

Configure Security Recommendations for an Azure Virtual Machine

Understand the scenario

You are an Azure® administrator. You need to configure security recommendations for an Azure virtual machine. First, you will configure a virtual machine for security. Next, you will enable security recommendations for the virtual machine. Finally, you will enable Azure Disk Encryption.

Understand your environment

You will be using an Azure subscription named Challenge Lab--lod47561086 and a resource group named corp-data that contains a virtual machine named WinVM.

# **Configure an Azure virtual machine for security**

* Open Microsoft Edge, and then sign in to http://portal.azure.com
* Display the corp-data resource group, and then wait for the deployment of the **WinVM** virtual machine to complete.

Expand this hint for guidance on viewing the status of a deployment.

* + On the Azure portal home page, select **Resource groups**.



* + On the Resource groups page, select **corp-data**.
  + On the corp-data Overview page, in Deployments, wait for the status to display **1 Succeeded**.

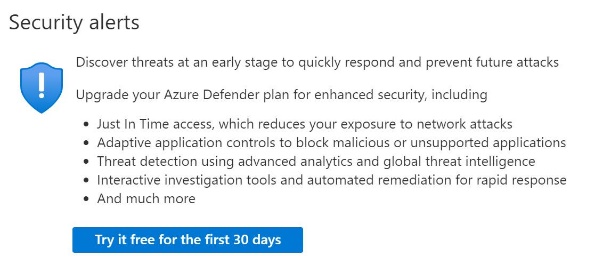
The deployment may take approximately 3–6 minutes. Wait for the deployment to complete before continuing. You may need to refresh the page to see the current status.



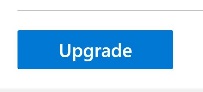
* Enable **Microsoft Defender for Cloud** Security alerts for the **WinVM** virtual machine.

Expand this hint for guidance on enabling security alerts for a virtual machine.

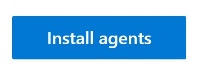
* + On the Azure portal home page, select **Virtual machines**, and then select **WinVM**.
  + On the WinVM resource menu, in Settings, select **Microsoft Defender for Cloud**.
  + On the Microsoft Defender for Cloud page, in Security alerts, select **Try it for free for the first 30 days**.



* + On the Getting started page, in the lower-left corner, select **Upgrade**.



* + On the Getting started page, select **Install agents**.



The security alerts may take 10-15 minutes or longer to enable in the background. You can continue the challenge without waiting.

* Connect to **WinVM** by using **RDP**, and then when prompted, sign in as AzureAdmin using Az!26435565! as the password.

Expand this hint for guidance on connecting to a virtual machine by using RDP.

* + On the WinVM resource menu, select **Connect**, and then select **Download RDP File**.
  + Open the RDP file, and then in the Remote Desktop Connection dialog box, select **Connect**.
  + When prompted for credentials, select **More choices**, and then select **Use a different account**.
  + In User name, enter AzureAdmin, in Password, enter Az!26435565!, and then select **OK**.
  + In the Remote Desktop Connection warning message box, select **Yes**, and then wait for the RDP session to initialize.
  + In the RDP session, if prompted to allow your PC to be discoverable by other PCs and devices on this network, select **No**.



Resize the Remote Desktop Connection window so that you can view the instructions for the challenge at the same time.

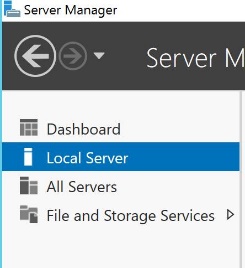
* Verify that **Windows Defender Firewall** is enabled on **WinVM** for security.

Expand this hint for guidance on verifying that Windows Defender is enabled.

* + In the Remote Desktop Connection window, wait for Server Manager to start automatically.
  + In Server Manager, if prompted to Try managing servers with Windows Admin Center, close the message box.



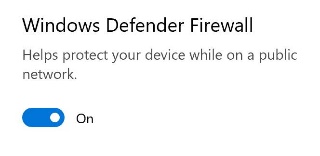
* + In Server Manager, select **Local Server**.



