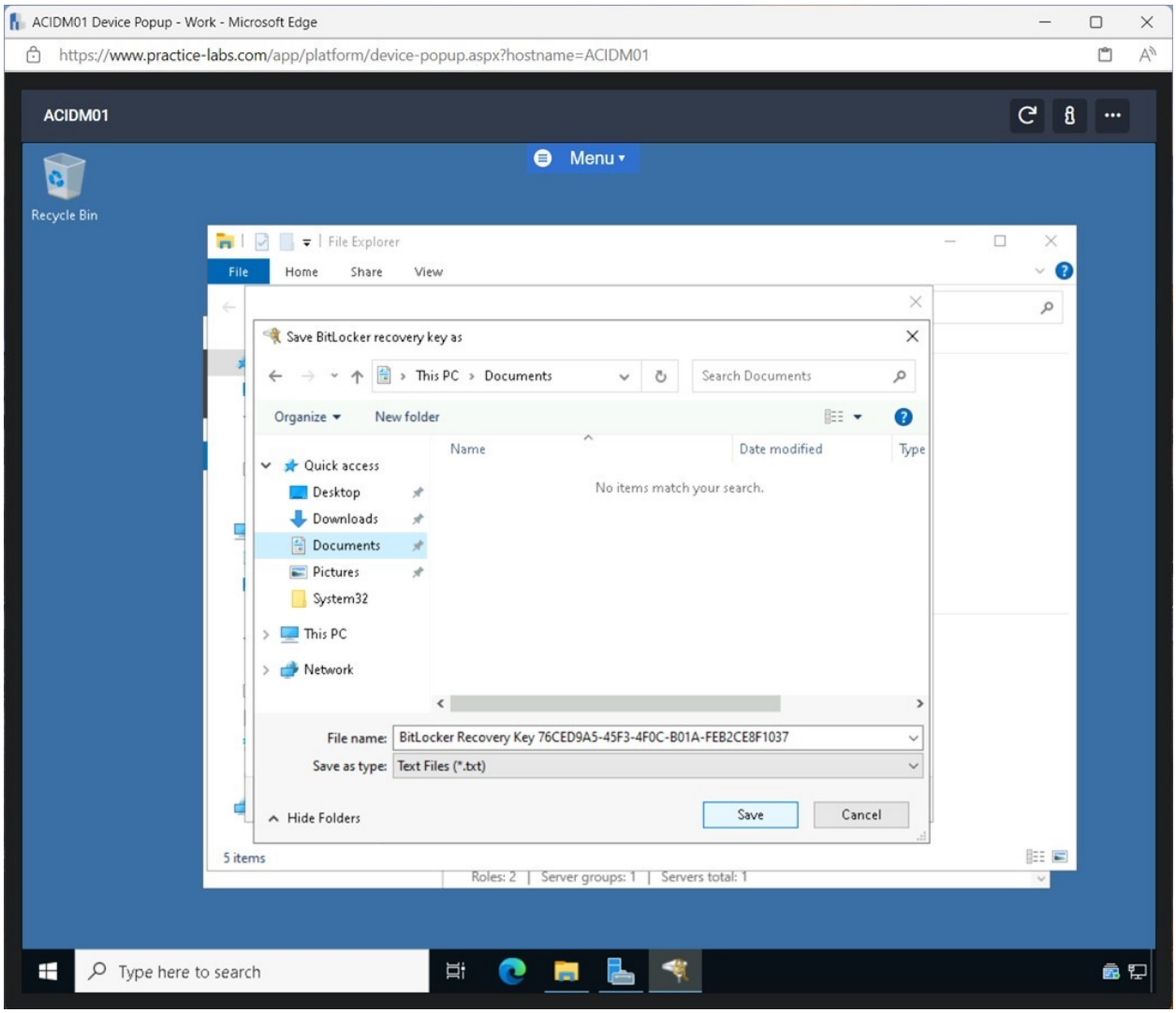
- **In the This PC pane, right-clicked New Volume (D:) and selected Turn on BitLocker.**



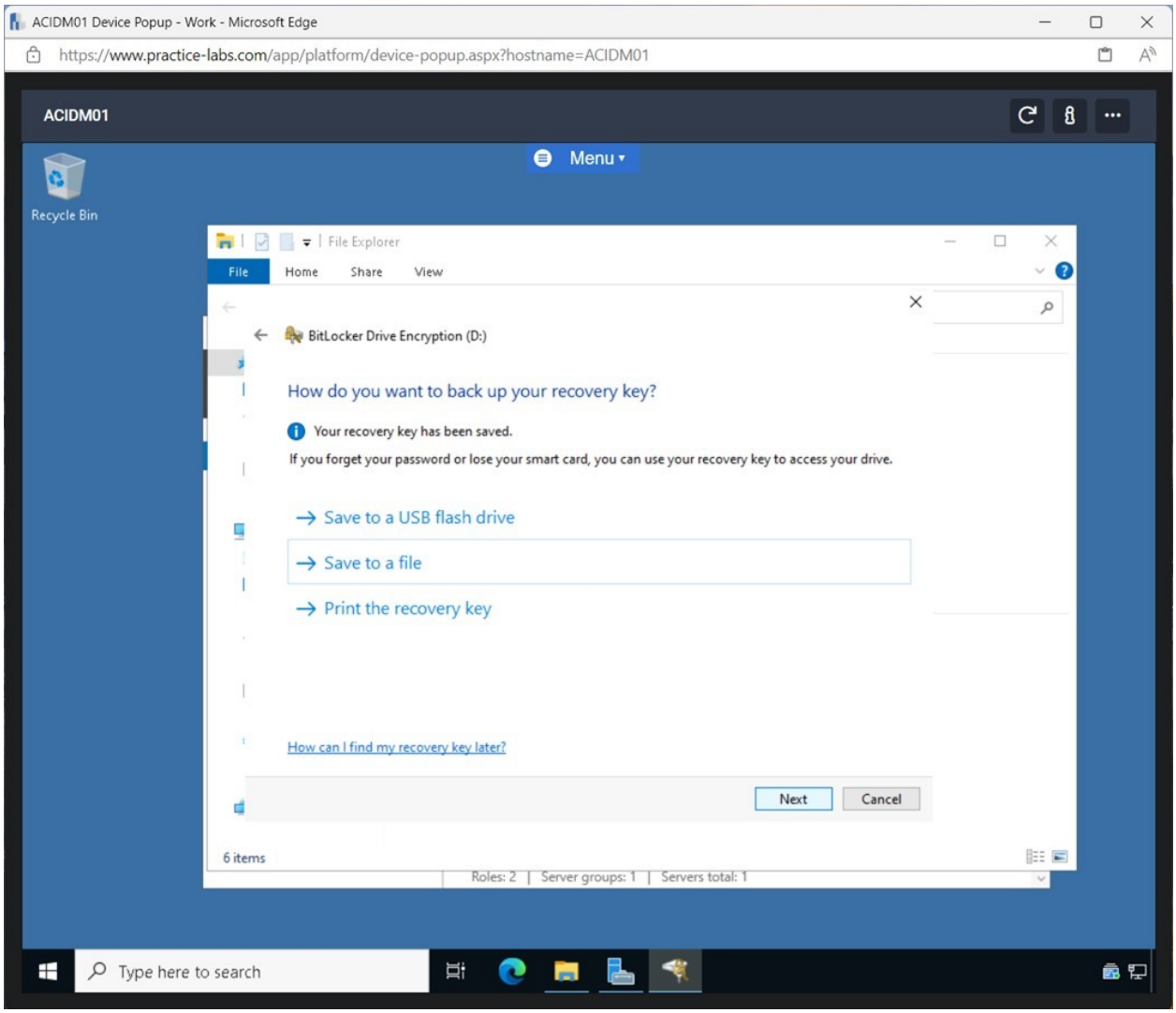
- **On the BitLocker Drive Encryption window, chose the Use a password to unlock this drive tick box and enter the following:**
- **Enter your password: Passw0rd**
- **Reenter your password: Passw0rd**
- **Clicked Next.**



