

Azure Disk Encryption (ADE) Home

Last updated by | Kevin Gregoire | Mar 29, 2022 at 11:47 AM PDT

Tags

cw.Azure-Encryption

cw.Reviewed-06-2021

Contents

- [Welcome!](#)
 - [Short URL](#)
- [Contact List](#)
- [Troubleshooting Guides \(TSGs\) and How To Articles](#)
- [Introduction](#)
 - [Reference](#)
- [How this works?](#)
 - [ADE Single-Pass feature](#)
 - [Workflow](#)
 - [Diagram](#)
 - [ADE Dual-Pass feature](#)
 - [Workflow](#)
 - [Diagram](#)
 - [Unsupported Scenarios](#)
 - [Portal Integration](#)
 - [Troubleshooting](#)
 - [Data Collection](#)
 - [Windows VM](#)
 - [Linux ADE Link](#)
 - [Escalation](#)
- [Need additional help or have feedback?](#)

Welcome!

Welcome to the Azure Disk Encryption (ADE) Homepage!

Short URL

<https://aka.ms/azvmade> 

Contact List




Below is a contact list for all of our SME's in each region. Please contact us if you have any questions after reviewing our public and internal resources.

North America	IST/EMEA	APAC
Edgar Garcia Mujica (Windows Champ)	Andrei Dita (Windows)	Sucheng Lai (Windows)
Carolina Hidalgo (Windows)	Gabriel Petre (Windows)	
Didier Ambroise (Windows)	Mohammad Daoud (Windows)	
Jose Francisco Franceschi (Linux Champ)	Amit Kumar Prasad (Linux)	
Eli Corrales (Linux)	Lirish Lal (Windows)	
Brandon Fett (Linux)	Amit Karmakar (Linux)	
	Marin Nedea (Linux)	

Troubleshooting Guides (TSGs) and How To Articles



- [ADE Troubleshooting Guides](#)
- [ADE How To Articles](#)

Introduction

Azure Disk Encryption is a capability that helps you encrypt your Windows and Linux IaaS virtual machine disks. Azure Disk Encryption leverages the industry standard [BitLocker](#)  feature of Windows and the [DM-Crypt](#)  feature of Linux to provide volume encryption for the OS and the data disks. The solution is integrated with [Azure Key Vault](#)  to help you control and manage the disk-encryption keys and secrets in your key vault subscription. The solution also ensures that all data on the virtual machine disks are encrypted at rest in your Azure storage.

Azure disk encryption for Windows and Linux IaaS VMs is now in General Availability in all Azure public regions and AzureGov regions for Standard VMs and VMs with premium storage.

Reference

- The link to the official online documentation for [Azure Disk Encryption \(ADE\)](#) 
- If the customer is looking to encrypt a storage account to ensure all VHDs to enter the storage account are encrypted, they should refer to [Azure Storage Service Encryption for Data at Rest](#) 

How this works?