* + In Properties for WinVM, in Windows Defender Firewall, select **Public: On**.
  + In the Windows Security window, select **Public network**.



* + In the Public network window, in Windows Defender Firewall, ensure that **On** is selected, and then close the **Windows Security** window.

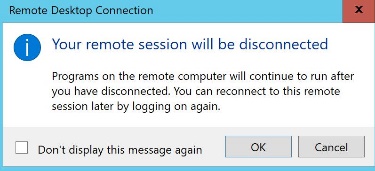


* + In the Remote Desktop Connection window, on the Start menu, select **Control Panel**.
  + In Control Panel, select **System and Security**, and then select **Windows Defender Firewall**.
  + Ensure that Incoming connections is set to **Block all connections to apps that are not on the list of allowed apps**, and then close the **Windows Firewall** window.



* Close the **Remote Desktop Connection** window.

If prompted, disconnect from the remote session.



## Check your work

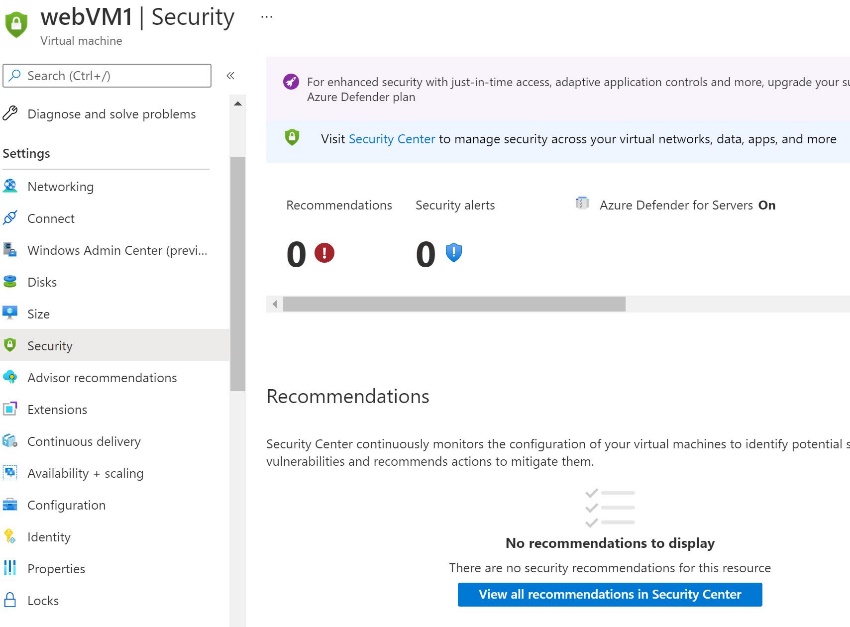
* Confirm that you configured WinVM for security alerts.
* Confirm that you connected to WinVM by using RDP.
* Confirm that you verified that Windows Defender Firewall is enabled on WinVM.

# **Enable security recommendations**

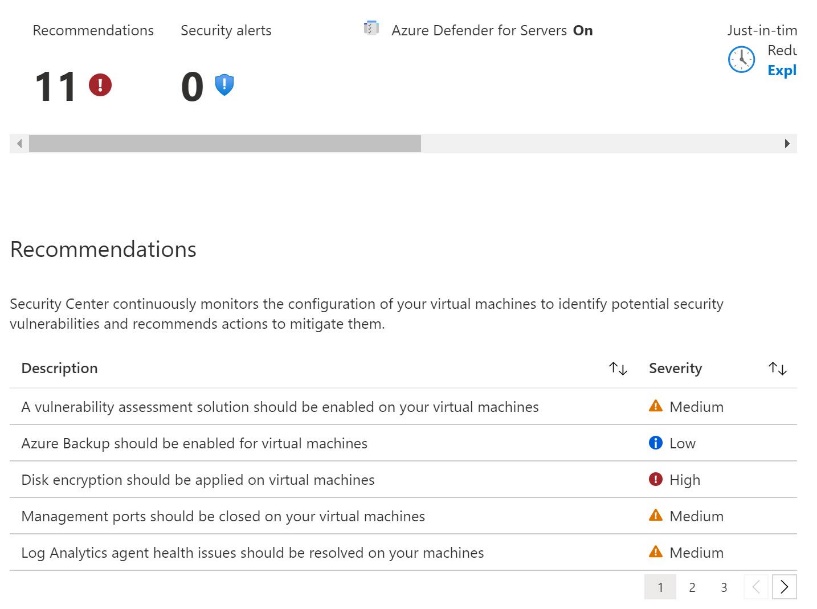
* Display the security recommendations for **WinVM**.