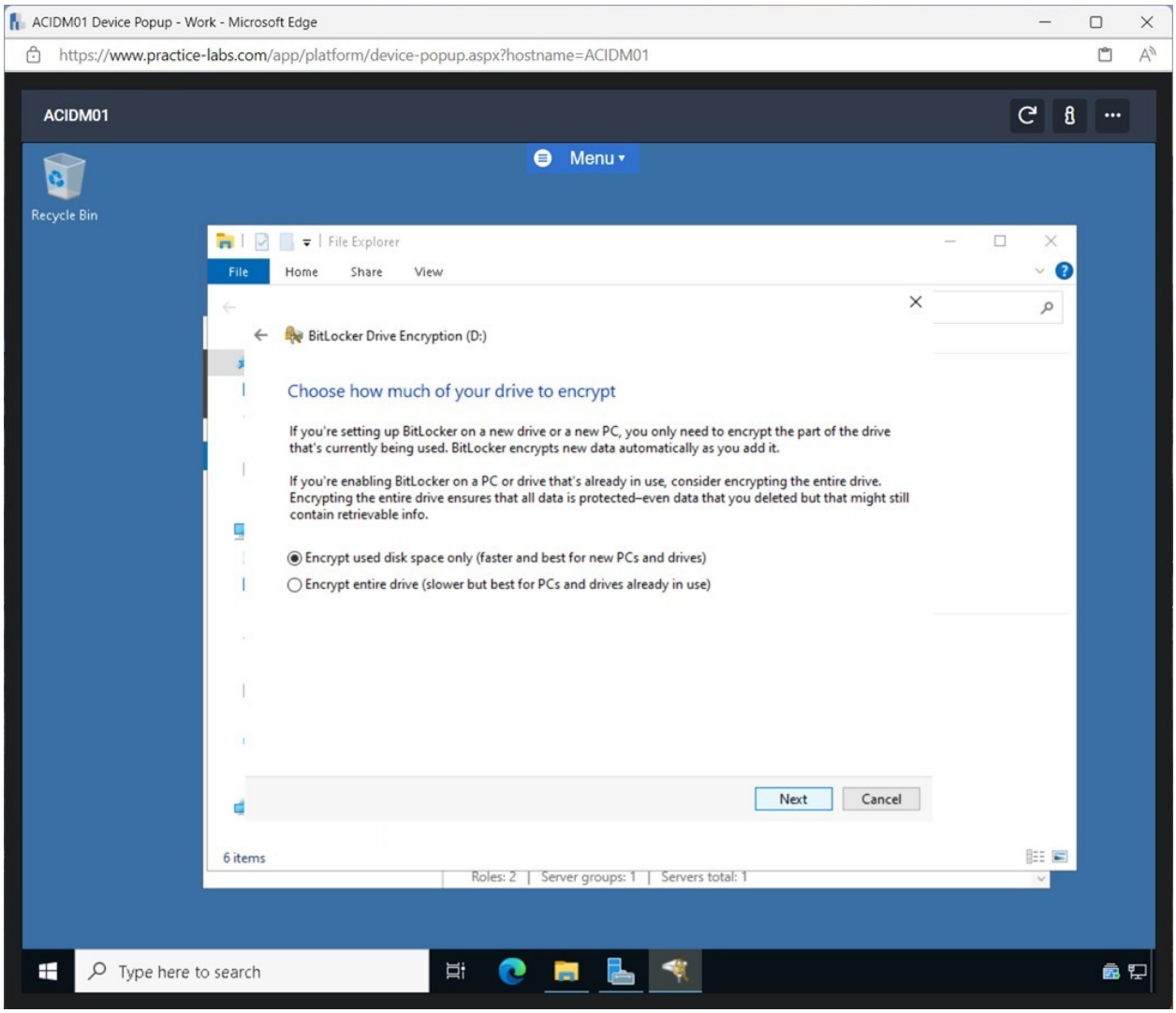
- **On the How do you want to back up your recovery key? window, I selected Save to a file.**
- **In the Save BitLocker recovery key as pop-up window, I selected Documents and clicked Save.**



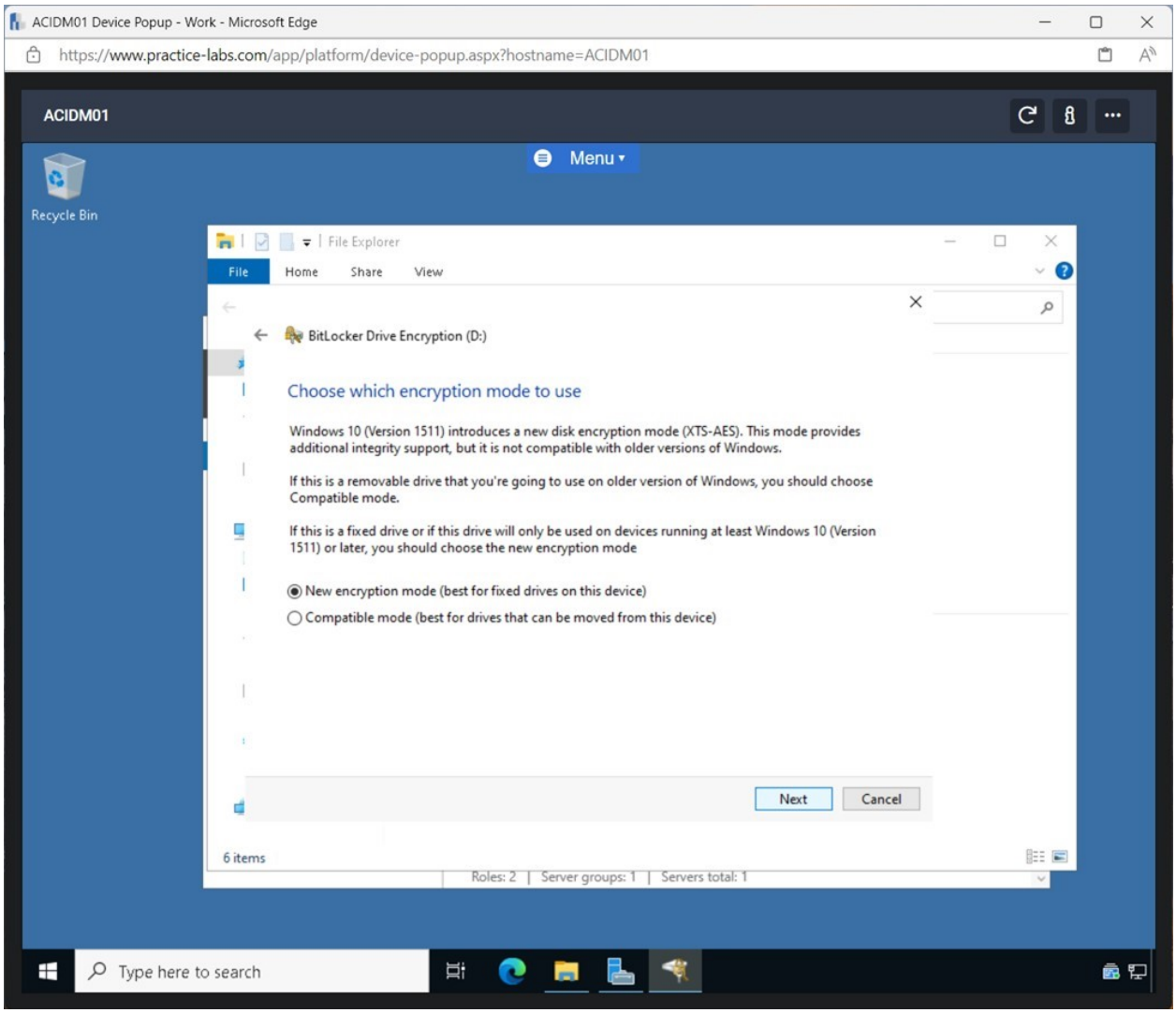
- **Clicked Next on the How do you want to back up your recovery key? pane.**



