Windows PowerShell Get-Help on Cmdlet 'New-NetIPsecMainModeCryptoProposal'

PS:\>Get-HELP New-NetIPsecMainModeCryptoProposal -Full

NAME

New-NetIPsecMainModeCryptoProposal

SYNOPSIS

Creates a main mode cryptographic proposal that specifies a suite of cryptographic protocols to offer in IPsec main mode negotiations with other computers.

SYNTAX

New-NetIPsecMainModeCryptoProposal [-Encryption {None | DES | DES3 | AES128 | AES192 | AES256 | AESGCM128 | AESGCM192 | AESGCM256}] [-Hash {None | MD5 | SHA1 | SHA256

| SHA384 | AESGMAC128 | AESGMAC192 | AESGMAC256}] [-KeyExchange {None | DH1 | DH2 | DH14 | DH19 | DH20 | DH24 | SameAsMainMode}] [<CommonParameters>]

DESCRIPTION

The New-NetIPsecMainModeCryptoProposal cmdlet creates a single cryptographic proposal to be used in main mode negotiations.

A NetIPsecMainModeCryptoProposal object provides three of the mandatory four parameters for the negotiation of a

main mode security association (SA): The encryption

algorithm is provided in the Encryption parameter, the hashing algorithm in the Hash parameter, and the Diffie-Hellman (DH) key exchange group to be used for the base

keying material in the KeyExchange parameter. The remaining parameter; the authentication method, such as Kerberos v5, certificate, or pre-shared key authentication,

is given through NetIPsecPhase1AuthSet and NetIPsecPhase2AuthSet objects.

Multiple NetIPsecMainModeCryptoProposal fields are grouped into a single NetIPsecMainModeCryptoSet object. The main mode exchange will use the first proposal that the

responder has in common with the sender. A NetIPsecPhase1AuthSet object and a NetIPsecMainModeCryptoSet object get associated to a NetIPsecMainModeRule object to

provide all the necessary SA parameters for customized main mode negotiations.

PARAMETERS

-Encryption <EncryptionAlgorithm>

Specifies the encryption algorithm to use for IPsec main mode security association negotiations. The block size of the encryption and hashing algorithms must be

the same. The acceptable values for this parameter are: None, DES, DES3, AES128, AES192, AES256, AESGCM128, AESGCM192, or AESGCM256. None implies Null Encryption

per the RFC standard. The default value is AES256. Neither GCM, for encryption, nor GMAC, for hashing, are supported in main mode. These are quick mode only.

Required?	false
Position?	named
Default value	None
Accept pipeline input?	False
Accept wildcard characters?	false

-Hash <HashAlgorithm>

Specifies the hashing function to use for IPsec main mode security association negotiations. The block size of the encryption and hashing algorithms should be the

same. The acceptable values for this parameter are: None, MD5, SHA1, SHA256, SHA384, AESGMAC128,

AESGMAC192, or AESGMAC256. The default value is SHA384.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-KeyExchange <DiffieHellmanGroup>

Specifies the Diffie-Hellman group to use for IPsec main mode security association negotiations. The acceptable values for this parameter are: None, DH1, DH2,

DH14, DH19, DH20, or DH24. The default value is None. SameAsMainMode is only valid for proposals added to quick mode cryptographic sets with

PerfectForwardSecrecyGroup (PFS) specified using SameAsMainMode.

Required? false

Position? named

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

None

OUTPUTS

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetIPsecMainModeCryptoProposal

The `Microsoft.Management.Infrastructure.CimInstance` object is a wrapper class that displays Windows Management Instrumentation (WMI) objects. The path after the

pound sign (`#`) provides the namespace and class name for the underlying WMI object.

NOTES

---------- EXAMPLE 1 ----------

PS C:\>$proposal1 = (New-NetIPsecMainModeCryptoProposal -Encryption DES3 -Hash MD5 -KeyExchange DH1)

PS C:\>$proposal2 = (New-NetIPsecMainModeCryptoProposal -Encryption AES192 -Hash MD5 -KeyExchange DH14)

PS C:\>$proposal3 = (New-NetIPsecMainModeCryptoProposal -Encryption DES3 -Hash MD5 -KeyExchange DH19)

PS C:\>$mMCryptoSet= (New-NetIPsecMainModeCryptoSet -DisplayName "Main Mode Crypto Set" -Proposal $proposal1,$proposal2,$proposal3)

This cmdlet shows an alternative method of accomplishing the previous steps.

PS C:\>$mMCryptoSet = New-NetIPsecMainModeCryptoSet -DisplayName "Main Mode Crypto Set" -Proposal (New-NetIPsecMainModeCryptoProposal -Encryption DES3 -Hash MD5

-KeyExchange DH1),(New-NetIPsecMainModeCryptoProposal -Encryption AES192 -Hash MD5 -KeyExchange

DH14),(New-NetIPsecMainModeCryptoProposal -Encryption DES3 -Hash MD5

-KeyExchange DH19)

PS C:\>New-NetIPsecMainModeRule -DisplayName "Main Mode Rule" -MainModeCryptoSet $mMCryptoSet.Name

This example creates a main mode rule linked to a cryptographic set that contains three cryptographic proposals.

RELATED LINKS

Online Version:

https://learn.microsoft.com/powershell/module/netsecurity/new-netipsecmainmodecryptoproposal?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

New-NetIPsecMainModeRule

New-NetIPsecMainModeCryptoSet