Expand this hint for guidance on viewing the security recommendations for a virtual machine.

* + On the WinVM resource menu, in Settings, select **Microsoft Defender for Cloud**.
  + On the Microsoft Defender page, in Recommendations, monitor the the security recommendations until you see recommendations for the virtual machine.
  + The following screenshot shows the initial display on the page:



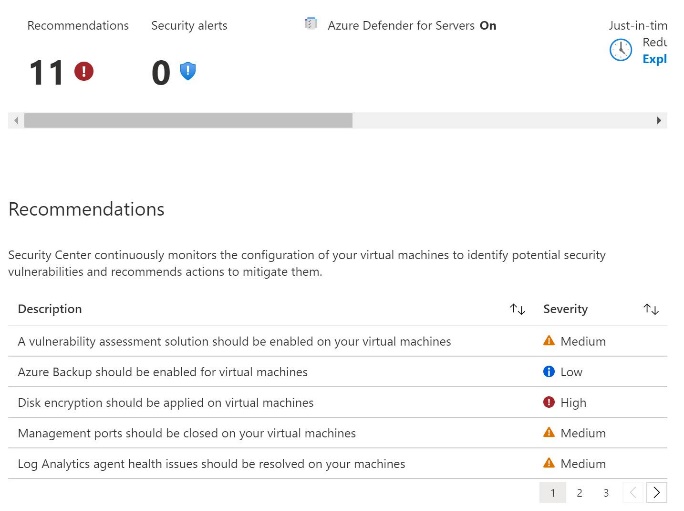
* + When the security recommendations are updated, they should resemble the following screenshot:



You will not see any recommendations until the agent has been installed on WinVM and has reported telemetry to Azure. Please be patient. It may take 10–15 minutes for all recommendations to appear.

You may need to refresh the browser window to see the recommendations. You can also select WinVM on the breadcrumb menu, and then select the Security page again.

When the security recommendations fully appear, they should resemble the following screenshot:

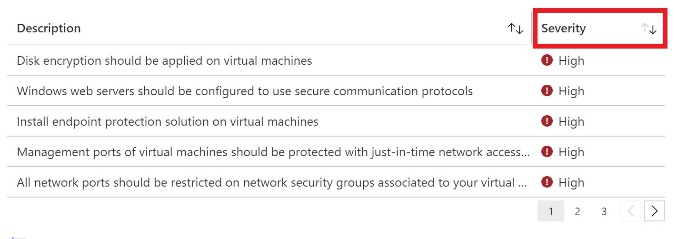


[Azure Security Center](https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction) is an expert system that advises you on security recommendations based on best practices. The security best practices can be customized to your own requirements for specific needs by using [Azure Policy](https://docs.microsoft.com/en-us/azure/security-center/policy-reference).

* Sort the security recommendations by **Severity** in descending order to view the high severity recommendations.

Expand this hint for guidance on sorting the security recommendations.

