Access Denied_Encryption

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

Tags

cw.Azure-Encryption cw.TSG

Contents

Summary

This article provides troubleshooting instructions for the scenario in which the customer receives the following error:

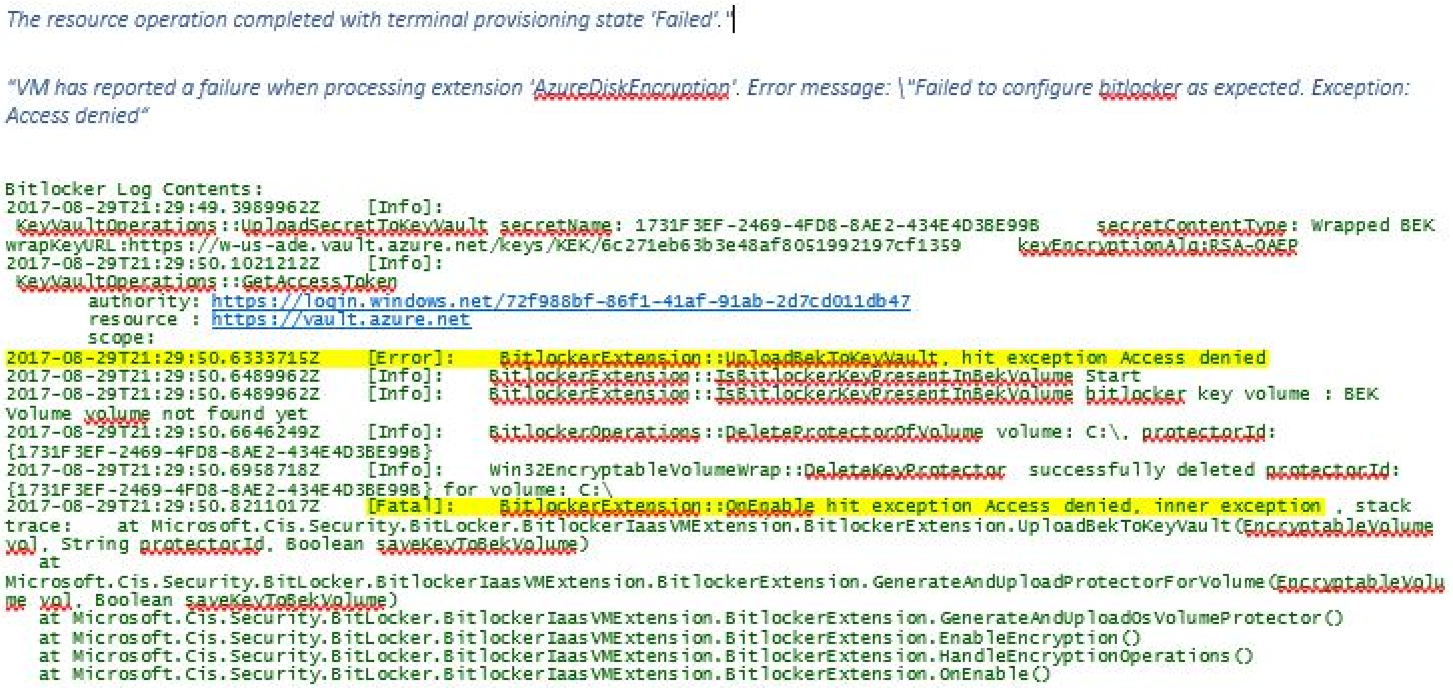
```
VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: \\"Failed to configu
```

Relevant Logs

Collect the following logs to investigate the error:

- C:\WindowsAzure\Logs\Plugins\Microsoft.Azure.Security.AzureDiskEncryption\<version>\Bitlocker.log
- MDM Tables found in ASC

The error message in **Bitlocker.log** should be as follows:



The resource operation completed with terminal provisioning state 'Failed'."

