Windows PowerShell Get-Help on Cmdlet 'Get-CmsMessage'

PS:\>Get-HELP Get-CmsMessage -Full

NAME

Get-CmsMessage

SYNOPSIS

Gets content that has been encrypted by using the Cryptographic Message Syntax format.

SYNTAX

Get-CmsMessage [-Content] <System.String> [<CommonParameters>]

Get-CmsMessage [-LiteralPath] <System.String> [<CommonParameters>]

Get-CmsMessage [-Path] <System.String> [<CommonParameters>]

DESCRIPTION

The `Get-CmsMessage` cmdlet gets content that has been encrypted using the Cryptographic Message Syntax (CMS) format.

The CMS cmdlets support encryption and decryption of content using the IETF format for cryptographically protecting

messages, as documented by RFC5652
(https://tools.ietf.org/html/rfc5652).

The CMS encryption standard uses public key cryptography, where the keys used to encrypt content (the public key) and the keys used to decrypt content (the private
key) are separate. Your public key can be shared widely, and is not sensitive data. If any content is encrypted with this public key, only your private key can
decrypt it. For more information, see Public-key cryptography (https://en.wikipedia.org/wiki/Public-key_cryptography).

`Get-CmsMessage` gets content that has been encrypted in CMS format. It does not decrypt or unprotect content. You can run this cmdlet to get content that you have
encrypted by running the `Protect-CmsMessage` cmdlet. You can specify content that you want to decrypt as a string, or by path to the encrypted content. You can pipe
the results of `Get-CmsMessage` to `Unprotect-CmsMessage` to decrypt the content, provided that you have information about the document encryption certificate that
was used to encrypt the content.

PARAMETERS

-Content <System.String>

Specifies an encrypted string, or a variable containing an encrypted string.

Required? true
Position? 0
Default value None
Accept pipeline input? True (ByValue)
Accept wildcard characters? false

-LiteralPath <System.String>

Specifies the path to encrypted content that you want to get. Unlike Path , the value of LiteralPath is used exactly as it is typed. No characters are interpreted
as wildcard characters. If the path includes escape characters, enclose each one in single quotation marks. Single quotation marks tell PowerShell not to

interpret enclosed characters as escape characters.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Path <System.String>

Specifies the path to encrypted content that you want to decrypt.

Required? true

Position? 1

Default value None

Accept pipeline input? False

Accept wildcard characters? false

<CommonParameters>

This cmdlet supports the common parameters: Verbose, Debug,

ErrorAction, ErrorVariable, WarningAction, WarningVariable,

OutBuffer, PipelineVariable, and OutVariable. For more information, see

about_CommonParameters (https:/go.microsoft.com/fwlink/?LinkID=113216).

INPUTS

OUTPUTS

NOTES

---------- Example 1: Get encrypted content ----------

```
$Msg = Get-CmsMessage -Path "C:\Users\Test\Documents\PowerShell\Future_Plans.txt"
$Msg.Content

-----BEGIN CMS-----
MIIBqAYJKoZIhvcNAQcDoIIBmTCCAZUCAQAxggFQMIIBTAIBADA0MCAxHjAcBgNVBAMBFWxlZWhv
bG1AbGljcm9zb2Z0LmNvbQIQQYHsbcXnjIJCtH+OhGmc1DANBgkqhkiG9w0BAQcwAASCAQAnkFHM
proJnFy4geFGfyNmxH3yeoPvwEYzdnsoVqqDPAd8D3wao77z7OhJEXwz9GeFLnxD6djKV/tF4PxR
E27aduKSLbnxfpf/sepZ4fUkuGibnwWFrxGE3B1G26MCenHWjYQiqv+Nq32Gc97qEAERrhLv6S4R
G+2dJEnesW8A+z9QPo+DwYP5FzD0Td0ExrkswVckpLNR6j17Yaags3ltNXmbdEXekhi6Psf2MLMP
TSO79lv2L0KeXFGuPOrdzPRwCkV0vNEqTEBeDnZGrjv/5766bM3GW34FXApod9u+VSFpBnqVOCBA
DVDraA6k+xwBt66cV84AHLkh0kT02SIHMDwGCSqGSIb3DQEHATAdBglghkgBZQMEASoEEJbJaiRl
KMnBoD1dkb/FzSWAEBaL8xkFwCu0e1AtDj7nSJc=
-----END CMS-----
```

This command gets encrypted content located at C:\Users\Test\Documents\PowerShell\Future_Plans.txt.

-- Example 2: Pipe encrypted content to Unprotect-CmsMessage --

```
$Msg = Get-CmsMessage -Path "C:\Users\Test\Documents\PowerShell\Future_Plans.txt"
$Msg | Unprotect-CmsMessage -To "cn=youralias@emailaddress.com"
```

Try the new Break All command

This command pipes the results of the `Get-CmsMessage` cmdlet from Example 1 to `Unprotect-CmsMessage`, to decrypt the message and read it in plain text. In this case, the value of the To parameter is the value of the encrypting certificate's Subject line. The decrypted message, "Try the new Break All command," is the result.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/microsoft.powershell.security/get-cmsmessage?view=powershell-5.1&WT.mc_id=ps-gethelp

about_Providers

Protect-CmsMessage

Unprotect-CmsMessage