

Failed to Configure Bitlocker as Expected Exception AADSTS_Encryption

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

Tags

[cw.Azure-Encryption](#)[cw.TSG](#)

Contents

- [Summary](#)
 - [Input and Output Example](#)
- [Cause](#)
- [Mitigation](#)
- [Related Content](#)
- [Need additional help or have feedback?](#)

Summary

This article provides troubleshooting steps for the scenario in which **Windows** virtual machine (VM) encryption fails with the following error:

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

Input and Output Example

This is an example of the PowerShell command customers can use to encrypt their Windows VM:

```
PS C:\WINDOWS\system32>>>> Set-AzVMDiskEncryptionExtension -ResourceGroupName "RGNAME" -VMName "VMNAME"  
-AadClientID $ADEApp.ApplicationId  
-AadClientSecret $aadClientSecret  
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl  
-DiskEncryptionKeyVaultId $keyVaultResourceId  
-KeyEncryptionKeyUrl $keyEncryptionKeyUrl  
-KeyEncryptionKeyVaultId $keyVaultResourceId
```

This is an example of the Bitlocker debug information for the failed operation:

```

Set-AzureRmVMDiskEncryptionExtension : Long running operation failed with status 'Failed'. Additional Info:'VM has reported
a failure when processing extension 'AzureDiskEncryption'. Error message: "Failed to configure bitlocker as expected.
Exception: AADSTS70002: Error validating credentials. AADSTS50012: Invalid client secret is provided.
Trace ID: d6e70ca6-694b-450c-9df7-fc61f57daf00
Correlation ID: abdabe31-02be-45b1-b4cc-21ca9962d97c
Timestamp: 2018-06-25 15:18:07Z, InnerException: System.Net.WebException: The remote server returned an error: (401)
Unauthorized.
    at System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)
    at System.Threading.Tasks.TaskFactory`1.FromAsyncCoreLogic(IAsyncResult iar, Func`2 endFunction, Action`1 endAction,
Task`1 promise, Boolean requiresSynchronization)
--- End of stack trace from previous location where exception was thrown ---
    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
    at Microsoft.IdentityModel.Clients.ActiveDirectory.HttpWebRequestWrapper.<GetResponseSyncOrAsync>d__2.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
    at Microsoft.IdentityModel.Clients.ActiveDirectory.HttpHelper.<SendPostRequestAndDeserializeJsonResponseAsync>d__0`1.MoveN
ext(), stack trace:
    at Microsoft.Cis.Security.BitLocker.BitlockerIaaSVMExtension.BitlockerExtension.UploadBekToKeyvault(EncryptableVolume vol,
String protectorId, Boolean saveKeyToBekVolume)
    at Microsoft.Cis.Security.BitLocker.BitlockerIaaSVMExtension.BitlockerExtension.GenerateAndUploadProtectorForVolume(Encrypt
ableVolume 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()".
Error Code: VMExtensionProvisioningError
ErrorMessage: VM has reported a failure when processing extension 'AzureDiskEncryption'. Error message: "Failed to configure
bitlocker as expected. Exception: AADSTS70002: Error validating credentials. AADSTS50012: Invalid client secret is provided.
Trace ID: d6e70ca6-694b-450c-9df7-fc61f57daf00
Correlation ID: abdabe31-02be-45b1-b4cc-21ca9962d97c
Timestamp: 2018-06-25 15:18:07Z, InnerException: System.Net.WebException: The remote server returned an error: (401)
Unauthorized.
    at System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)
    at System.Threading.Tasks.TaskFactory`1.FromAsyncCoreLogic(IAsyncResult iar, Func`2 endFunction, Action`1 endAction,
Task`1 promise, Boolean requiresSynchronization)
--- End of stack trace from previous location where exception was thrown ---
    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
    at Microsoft.IdentityModel.Clients.ActiveDirectory.HttpWebRequestWrapper.<GetResponseSyncOrAsync>d__2.MoveNext()
--- End of stack trace from previous location where exception was thrown ---
    at System.Runtime.ExceptionServices.ExceptionDispatchInfo.Throw()
    at System.Runtime.CompilerServices.TaskAwaiter.HandleNonSuccessAndDebuggerNotification(Task task)
    at Microsoft.IdentityModel.Clients.ActiveDirectory.HttpHelper.<SendPostRequestAndDeserializeJsonResponseAsync>d__0`1.MoveN
ext(), stack trace:
    at Microsoft.Cis.Security.BitLocker.BitlockerIaaSVMExtension.BitlockerExtension.UploadBekToKeyvault(EncryptableVolume vol,
String protectorId, Boolean saveKeyToBekVolume)
    at Microsoft.Cis.Security.BitLocker.BitlockerIaaSVMExtension.BitlockerExtension.GenerateAndUploadProtectorForVolume(Encrypt
ableVolume 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()".
StartTime: 6/25/2018 11:15:16 AM
EndTime: 6/25/2018 11:18:20 AM
OperationID: 086d88dc-ca16-468b-a926-9481c4e1a955
Status: Failed
At line:7 char:1
+ Set-AzureRmVMDiskEncryptionExtension -ResourceGroupName "Classic-win2 ...
+ ~~~~~
+ CategoryInfo          : (CloseError: (:)) [Set-AzureRmVMDiskEncryptionExtension], ComputeCloudException
+ FullyQualifiedErrorId : Microsoft.Azure.Commands.Compute.Extension.AzureDiskEncryption.SetAzureDiskEncryptionExtension
Command

```

Cause

1. Incorrect Azure Active Directory (AAD) App Credential (**AadClientSecret**).
2. Expired AAD App Credential (**AadClientSecret**) - By default, AAD App Credentials have a lifetime of 1 year when created.

Mitigation

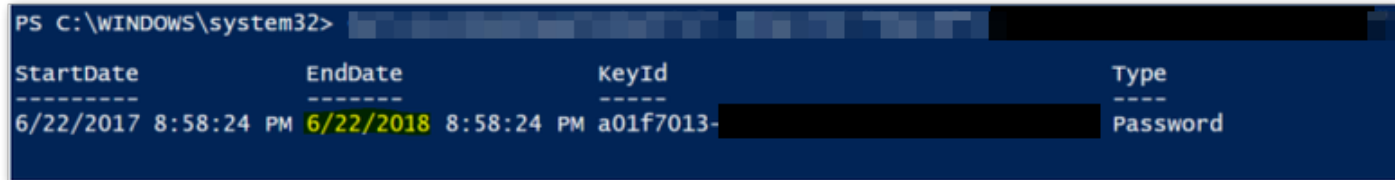
1. Confirm that the customer has entered the correct **AadClientSecret** string in the password variable.