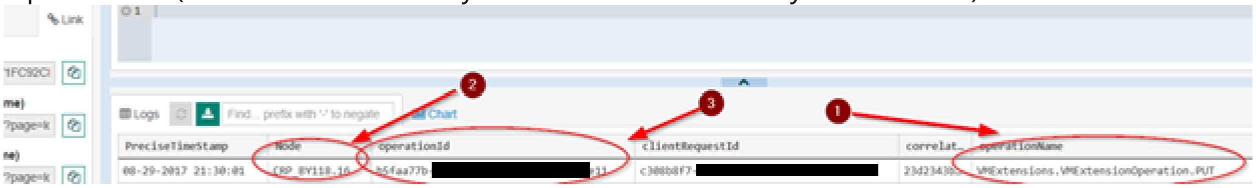
"VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: \"Failed to configure bitlocker as expected. Exception: Access denied"

```
Bitlocker Log Contents:
2017-08-29T21:29:49.3989962Z    [Info]:
 KeyVaultOperations::UploadSecretToKeyVault secretName: 1731F3EF-2469-4FD8-8AE2-434E4D3BE99B     secretContentType: Wrapped BEK
wrapKeyURL:https://w-us-ade.vault.azure.net/keys/KEK/6c271eb63b3e48af8051992197cf1359     keyEncryptionAlg:RSA-OAEP
2017-08-29T21:29:50.1021212Z    [Info]:
 KeyVaultOperations::GetAccessToken
        authority: https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47
        resource : https://vault.azure.net
        scope:
2017-08-29T21:29:50.6333715Z    [Error]:    BitlockerExtension::UploadBekToKeyVault, hit exception Access denied
2017-08-29T21:29:50.6489962Z    [Info]:    BitlockerExtension::IsBitlockerKeyPresentInBekVolume Start
2017-08-29T21:29:50.6489962Z    [Info]:    BitlockerExtension::IsBitlockerKeyPresentInBekVolume bitlocker key volume : BEK
Volume volume not found yet
2017-08-29T21:29:50.6646249Z    [Info]:    BitlockerOperations::DeleteProtectorOfVolume volume: C:\, protectorId:
{1731F3EF-2469-4FD8-8AE2-434E4D3BE99B}
2017-08-29T21:29:50.6958718Z    [Info]:    Win32EncryptableVolumeWrap::DeleteKeyProtector  successfully deleted protectorId:
{1731F3EF-2469-4FD8-8AE2-434E4D3BE99B} for volume: C:\
2017-08-29T21:29:50.8211017Z    [Fatal]:    BitlockerExtension::OnEnable hit exception Access denied, inner exception , stack
trace:    at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.UploadBekToKeyVault(EncryptableVolume
vol, String protectorId, Boolean saveKeyToBekVolume)
   at
Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadProtectorForVolume(EncryptableVolu
me vol, Boolean saveKeyToBekVolume)
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.GenerateAndUploadOsVolumeProtector()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.EnableEncryption()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.HandleEncryptionOperations()
   at Microsoft.Cis.Security.BitLocker.BitlockerIaasVMExtension.BitlockerExtension.OnEnable()
```

Troubleshooting

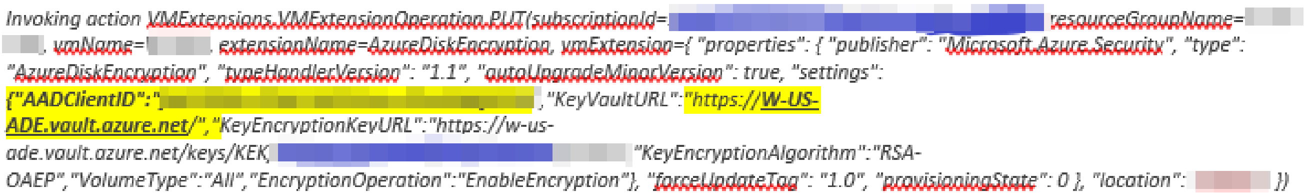
Mitigation 1

1. Identify the Vault + Client ID (Application ID) that was used in the APIOoSEvent table. (ProTip: Be sure to change the region you are looking in to match the operation)
    1. Gather the following information:
        1. Find the extension PUT operation
        2. Node Name (you have to show this column below)
        3. OperationID (this will be the activityID in the Context Activity table search)



```
PreciseTimeStamp      Node          operationId            clientRequestId      correlat...  operationName
08-29-2017 21:30:01   CRP_BY118.16  b5faa77b-[redacted]e11  c308b8f7-[redacted]  23d23430...  VMExtensions.VMExtensionOperation.PUT
```