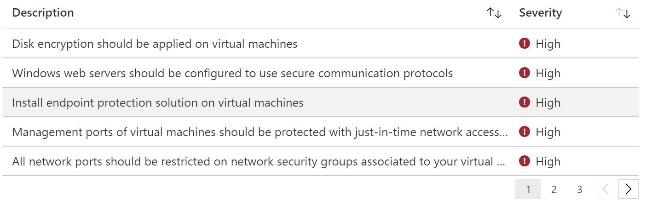
* + On the WinVM Security page, in Recommendations, select the **Severity** column header twice to sort the recommendations in descending order.



* Follow the **Install endpoint protection solution on virtual machines** recommendation by installing the **Microsoft Antimalware** extension on **WinVM**.

Expand this hint for guidance on installing the Microsoft Antimalware extension.

* + On the WinVM Security page, in Recommendations, select the **Install endpoint protection solution on virtual machines** recommendation.



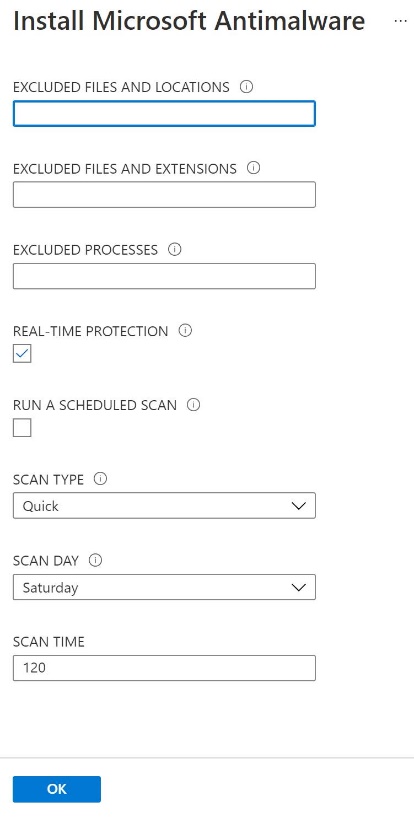
* + On the Endpoint Protection not installed on Azure VMs page, ensure that **WinVM** is selected, and then on the command bar, select **Install on 1 VMs**.



* + On the Select Endpoint Protection page, select **Microsoft Antimalware**.



* + On the Microsoft Antimalware page, select **Create**.
  + On the Install Microsoft Antimalware blade, review the default settings, and then select **OK** to initiate the deployment.



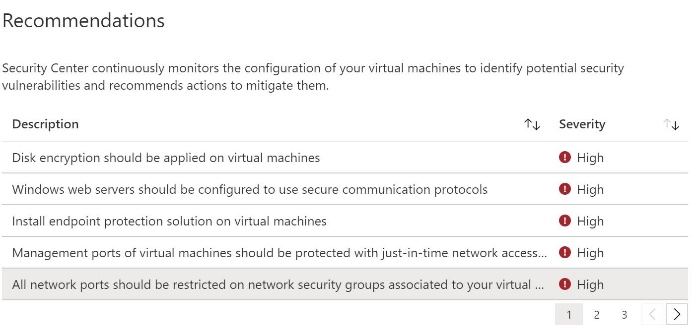
* + Close the **Endpoint Protection not installed on Azure VMs** page.

The Microsoft Antimalware extension may take at least 5–10 minutes to install in the background. You can continue the challenge without waiting.

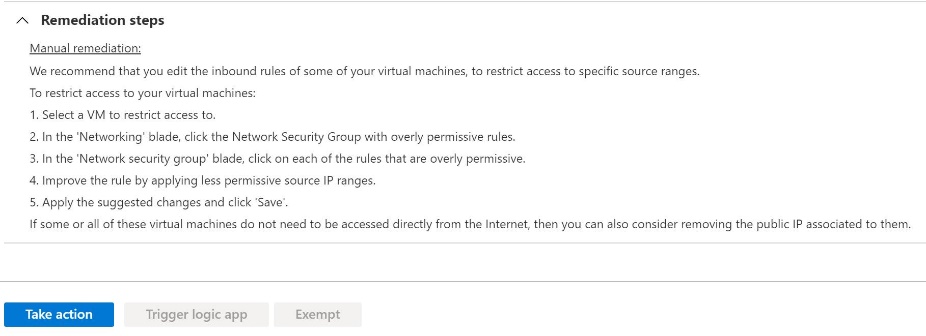
* Follow the **All network ports should be restricted on network security groups associated to your virtual machine** recommendation by deleting the **default-allow-3389** inbound security rule for the **WinVM** virtual machine.