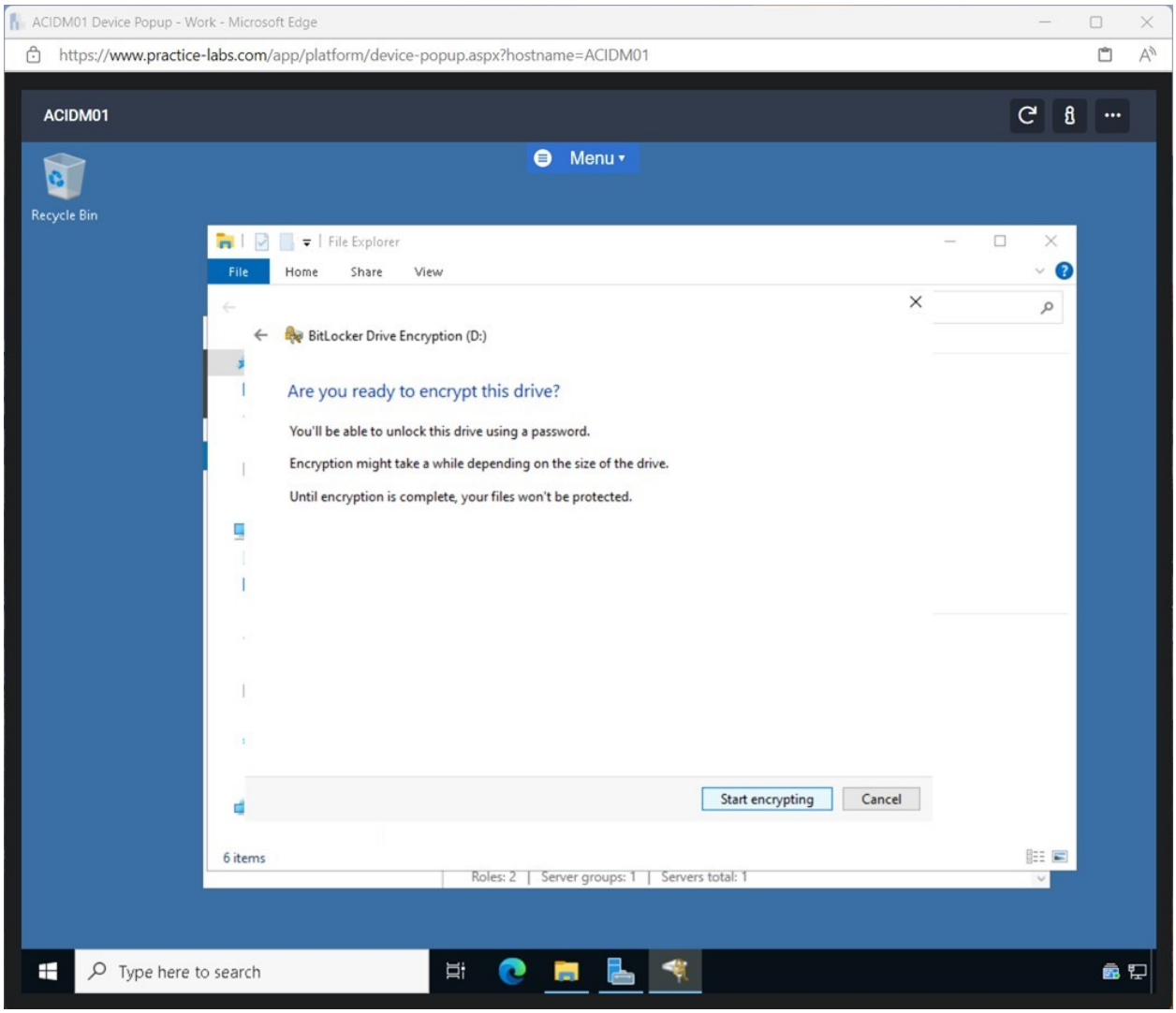
-
- **I Clicked Next on the Choose how much of your drive to encrypt pane.**



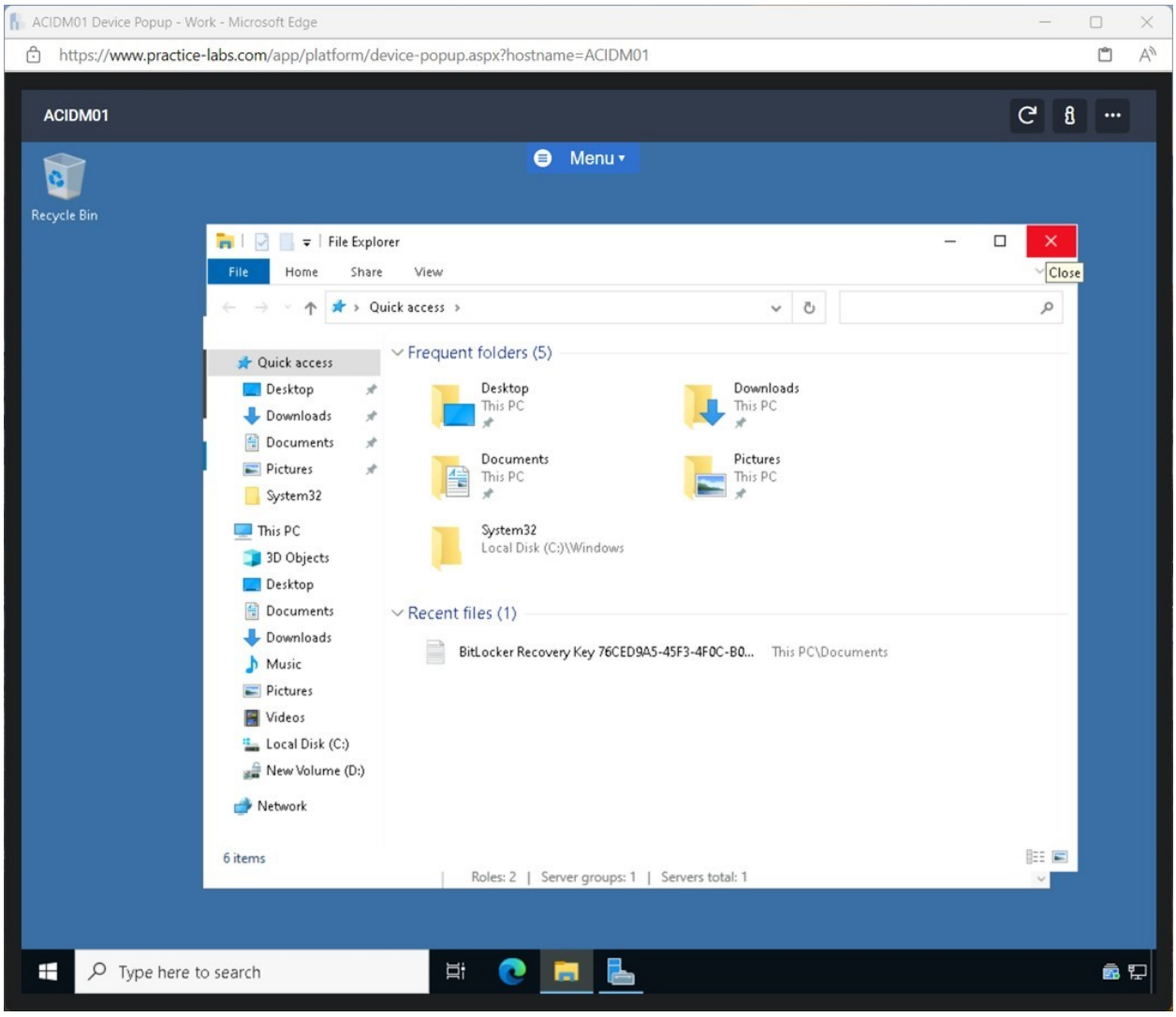
- **Clicked Next on the Choose which encryption mode to use pane.**



-
- **On the Are you ready to encrypt this drive? Pane I clicked Start encrypting.**



- **Closed File Explorer.**



- **Figure 2.19 Screenshot of ACIDM01: Displaying closing File Explorer.**

Exercise 3 - Enable Multifactor Authentication

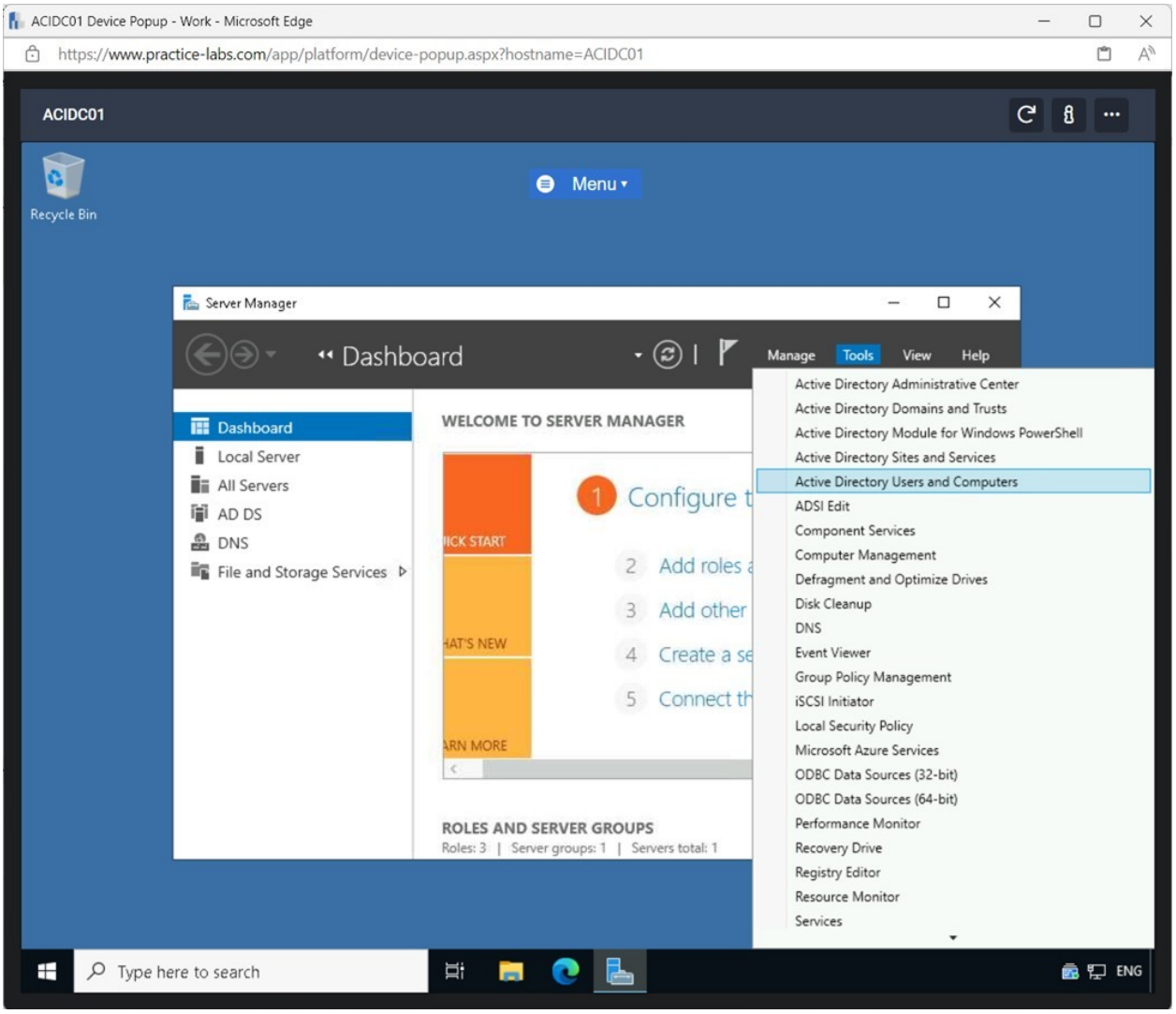
Multifactor Authentication can be enabled to add an additional layer of security to protect user accounts. Several different methods can be used to implement multifactor authentication. These include smart cards, using an authentication application, or a secure USB key.