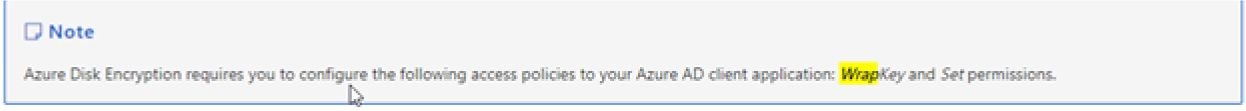
2. Identify the ClientID (ApplicationID) that was used in the SPIOoSEvent table. (ProTip: Filter on "Invoking action VMExtensions.VMExtensionOperation.PUT")



*Invoking action VMExtensions.VMExtensionOperation.PUT(subscriptionId=[redacted] resourceGroupName=[redacted], vmName=[redacted], extensionName=AzureDiskEncryption, vmExtension={ "properties": { "publisher": "Microsoft.Azure.Security", "type": "AzureDiskEncryption", "typeHandlerVersion": "1.1", "autoUpgradeMinorVersion": true, "settings": **{"AADClientID":"**[redacted],"KeyVaultURL":"https://**W-US-ADE.vault.azure.net**/","KeyEncryptionKeyURL":"https://w-us-ade.vault.azure.net/keys/KEK[redacted]"KeyEncryptionAlgorithm":"RSA-OAEP","VolumeType":"All","EncryptionOperation":"EnableEncryption"}, "forceUpdateTag": "1.0", "provisioningState": 0 }, "location": [redacted] })*

1.

3. Have customer validate and update the permissions settings on the vault.



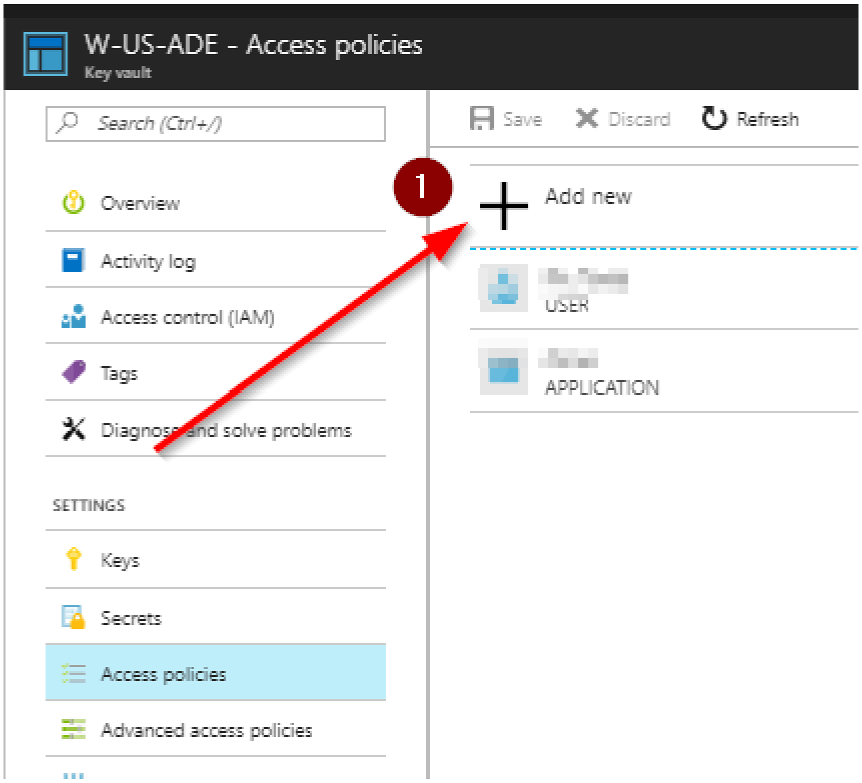
Note

Azure Disk Encryption requires you to configure the following access policies to your Azure AD client application: *WrapKey* and *Set* permissions.