Expand this hint for guidance on deleting the RDP inbound security rule for a virtual machine.

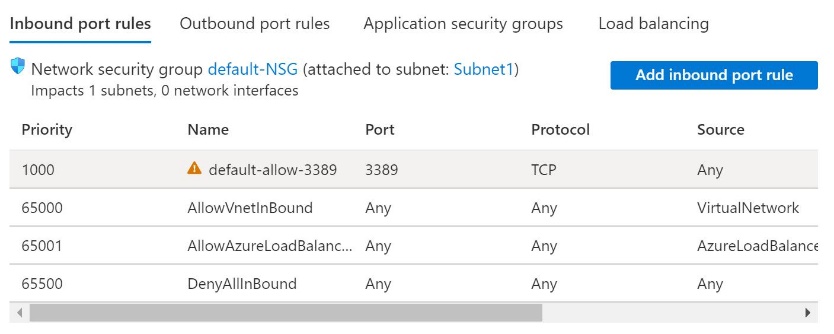
* + On the WinVM Security page, in Recommendations, select the **All network ports should be restricted on network security groups associated to your virtual machine** recommendation.



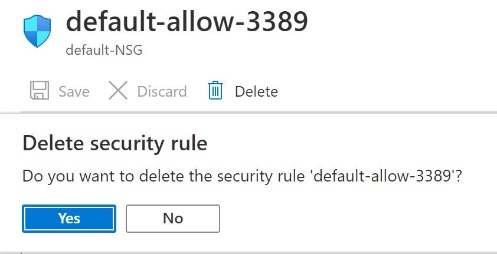
* + Expand **Remediation steps** to view the manual steps to remediate the security vulnerability, and then select **Take action** to display the WinVM Networking page.



* + On the WinVM Networking page, in Inbound port rules, select the **default-allow-3389** rule.



* + On the default-allow-3389 blade, on the command bar, select **Delete**, and then in the Delete security rule message, select **Yes**.



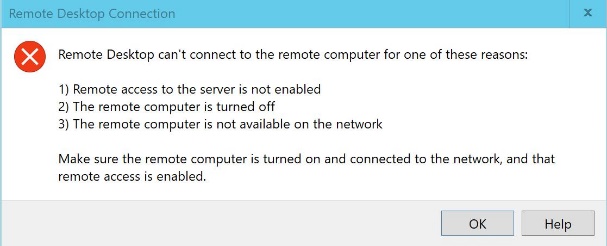
Wait for the default-allow-3389 inbound security rule to be deleted. This may take approximately 1-2 minutes.

* Attempt to connect to **WinVM** by using **RDP**, and then when prompted, sign in as AzureAdmin using Az!26435565! as the password.

Expand this hint for guidance on attempting to connect to a virtual machine by using RDP.

* + On the WinVM resource menu, select **Connect**, and then select **Download RDP File**.
  + Open the RDP file, and then in the Remote Desktop Connection dialog box, select **Connect**.
  + Wait for the error message that RDP connections are no longer allowed, and then select **OK** to dismiss the message box.

You should see a Remote Desktop Connection error message that RDP connections are no longer allowed for the WinVM virtual machine.



If the connection is allowed, try again. The security rule may take 1-2 minutes to be deleted.

## Check your work

* Confirm that you reviewed the security recommendations.
* Confirm that you initiated the installation of the Microsoft Antimalware extension on WinVM.
* Confirm that you deleted the default-allow-3389 inbound security rule on WinVM.
* Confirm that you verified that RDP connections are no longer allowed for WinVM.