A user account was created, and multifactor authentication will be enabled.

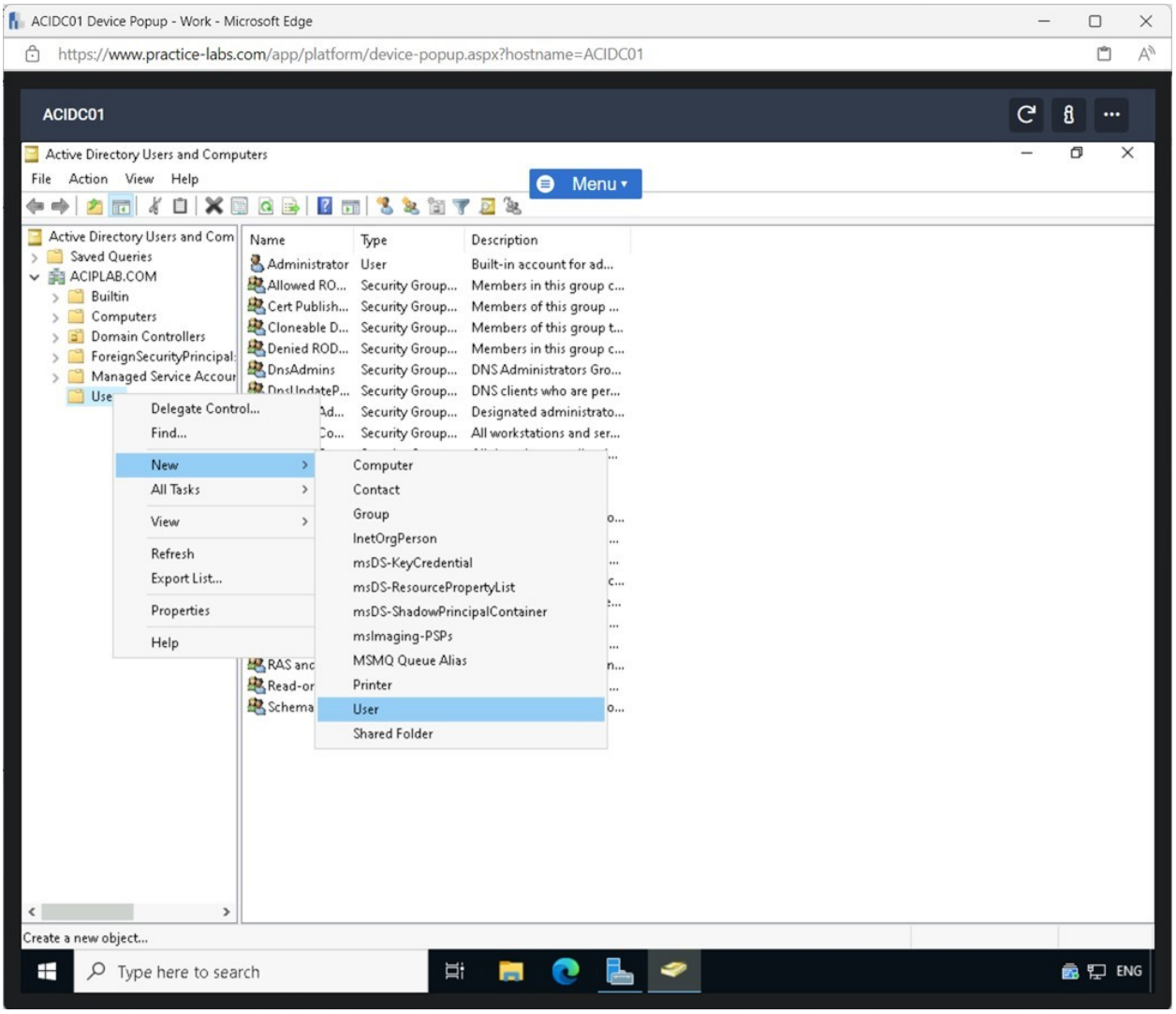
- **Enable Multifactor Authentication**
- **Verify Multifactor Authentication**

Task 1 - Enable Multifactor Authentication

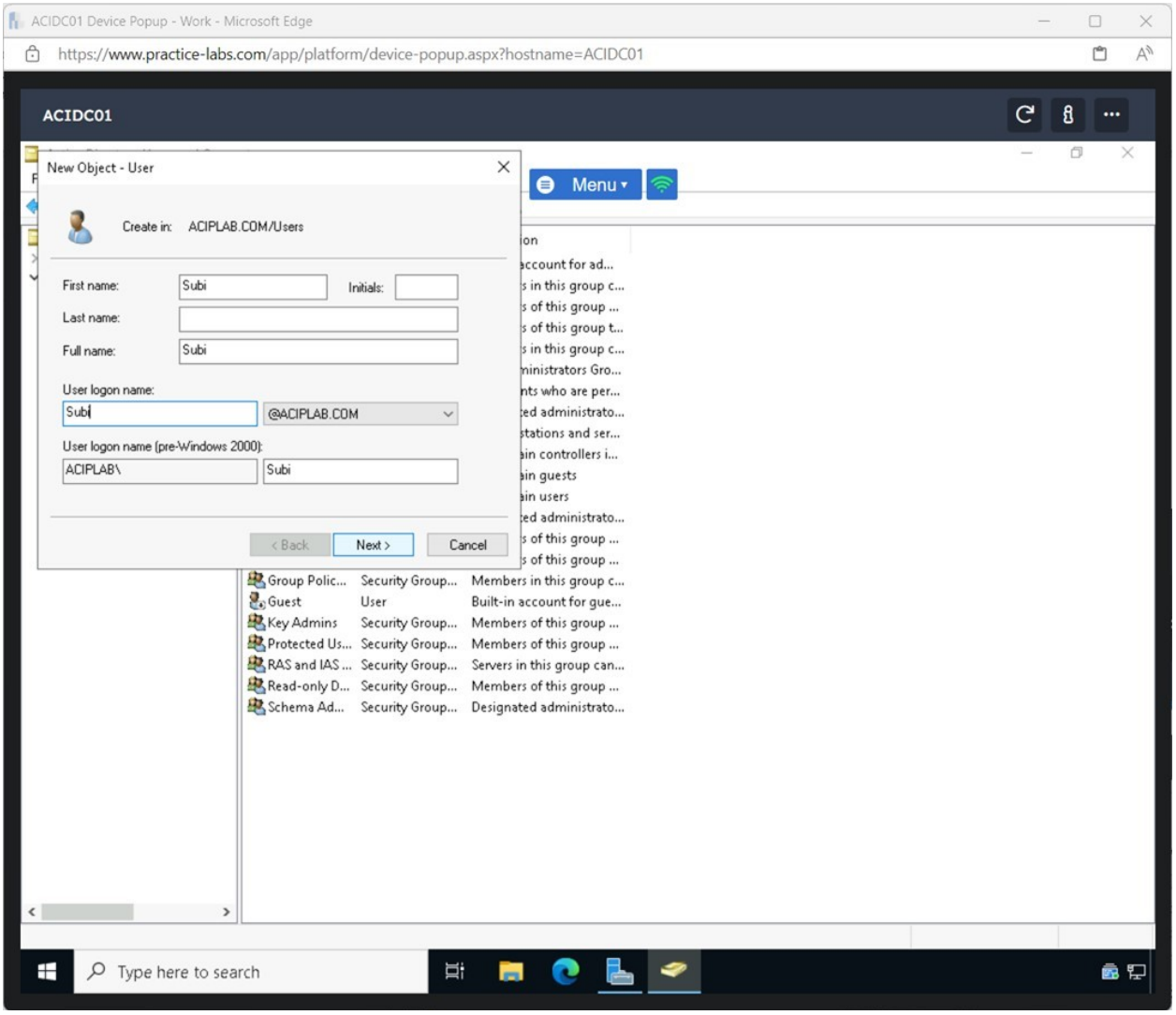
Connected to ACIDC01in Server Manager, clicked Tools, and selected Active Directory Users and Computers.