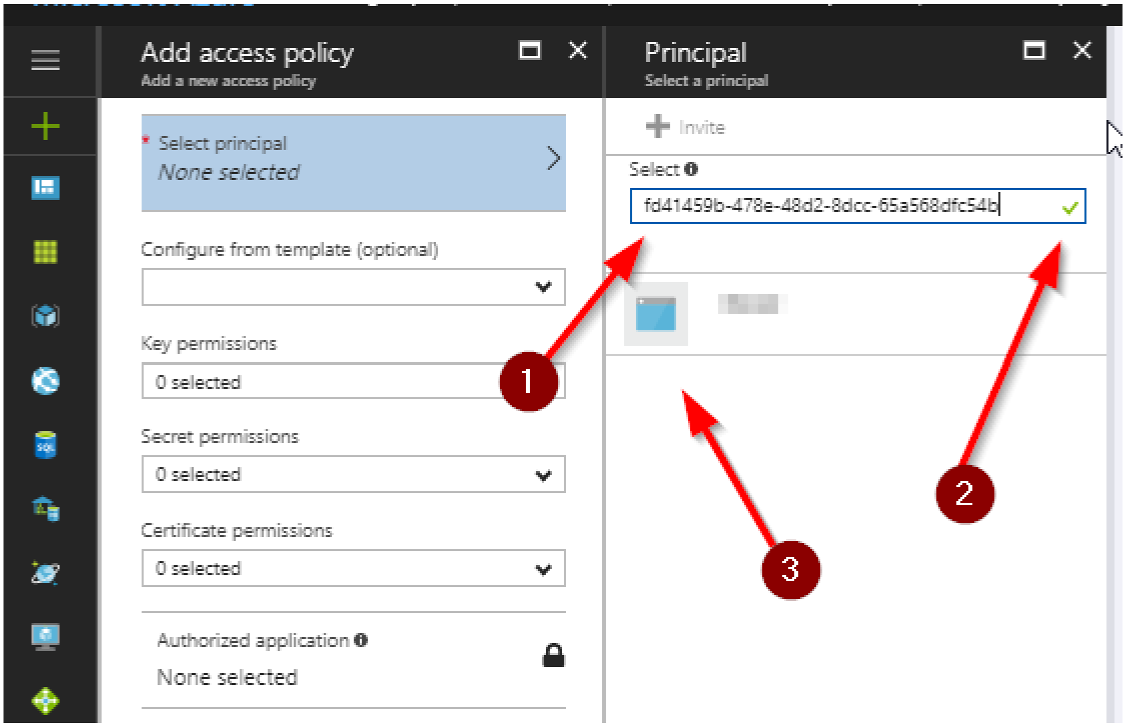
```
$keyVaultName = '\<yourKeyVaultName\>'

$aadClientID = '\<yourAadAppClientID\>'

$rgname = '\<yourResourceGroup\>'

Set-AzKeyVaultAccessPolicy -VaultName $keyVaultName -ServicePrincipalName $aadClientID -PermissionsToKeys 'W
```

Mitigation 2

Add the ApplicationID to the Key Vault:

1. 

2.



Add access policy
Add a new access policy

* Select principal
None selected

Configure from template (optional)