# **Enable Azure Disk Encryption**

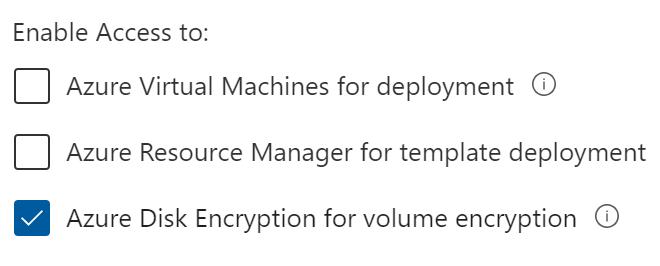
* Create an Azure key vault by using the values in the following table. For any property that is not specified, use the default value.

| **Property** | **Value** |
| --- | --- |
| Resource group | **corp-data** |
| Key vault name | KV26435565 |
| Pricing tier | **Standard** |
| Enable access to | **Azure Disk Encryption for volume encryption** |

* Expand this hint for guidance on creating an Azure key vault.
  + On the Azure portal menu, select **Create a resource** to display the Azure Marketplace.
  + In the Azure Marketplace, search for and select Key Vault, and then select **Create**.



* + On the Create key vault blade, on the Basics page, in Resource group, select **corp-data**, in Key vault name, enter KV26435565, and then in Pricing tier, ensure that **Standard** is selected.
  + On the Access policy page, select the **Azure Disk Encryption for volume encryption** check box.



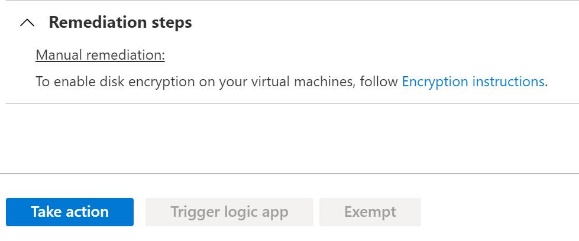
* + Select **Review + create**, and then review the specifications for the key vault.
  + Select **Create**, and then wait for the deployment to complete.

The deployment will take approximately 1–2 minutes.

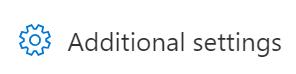
* Follow the **Disk Encryption should be applied on virtual machines** recommendation for the **OS disk** on the **WinVM** virtual machine by using a new key named BEK1 in the **KV26435565** key vault.

Expand this hint for guidance on applying Azure Disk Encryption on a virtual machine.

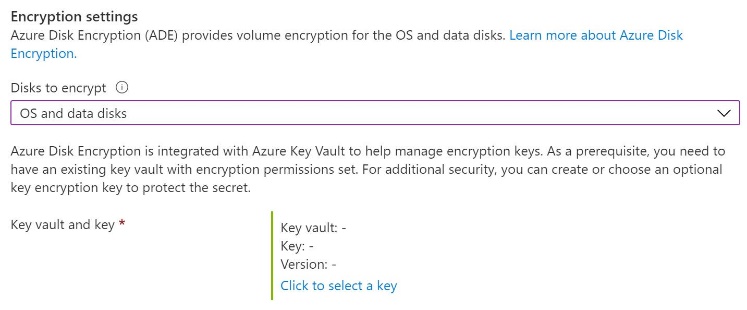
* + On the Azure portal home page, select **Virtual machines**, and then select **WinVM**.
  + On the WinVM resource menu, select **Security**.
  + On the Security page, in Recommendations, select the **Disk Encryption should be applied on virtual machines** recommendation.
  + On the Disk Encryption should be applied on virtual machines page, expand **Remediation steps** to view the manual steps to remediate the security vulnerability, and then select **Take action** to display the WinVM Disks page.