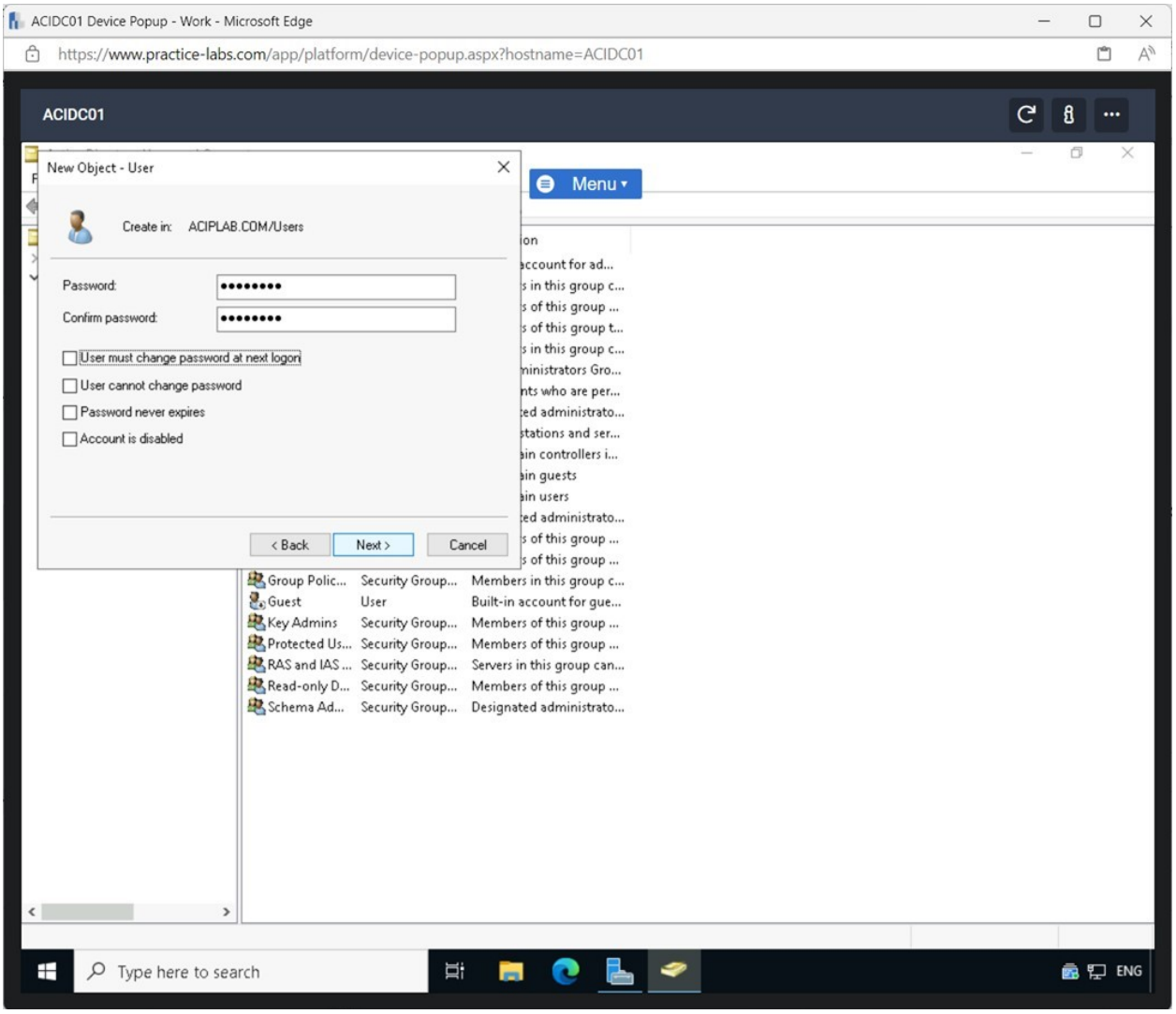
In the Active Directory Users and Computers pane on the left I expanded a VM named ACIPLAB.COM. Next, I right-clicked Users, selected new, and clicked User.



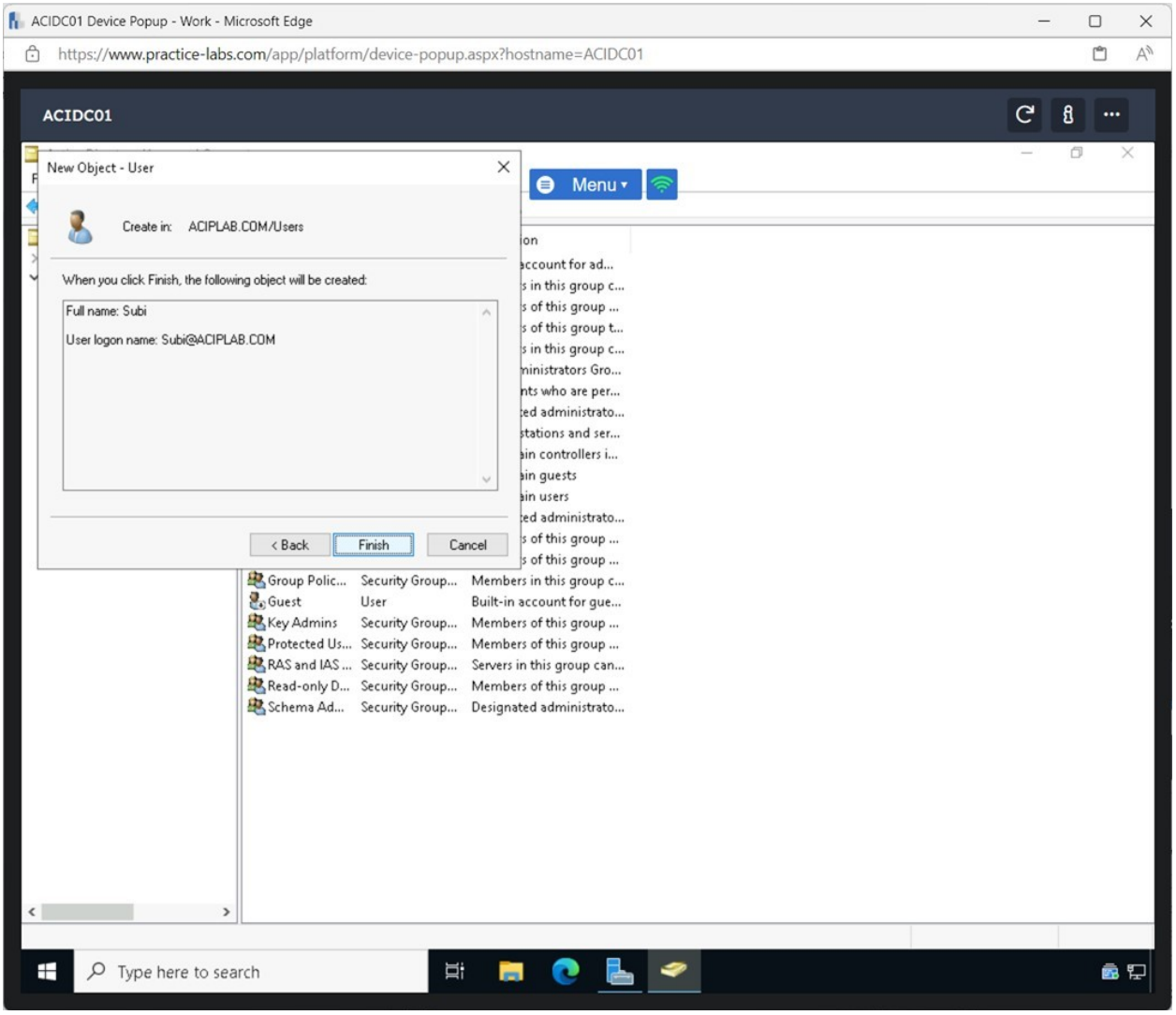
On the New Object - User complete the following:
First name: Subi
User logon name: Subi
Clicked Next.