Key permissions
0 selected

Secret permissions
0 selected

Certificate permissions
0 selected

Authorized application
None selected

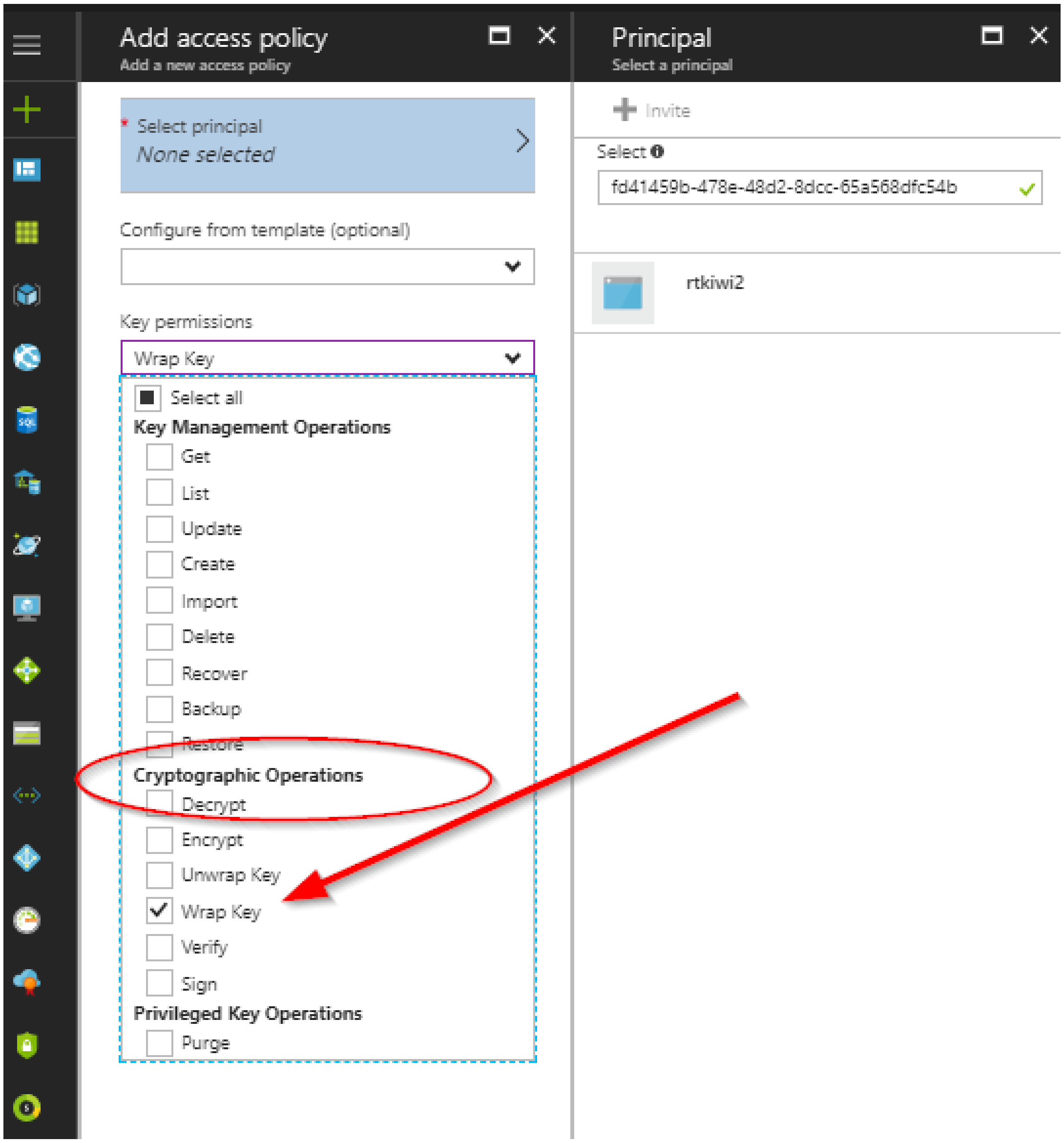
Principal
Select a principal

Invite

Select
fd41459b-478e-48d2-8dcc-65a568dfc54b

[redacted]

3.



Add access policy
Add a new access policy

* Select principal
None selected

Configure from template (optional)

