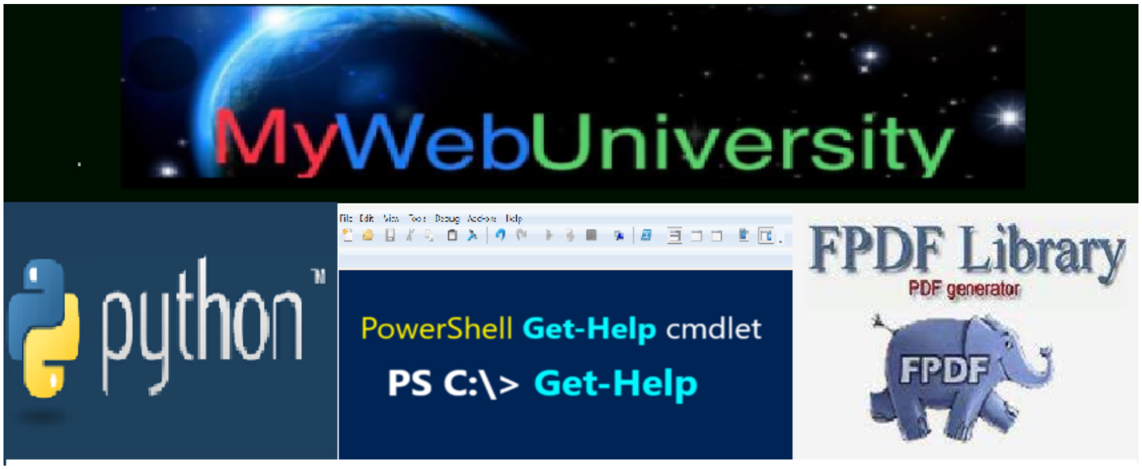

Full credit is given to all the above companies including the Operating System that this PDF file was generated!

Windows PowerShell Get-Help on Cmdlet 'Remove-NetIPsecMainModeSA'

PS:\>Get-HELP Remove-NetIPsecMainModeSA -Full

NAME

Remove-NetIPsecMainModeSA

SYNOPSIS

Removes an active main mode security association (SA).

SYNTAX

Remove-NetIPsecMainModeSA [-All] [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

Remove-NetIPsecMainModeSA [-AsJob] -AssociatedNetIPsecQuickModeSA <CimInstance> [-CimSession <CimSession[]>] [-Confirm] [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

Remove-NetIPsecMainModeSA [-AsJob] [-CimSession <CimSession[]>] [-Confirm] -InputObject <CimInstance[]> [-PassThru] [-ThrottleLimit <Int32>] [-WhatIf]

[<CommonParameters>]

Remove-NetIPsecMainModeSA [-Name] <String[]> [-AsJob] [-CimSession <CimSession[]>] [-Confirm] [-PassThru]

[-ThrottleLimit <Int32>] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The Remove-NetIPsecMainModeSA cmdlet deletes an established main mode security association (SA).

The main mode SAs can be monitored for information including which peers are currently connected to this computer and which protection suite was used to create the

SA. To view the active main mode SAs with the computer, run the Get-NetIPsecMainModeSA cmdlet. Use the InputObject parameter, or the pipeline, to input the SA into

this cmdlet to remove the association from the computer.

PARAMETERS

-All [<SwitchParameter>]

Indicates that all of the main mode security associations within the specified policy store are removed.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-AsJob [<SwitchParameter>]

Runs the cmdlet as a background job. Use this parameter to run commands that take a long time to complete.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-AssociatedNetIPsecQuickModeSA <CimInstance>

Gets the quick mode security associations associated with the given main mode security association.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-CimSession <CimSession[]>

Runs the cmdlet in a remote session or on a remote computer. Enter a computer name or a session object, such as the output of a New-CimSession (https://go.microsoft.com/fwlink/p/?LinkId=227967) or [Get-CimSession](https://go.microsoft.com/fwlink/p/?LinkId=227966)cmdlet. The default is the current session on the local computer.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Confirm [<SwitchParameter>]

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-InputObject <CimInstance[]>

Specifies the input object that is used in a pipeline command.

Required?   true

Position?   named

Default value   None

Accept pipeline input?   True (ByValue)

Accept wildcard characters? false

-Name <String[]>

Specifies that only matching main mode rules of the indicated name are removed. Wildcard characters are accepted. This parameter acts just like a file name, in

that only one rule with a given name may exist in a policy store at a time. During group policy processing and policy merge, rules that have the same name but

come from multiple stores being merged, will overwrite one another so that only one exists. This overwriting behavior is desirable if the rules serve the same

purpose. For instance, all of the firewall rules have specific names, so if an administrator can copy these rules to a GPO, and the rules will override the local

versions on a local computer. Since GPOs can have precedence, if an administrator that gives a rule with a different or more specific rule the same name in a

higher-precedence GPO, then it overrides other rules that exist. The default value is a randomly assigned value. When the defaults for main mode encryption are

overridden, specify the customized parameters and set this parameter value, making this parameter the new default setting for encryption.

Required?   true

Position?   0

Default value   None

Accept pipeline input?   False

Accept wildcard characters? false

-PassThru [<SwitchParameter>]

Returns an object representing the item with which you are working. By default, this cmdlet does not generate any output.

Required?   false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ThrottleLimit <Int32>

Specifies the maximum number of concurrent operations that can be established to run the cmdlet. If this parameter is omitted or a value of `0` is entered, then

Windows PowerShellr calculates an optimum throttle limit for the cmdlet based on the number of CIM cmdlets that are running on the computer. The throttle limit

applies only to the current cmdlet, not to the session or to the computer.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf [<SwitchParameter>]

Shows what would happen if the cmdlet runs. The cmdlet is not run.

Required? false

Position? named

Default value False

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

Microsoft.Management.Infrastructure.CimInstance#root\StandardCimv2\NetIPsecMainModeSA[]

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.

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

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.

OUTPUTS

None

NOTES

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

```
PS C:\>Remove-NetIPsecMainModeSA -PolicyStore ActiveStore
```

This example removes all of the active main mode cryptographic sets on the local computer.

-------------------------- EXAMPLE 2 --------------------------

```
PS C:\>$computer1 = "RemoteMachineName"
PS C:\>$ipsQMSA = Get-NetIPsecQuickModeSA -Name "3456" -CimSession $computer1
```

```
PS C:\>Remove-NetIPsecMainModeSA -CimSession $computer1 -InputObject $ipsQMSA
```

This example removes a specified main mode security association on a remote computer.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/netsecurity/remove-netipsecmainmodesa?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Get-NetIPsecMainModeSA