ADE Single-Pass feature

▼ Click here to expand or collapse this section

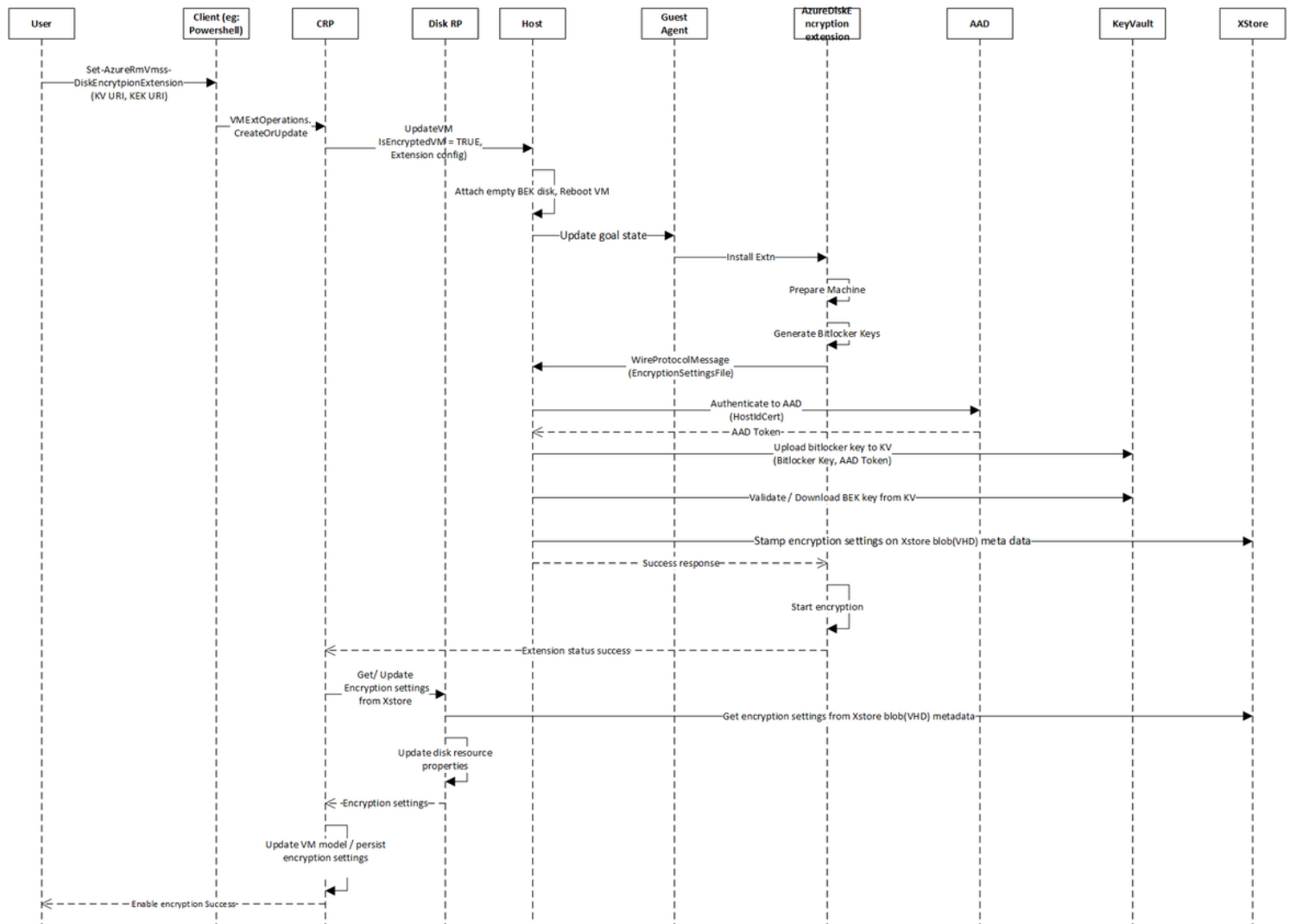
The new release of Azure Disk Encryption (single-pass) eliminates the requirement to provide an Azure Active Directory (Azure AD) application parameter to enable VM disk encryption. With the new release, you're no longer required to provide an Azure AD credential during the enable encryption step. All new VMs must be encrypted without the Azure AD application parameters when you use the new release. VMs that were already encrypted with Azure AD application (dual-pass) parameters are still supported and should continue to be maintained with the Azure AD syntax.

Workflow

To enable disk encryption for Windows and Linux VMs, do the following steps:

1. Choose an encryption scenario from the scenarios listed in the Encryption scenarios section.
2. Opt in to enable disk encryption via the Azure Disk Encryption Resource Manager template, PowerShell cmdlets, or the Azure CLI, and specify the encryption configuration.
 - For the customer-encrypted VHD scenario, upload the encrypted VHD to your storage account and the encryption key material to your key vault. Then, provide the encryption configuration to enable encryption on a new IaaS VM.
 - For new VMs that are created from the Marketplace and existing VMs that already run in Azure, provide the encryption configuration to enable encryption on the IaaS VM.
3. Grant access to the Azure platform to read the encryption key material (BitLocker encryption keys for Windows systems and Passphrase for Linux) from your key vault to enable encryption on the IaaS VM.
4. Azure updates the VM service model with encryption and the key vault configuration, and sets up your encrypted VM.

Diagram



ADE Dual-Pass feature

▼ Click here to expand or collapse this section

This previous release needed Azure AD credentials during the enable encryption process.