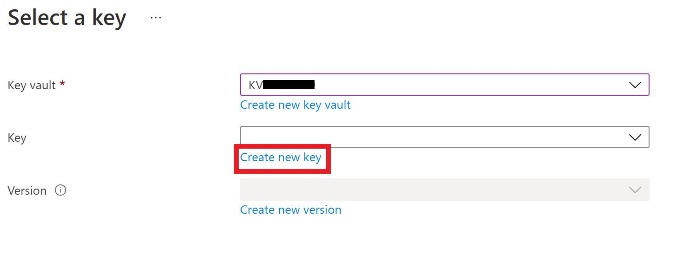
* + On the WinVM Disks page, on the command bar, select **Additional settings**.



* + On the Disk settings pane, in Disks to encrypt, select **OS disk**, and then in Key vault and key, select **Click to select a key**.



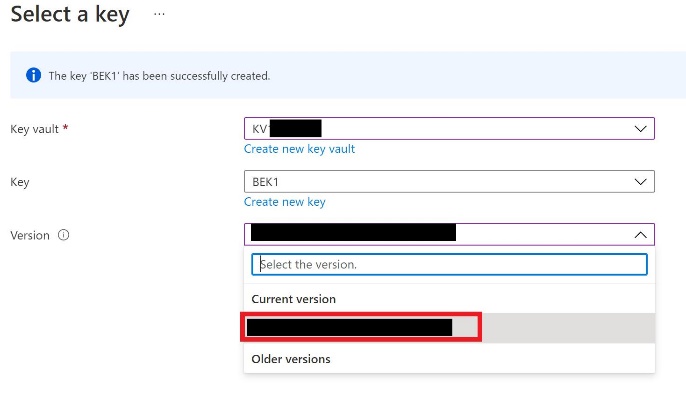
* + On the Select a key blade, in Key vault, select **KV26435565**, and then in Key, select **Create new key**.



* + On the Create a key blade, in Name, enter BEK1, accept the remaining default values, and then select **Create**.



* + On the Select a key blade, in Key, ensure that **BEK1** is selected, in Version, ensure that the current version number—a 32 digit hexadecimal number—is selected, and then select **Select**.



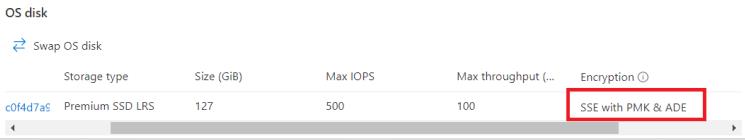
* + On the Disk settings page select **Save**, and then wait for the disk encryption operation to complete.

Wait for the disk encryption operation to complete. This may take approximately 3–5 minutes.

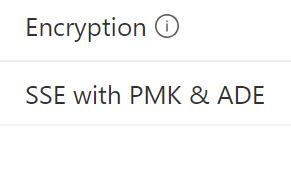
* Verify that the updated OS disk specifications include Azure Disk Encryption.

Expand this hint for guidance on verifying the updated disk specifications.

* + On the WinVM Disks page, in OS disk, verify that the Encryption column is set to **SSE with PMK & ADE** encryption.



The updated OS disk specifications should show the OS disk is encrypted by using server-side encryption with a platform-managed key and Azure Disk Encryption (SSE with PMK & ADE).



[Server-side encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption) (SSE) of Azure Disk Storage is enabled by default and encrypts disks at the storage server level by using a platform-managed key (PMK). The encryption key is managed automatically by the platform—in this case, Azure—including protection and regular rotation.

Server-side encryption with a customer-managed key (SSE with CMK) enables a customer to manage the encryption key manually for compliance reasons. You can combine SSE with [Azure Disk Encryption](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview) (ADE) to encrypt the disk at the OS level by using technologies such as BitLocker (Windows) or DM-Crypt (Linux) for situations in which you have what are called double encryption at rest high security requirements.

## Check your work

* Confirm that you created an Azure key vault.
* Confirm that you enabled Azure Disk Encryption.
* Confirm that you verified Azure Disk Encryption.

# **Summary**

Congratulations, you completed the **Configure Security Recommendations for Virtual Machines** challenge.

You have accomplished the following:

* Configured an Azure virtual machine for security.
* Enabled security recommendations.
* Enabled Azure Disk Encryption.