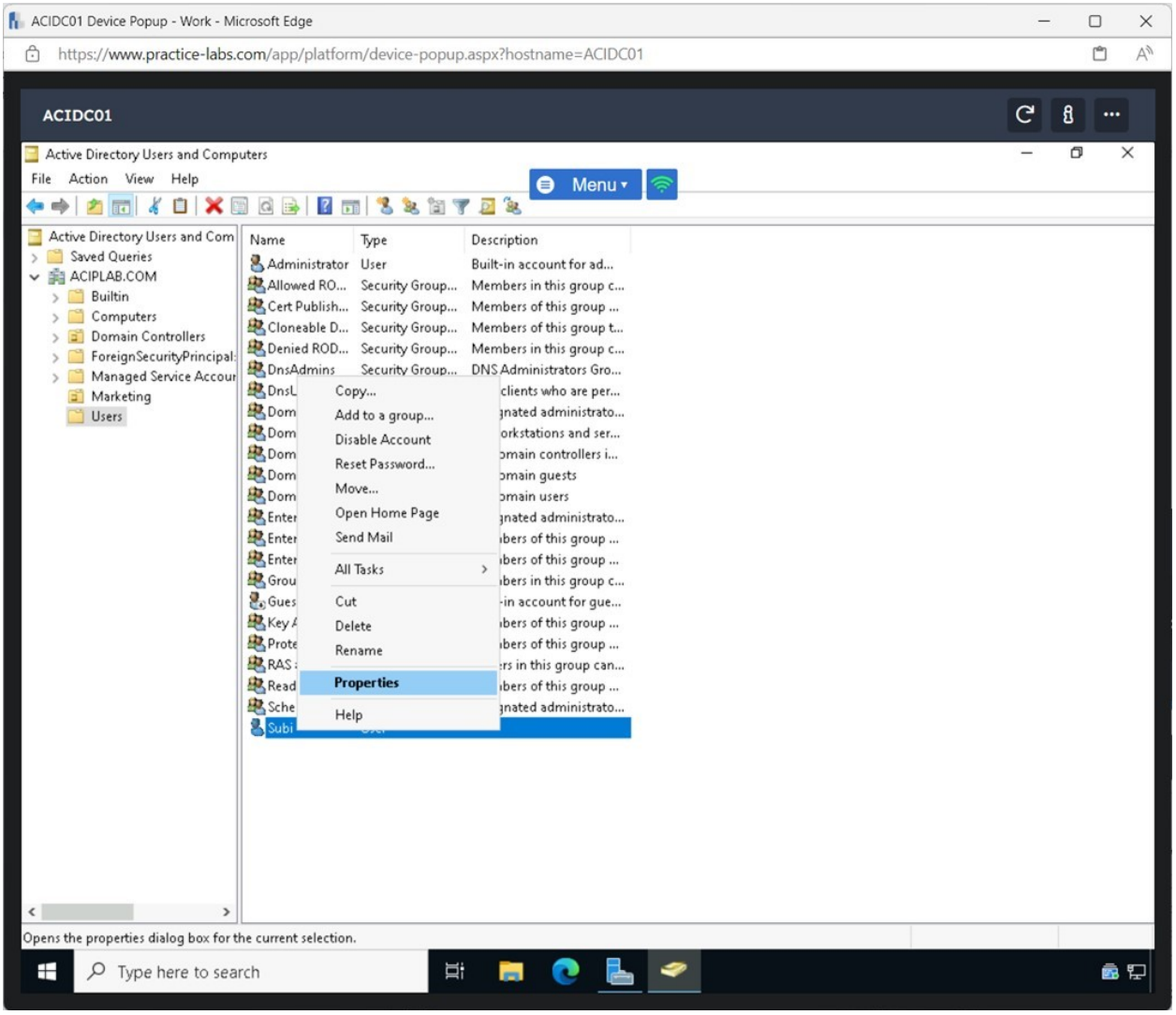
On the next screen, I completed the following fields:
Password: Passw0rd
Confirm password: Passw0rd
Unchecked the User must change password at next logon checkbox
Clicked Next.



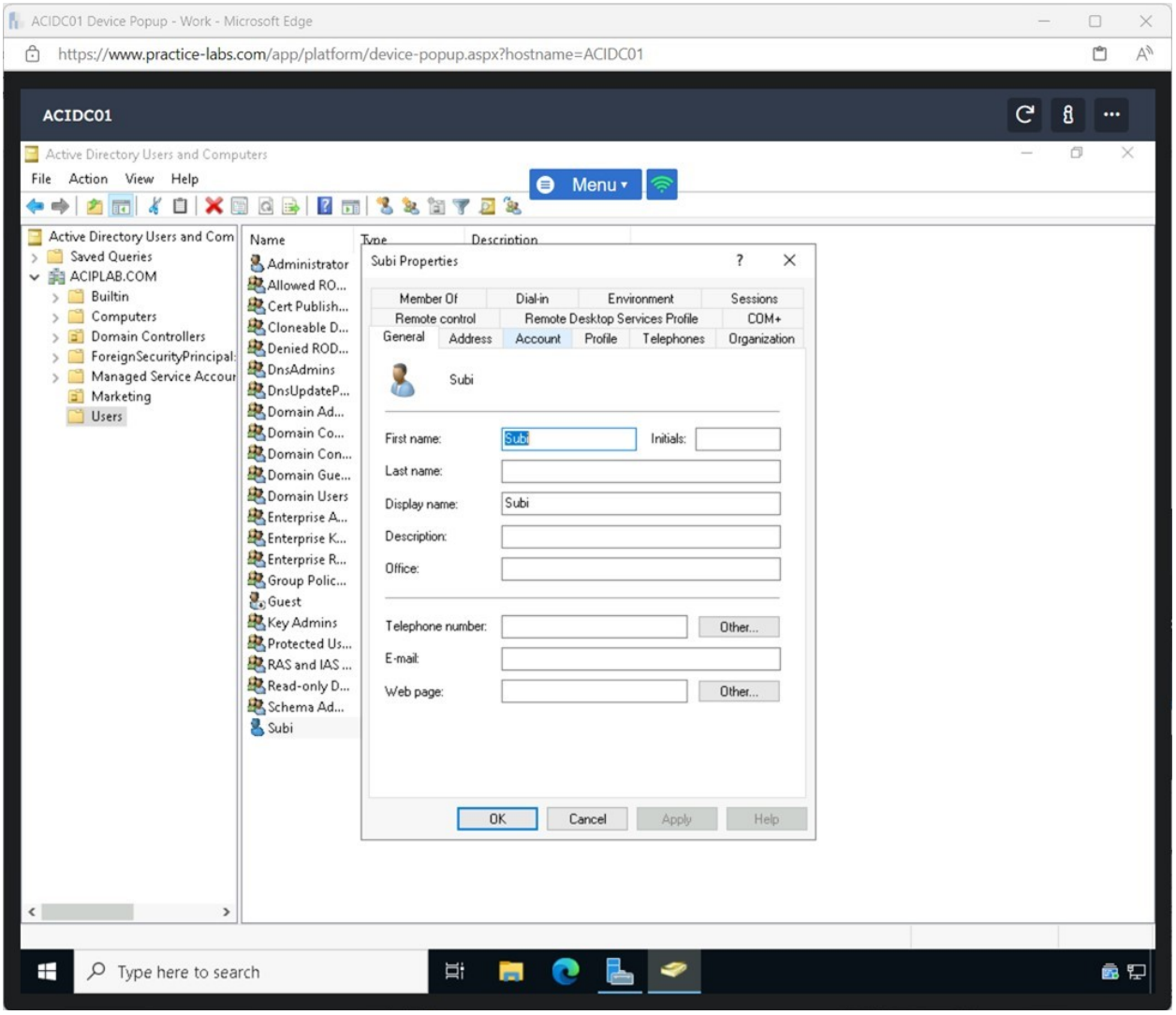
Clicked Finish on the New Object - User window.