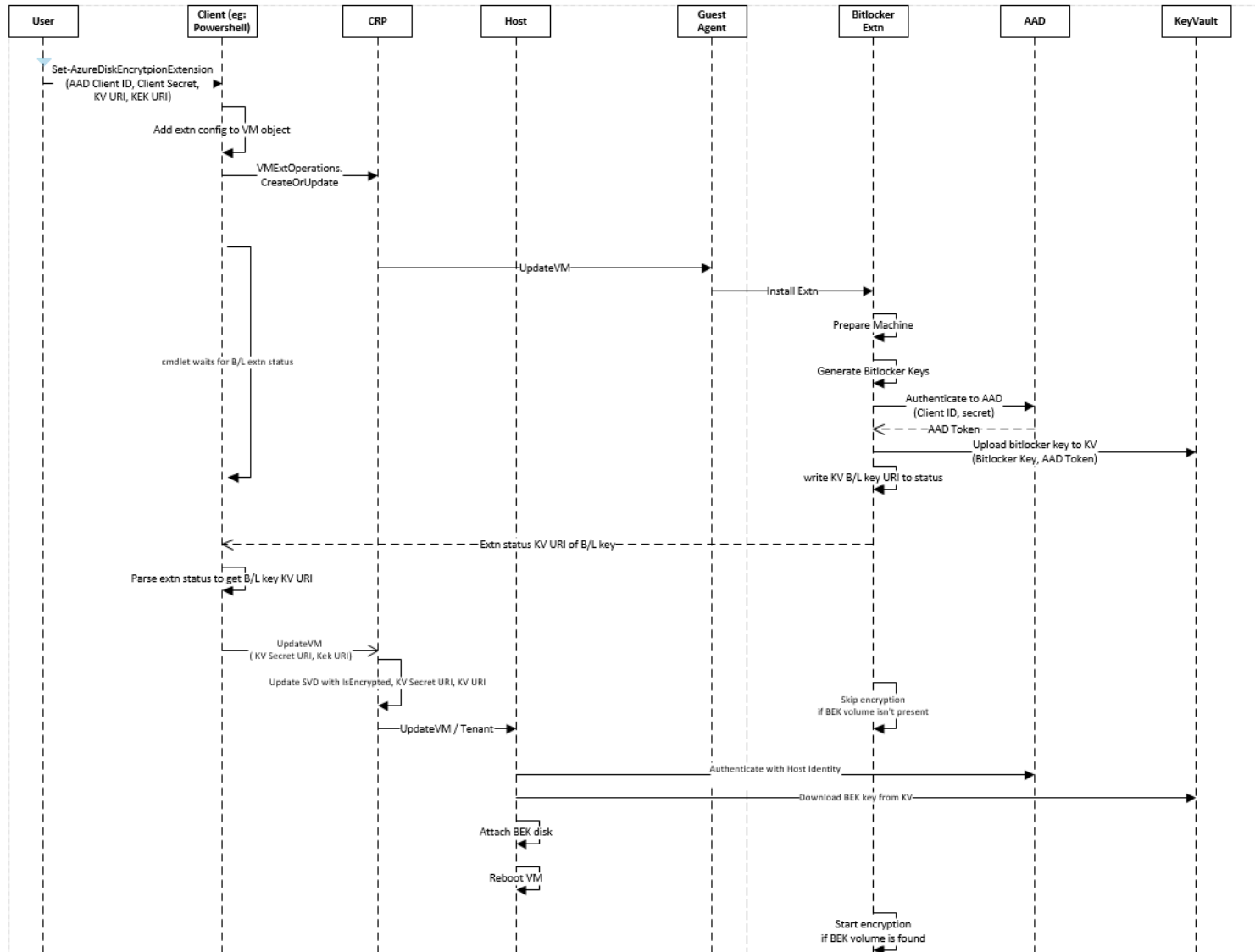
Workflow

To enable disk encryption for Windows and Linux VMs on the previous ADE release, do the following steps:

1. Choose an encryption scenario from the scenarios listed in the Encryption scenarios section.
2. Opt in to enable disk encryption via the Azure Disk Encryption Resource Manager template, PowerShell cmdlets, or the Azure CLI, and specify the encryption configuration.
 - For the customer-encrypted VHD scenario, upload the encrypted VHD to your storage account and the encryption key material to your key vault. Then, provide the encryption configuration to enable encryption on a new IaaS VM.
 - For new VMs that are created from the Marketplace and existing VMs that already run in Azure, provide the encryption configuration to enable encryption on the IaaS VM.
3. Grant access to the Azure platform to read the encryption key material (BitLocker encryption keys for Windows systems and Passphrase for Linux) from your key vault to enable encryption on the IaaS VM.
4. Provide the Azure AD application identity to write the encryption key material to your key vault. This step enables encryption on the IaaS VM for the scenarios mentioned in step 2.