Key permissions
Wrap Key

■ Select all

Key Management Operations

□ Get
□ List
□ Update
□ Create
□ Import
□ Delete
□ Recover
□ Backup
□ Restore

Cryptographic Operations

□ Decrypt
□ Encrypt
□ Unwrap Key
☑ Wrap Key
□ Verify
□ Sign

Privileged Key Operations

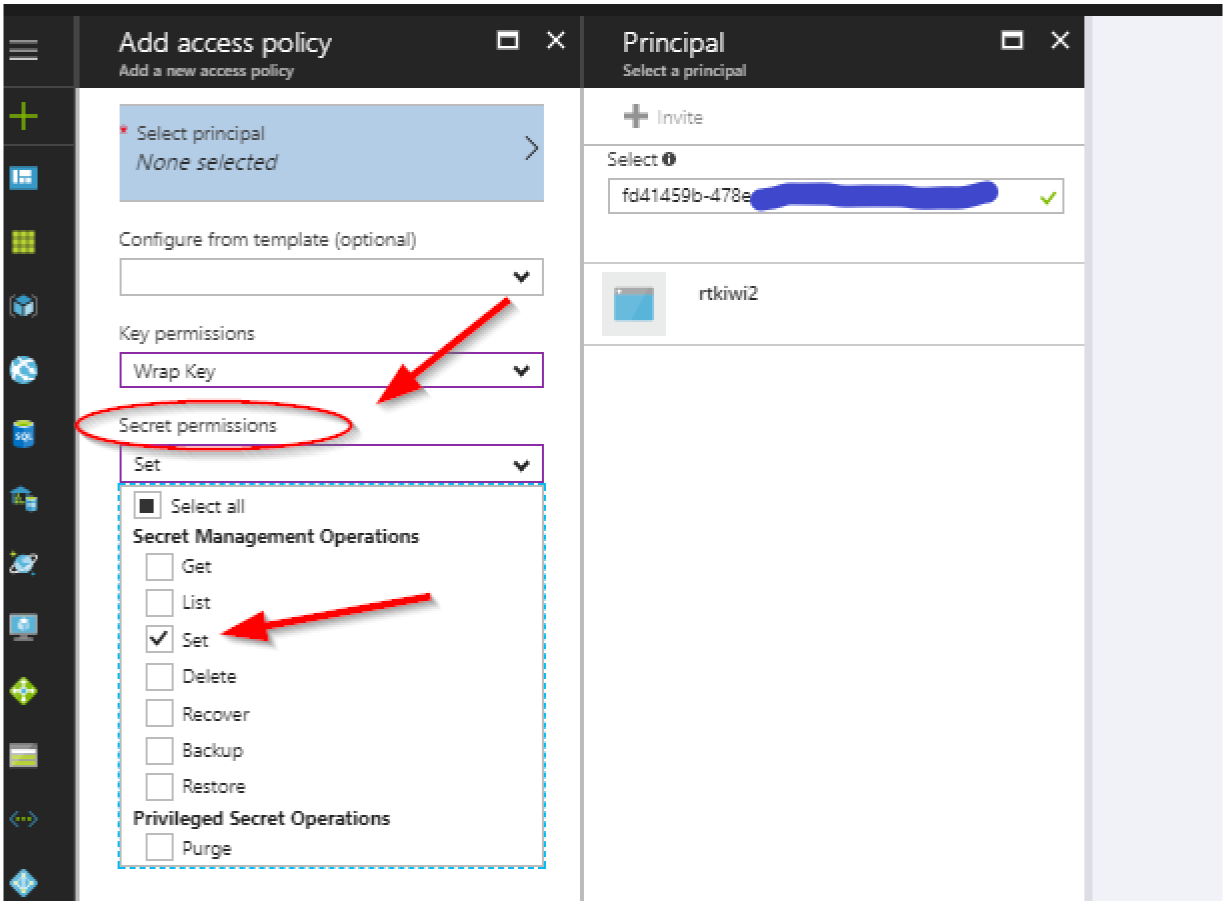
□ Purge

Principal
Select a principal

Invite

Select
fd41459b-478e-48d2-8dcc-65a568dfc54b

rtkiwi2

4. 

Add access policy
Add a new access policy

* Select principal
None selected

Configure from template (optional)

Key permissions
Wrap Key

Secret permissions
Set

■ Select all
Secret Management Operations
□ Get
□ List
☑ Set
□ Delete
□ Recover
□ Backup
□ Restore
Privileged Secret Operations
□ Purge

Principal
Select a principal

Invite

Select
fd41459b-478e[redacted] ✓

rtkiwi2

5. Don't forget to **SAVE** your changes.

Documentation

- [Set-AzKeyVaultAccessPolicy](#)
- [Azure Disk Encryption for virtual machines and virtual machine scale sets](#)

Need additional help or have feedback?

To engage the Azure Encryption SMEs...	*To provide feedback on this page...*	*To provide kudos on this page...*
Please reach out to the **Azure Encryption SMEs** for faster assistance. Make sure to use the **Ava process** for faster assistance.	Use the **Azure Encryption Feedback** form to submit detailed feedback on improvements or new content ideas for Azure Encryption. ***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.	Use the **Azure Encryption Kudos** form to submit kudos on the page. Kudos will help us improve our wiki content overall! ***Please note*** the link to the page is required when submitting kudos!