```
PS C:\WINDOWS\system32>>>> $aadClientSecret = '<PASSWORD>'
```

- Once the AadClientSecret has been verified to be the correct one, check to see if the credentials have expired by running the commands below:

```
$ADEApp = Get-AzADApplication -DisplayName "***Name Of ADE App Created**"
Get-AzADAppCredential -ObjectId $ADEApp.ObjectId
```

- Example Output



StartDate	EndDate	KeyId	Type
6/22/2017 8:58:24 PM	6/22/2018 8:58:24 PM	a01f7013- [REDACTED]	Password

- If the EndDate shows a past date, the credentials for the AAD App have expired and new ones will need to be created.
- Create new credentials for the application with the commands below (**Note:** Replace the string value with whatever value the customer desires and be sure to save that value!)




```
$newPassword = ConvertTo-SecureString -String "P@ssword1\!" -AsPlainText -Force
New-AzADAppCredential -ObjectId $ADEApp.ObjectId -Password $newPassword
```

- Attempt to encrypt the VM once again by running the Set-AzVMDiskEncryptionExtension command with the AadClientSecret switch containing the \$newPassword variable which has the string that was used to create the new AAD App Credentials.


```
PS C:\WINDOWS\system32>>>> Set-AzVMDiskEncryptionExtension -ResourceGroupName "RGNAME" -VMName "VMNAME"
-AadClientID $ADEApp.ApplicationId
-AadClientSecret (New-Object PSObject ("user",$newPassword).GetNetworkCredential()).Password
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl
-DiskEncryptionKeyVaultId $keyVaultResourceId
-KeyEncryptionKeyUrl $keyEncryptionKeyUrl
-KeyEncryptionKeyVaultId $keyVaultResourceId

RequestId IsSuccessStatusCode StatusCode ReasonPhrase
-----
True OK OK
```

Related Content

- [Azure Disk Encryption for Windows VMs](#) 
- [Explore and manage your resources with asset inventory](#) 
- [New-AzADAppCredential](#) 

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>