5. Azure updates the VM service model with encryption and the key vault configuration, and sets up your encrypted VM.

Diagram



Unsupported Scenarios

- [Unsupported Windows ADE scenarios](#)
- [Unsupported Linux ADE scenarios](#)

Portal Integration

Currently engineering is releasing the Azure Disk Encryption integration in the Azure portal. This is currently live in MPAC while further tests are needed

Troubleshooting

The cases/problem to troubleshoot this tool, should be coded with the following support topic:

Routing Azure Virtual Machine V3\Configuration and Setup\Encrypt virtual machine disk

Data Collection

▼ Click here to expand or collapse this section

1. Review the Customer verbatim and validate if the case has all the minimum required details as below to start working.
 1. The VM needs to be started
 2. Check if we have the approval from the customer to collect the Guest OS Logs. You could find this within the Customer Verbatim under the GrantPermission variable:
2. Permission:
 1. If granted go to 3:
 2. If NOT granted, direct customer to forward an archive of the root folder found in Step 4.
3. Run Inspect IaaS against the respective VM(s) (Note: If the VM OS disk is successfully encrypted, InspectIaaS should not be successful.)
4. Subscription Id:
5. Region of the VM:
6. Resource Group of the VM:
7. Name of the VM:
8. Size of the VM:
9. Approximate time at which encryption was attempted:
10. For Linux VMs, 2 additional information required:
 1. Distro and version of Linux VM, eg. RHEL 7.2
 2. Get Boot diagnostics log from the VM if the VM fails to boot.
11. Get the VM / extension logs from customer's VM
 1. For **Windows VMs**
 1. AzureDiskEncryption extension logs

```
C:\WindowsAzure\Log\Plugins\Microsoft.Azure.Security.AzureDiskEncryption
```

2. AzureDiskEncryption extension config

```
C:\Packages\Plugins\Microsoft.Azure.Security.AzureDiskEncryption\RuntimeSettings
```

3. Bitlocker state of the machine, from an elevated CMD:

```
Manage-bde -status
Manage-bde -protectors -get C:
```

4. Bitlocker system event logs:

```
C:\Windows\System32\winevt\Logs\Microsoft-Windows-BitLocker%4BitLocker Management.evtx
C:\Windows\System32\winevt\Logs\Microsoft-Windows-BitLocker-DrivePreparationTool%4Operation
```



2. For **Linux VMs**

1. AzureDiskEncryption extension logs **ADE Single-pass:**

```
/var/log/azure/Microsoft.Azure.Security.AzureDiskEncryptionForLinux/extension.log
```

ADE Dual-pass:

```
/var/log/azure/Microsoft.Azure.Security.AzureDiskEncryptionForLinux/*/extension.log
```

2. AzureDiskEncryption extension configs:

```
/var/lib/waagent/Microsoft.Azure.Security.AzureDiskEncryptionForLinux-*/config/*.settings
```

3. AzureDiskEncryption extension internal configs:

```
/var/lib/azure_disk_encryption_config/
```

4. Azure Linux Agent Logs:

```
/var/log/waagent.log
```

5. Output of following commands:

```
# lsblk
# cat /etc/fstab
# df -h
```

6. The extension version may change in the future. Get the logs from the extension version installed on the VM. The following commands can be used to extract the required logs

```
# lsblk > /tmp/ADEoutputs; df -h >> /tmp/ADEoutputs; cat /etc/fstab* >> /tmp/ADEoutputs; cat /etc
# tar -cvzf /tmp/ADELogs.tar.gz /var/log/azure /var/lib/azure_disk_encryption_config/ /tmp/ADEc
```



12. Look at the CRP Logs to follow the life cycle of the VM. Look at Context activity logs for the two update VM calls for enabling encryption. Provide short links to CRP logs searched in the Jarvis portal, so its faster to debug.