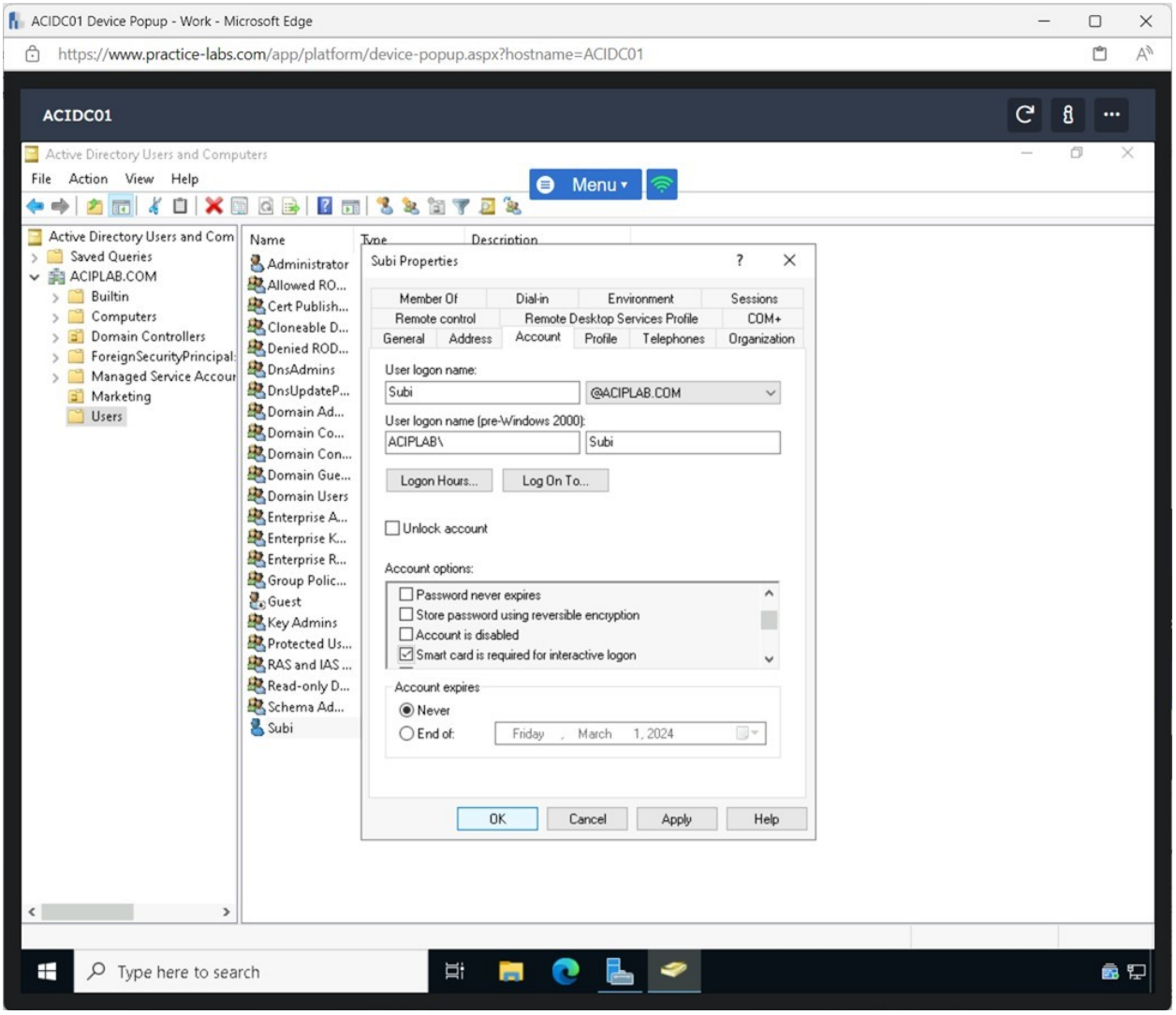
Double-clicked the Users folder on the left pane. Right-clicked Subi and selected Properties in the Active Directory Users and Computers window.



On the Subi Properties window, selected the Account tab.



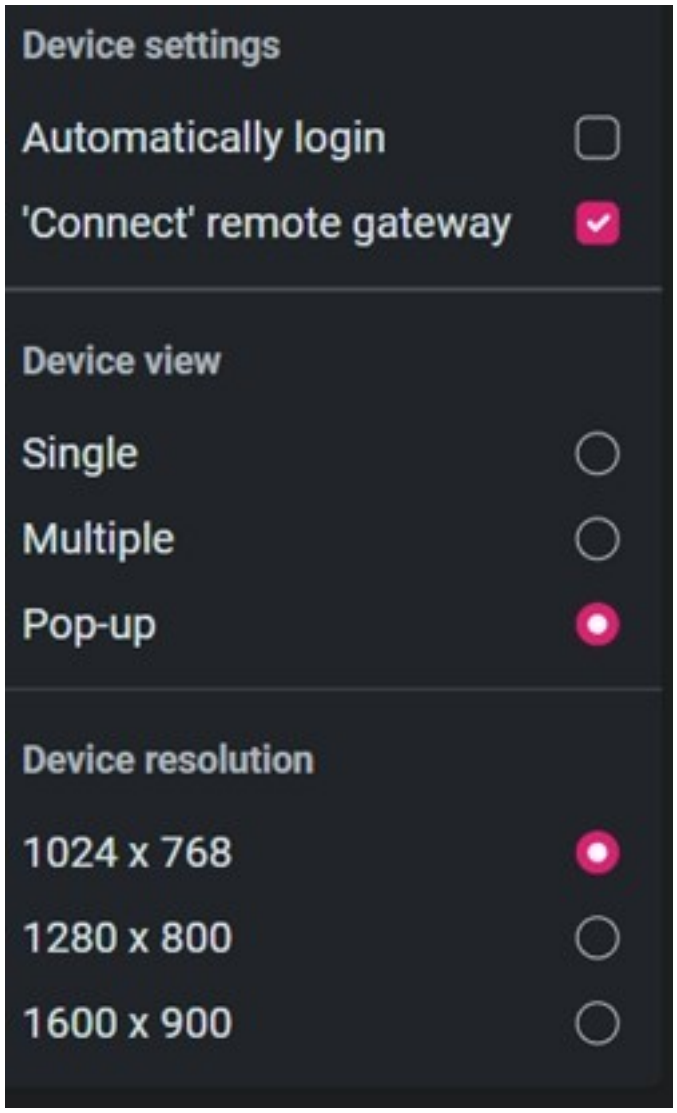
On the Properties window in the Account options pane, I scrolled down and checked the Smart card is required for interactive logon tick box.
Clicked OK.



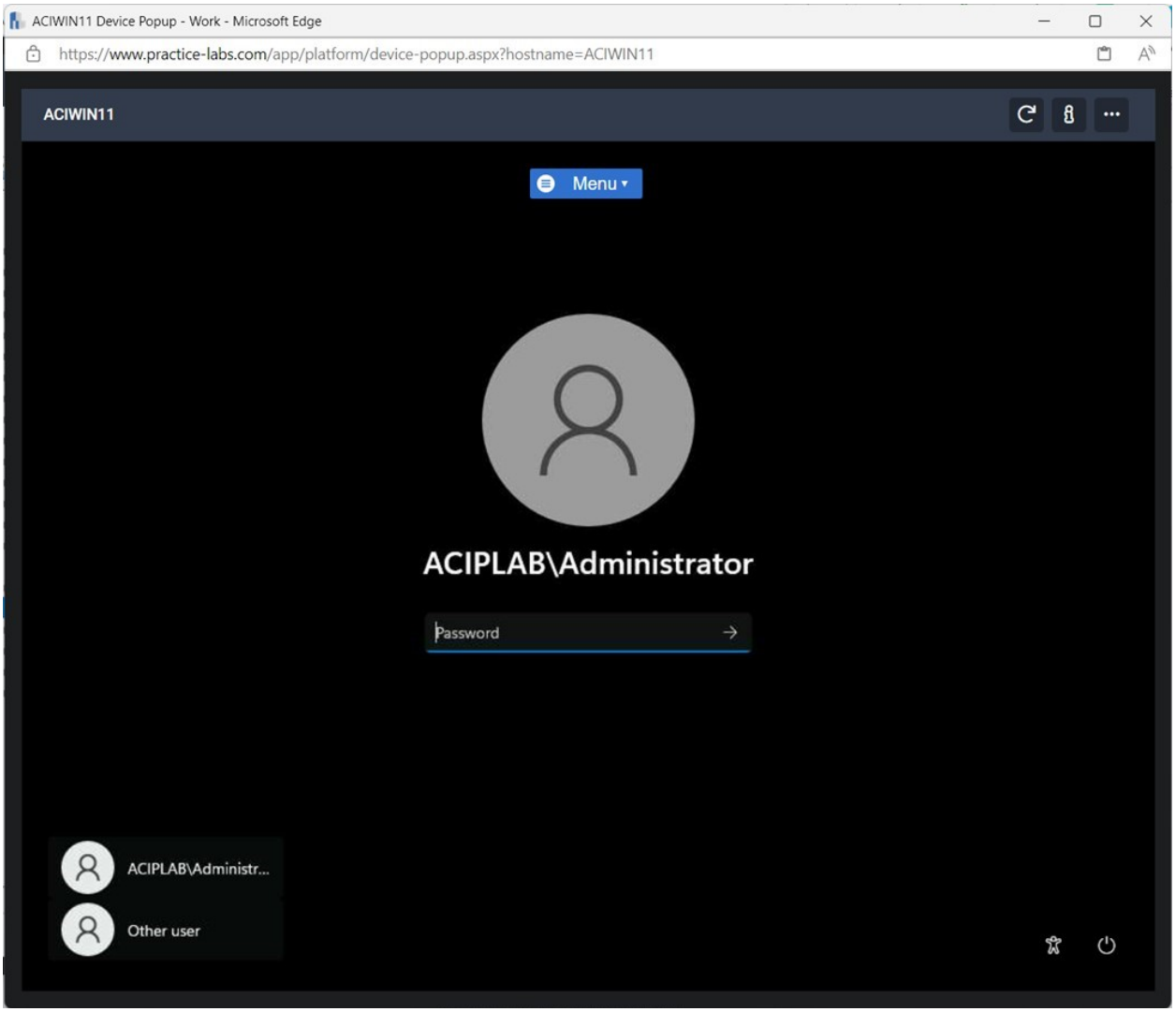
Task 2 - Verifying Multifactor Authentication

In this task, Multifactor Authentication for the newly created user was verified.