1. Look at context activity logs

1. Go to [Jarvis](#) from your SAW device

1. Look at **ApiQos** Event logs

1. [Sample Query](#)

2. Fill in the values here:

Jarvis | Dashboard | Health | **Logs** | Actions NEW | Manage

DGrep

Q Server Query

Endpoint
 Diagnostics PROD

Namespace
 Crp

Events to search
 type event name...
☐ Select All
☒ ApiQosEvent
☐ AlertingEvent
☐ AllocatorGlobalContextActivity
☐ ApiQosEventEx
☐ BackupContextActivityEvent

Time range
 Now 03/31/2017 21:06 UTC
 -5mins -1 min +1 min +5mins
 ± + - 2 Days
 1 2 3 5 15 30

Scoping conditions
 MonitoringAp... == CRP-NorthEurope_Mon

Field

Filtering conditions Advanced Query ☐
 subscriptionId contains f12880d5-584c-4d8
 resourceGroup contains ANLFINANCEDEV
 resourceName contains AZUREANLFD00
 operationName contains get

3. In the results, select / filter the columns:

- *PreciseTimeStamp*: Time at which the operation is performed
- *ResourceName*: For extensions it would VMName/AzureDiskEncryptionExtension or VmName/AzureDiskEncryptionExtensionForLinux
- *OperationName*: PUT for update VMs. START for start VM
- *OperationId*: This is the id to be used to co-relate with Context activity logs . This maps to 'activityId' in ContextActivity events
- *Node*: Node ID can be used to filter context activity logs
- *ErrorDetails*: All extension thrown error messages show up here
- *UserAgent*: This tells whether user used powershell / cli / templates to enable encryption
- *ClientPrincipalName*: user's mEmail id , in case to contact
- *Client query*: orderby PreciseTimeStamp desc

2. Check the **ContextActivity** Logs

1. Leave namespace = CRP. In Events to Search, deselect all and then select "ContextActivity"
2. In the Scoping conditions clear all, then add Node
3. In the Filtering conditions clear all, then add activityID

Windows VM

▼ Click here to expand or collapse this section

The cases/problem to troubleshoot this tool, should be coded with the following support topic:

Eligible product:	Azure Virtual Machine – Windows
Routing product:	<div>1</div> <div>Azure Virtual Machine – Windows</div> <div>Windows</div>
Support topic:	<div>Routing Azure Virtual Machine V3\Configuration and Setup\Encrypt virtual machine disk</div> <div>2</div>

Linux ADE Link

[Azure Linux Disk Encryption \(ADE Linux\)](#)

Escalation

If the troubleshooting steps found in the wiki don't work please follow the escalation process outlined below:

ADE Windows Escalation Process:

1. You can reach out to the Teams Channel [Azure Disk Encryption teams channel](#) ☑ for advise providing the case number, issue description and your question.
2. You can also contact by sending an email to the [Azure Disk Encryption Support DL](#)
3. For escalation on this feature, please file an [ICM to the Azure Disk Encryption team](#) ☑
 1. For **production down** scenarios, before filing a sev 2 ICM, check this with your TA or ADE SME
 2. Otherwise, file it as sev 3
3. You can follow up on your ICM sending an email to the [ADE PG](#) and [Azure Disk Encryption Support DLs](#)
4. In all cases work on getting approval from your TA or ADE SME prior filing an ICM. ICMs should be created to get assistance on product issues rather than normal support issues.

ADE Linux Escalation Process:

1. You can reach out to the Teams Channel [Azure Disk Encryption teams channel](#) ☑ for advise providing the case number, issue description and your question.
2. You can also contact by sending an email to the [Azure Disk Encryption Support DL](#)
3. For escalation on this feature, please [create a collaboration task with the Linux Escalation team](#) using Service Desk
 1. The Linux Escalation Engineers will be taking care of creating any needed ICM with ADE PG: [ICM to the Azure Disk Encryption team](#) ☑
 1. For **production down** scenarios, before filing a sev 2 ICM, check this with your TA or ADE SME
 2. Otherwise, file it as sev 3

Need additional help or have feedback?

<i>To engage the Azure Encryption SMEs...</i>	<i>To provide feedback on this page...</i>	<i>To provide kudos on this page...</i>
<p>Please reach out to the Azure Encryption SMEs ☐ for faster assistance.</p> <p>Make sure to use the Ava process for faster assistance.</p>	<p>Use the Azure Encryption Feedback form to submit detailed feedback on improvements or new content ideas for Azure Encryption.</p> <p>Please note the link to the page is required when submitting feedback on existing pages! If it is a new content idea, please put N/A in the Wiki Page Link.</p>	<p>Use the Azure Encryption Kudos form to submit kudos on the page. Kudos will help us improve our wiki content overall!</p> <p>Please note the link to the page is required when submitting kudos!</p>