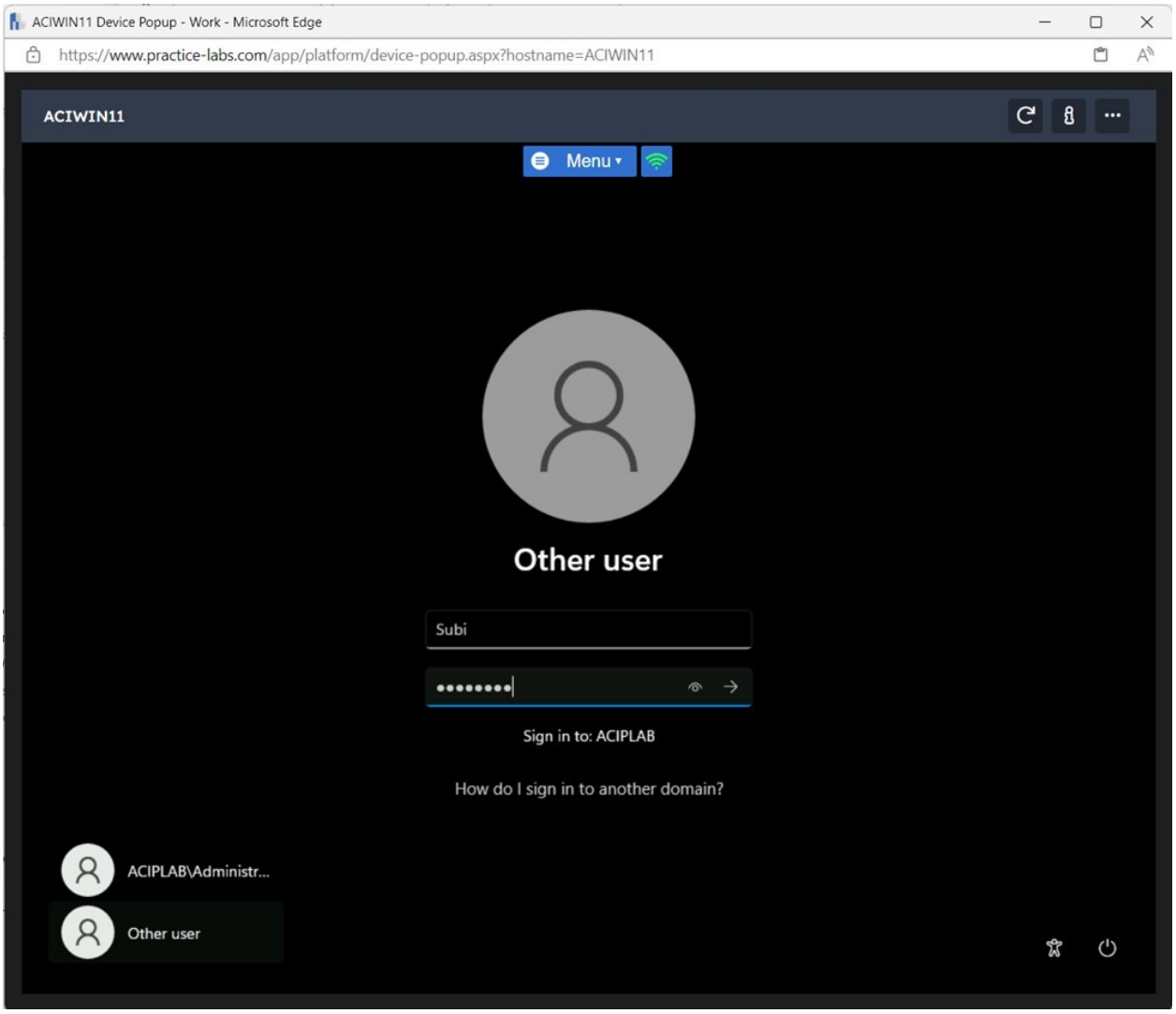
Before continuing with this task, the VM's automatic login feature needed tp be disabled.



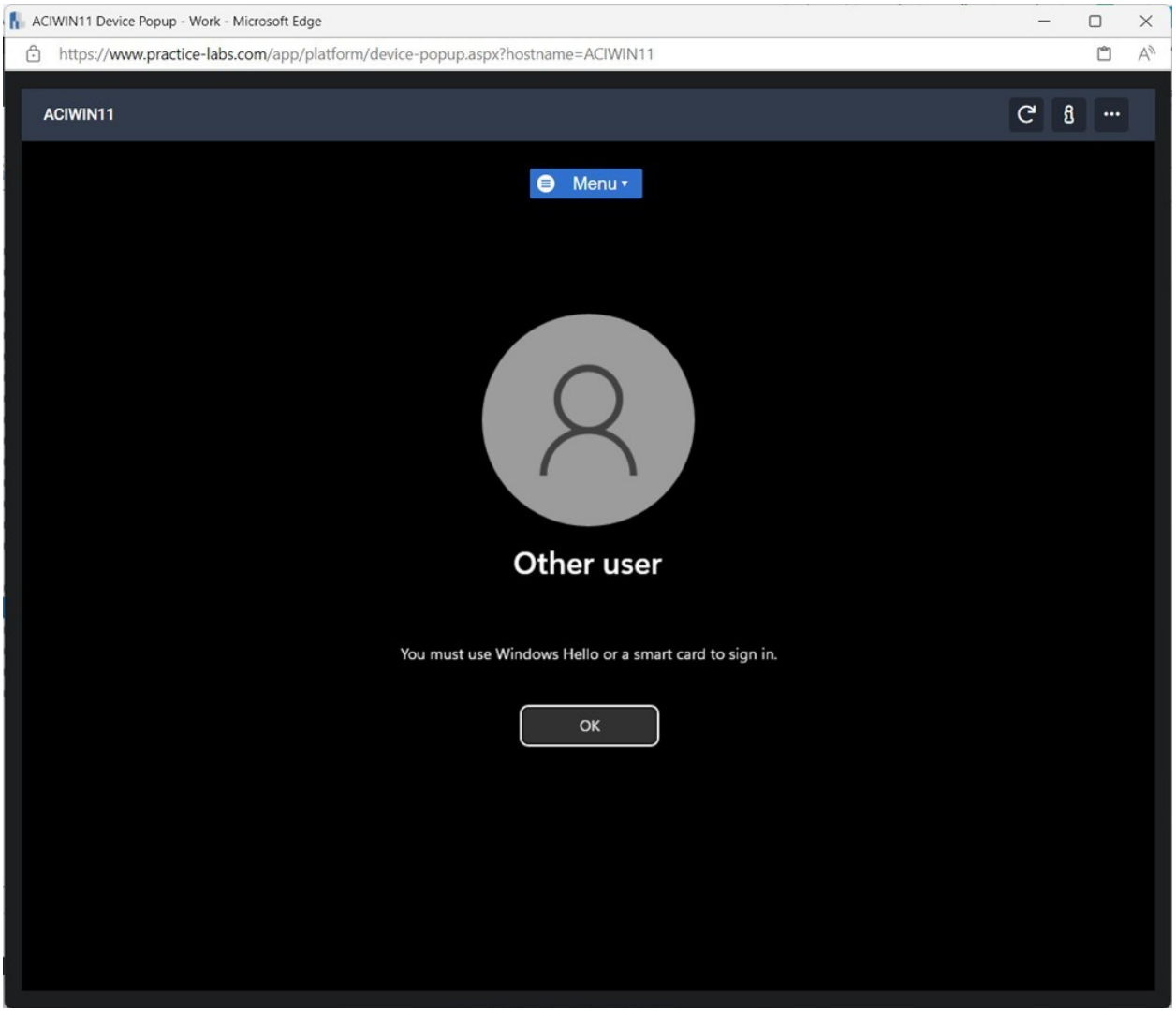
Connected to the VM, and clicked Other user on the login screen.



Entered the following on the login screen:
Username: Subi
Password: Passw0rd
Pressed Enter.



Noticed the error message when trying to log in with the user account.



Summary:

- **Install and Configure the Splunk Enterprise Application**
- **Configure a Splunk Client**
- **Collect Logs using Splunk Enterprise**
- **Install the BitLocker Drive Encryption Feature**
- **Encrypt a Local Drive on a Server**
- Overall, I learned that the importance of system and network architecture concepts in security operations includes providing an organized way for implementing security measures to identify potential threats to a network.