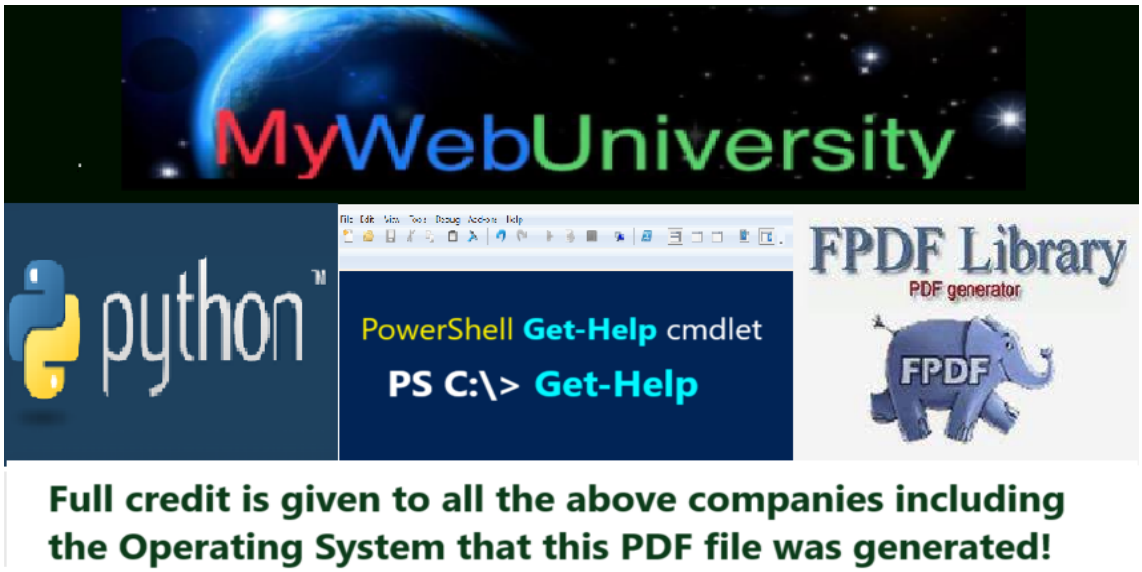

Windows PowerShell Get-Help on Cmdlet 'New-NetIPsecAuthProposal'

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

NAME

New-NetIPsecAuthProposal

SYNOPSIS

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

SYNTAX

New-NetIPsecAuthProposal [-Machine] [-Cert] [[-Health]] [-AccountMapping] -Authority <String> [-AuthorityType {Invalid | Root | Intermediate}] [-ExcludeCAName]

[-ExtendedKeyUsage <String[]>] [-FollowRenewal] [-SelectionCriteria] [-Signing {Invalid | RSA | ECDSA256 | ECDSA384}] [-SubjectName <String>] [-SubjectNameType {None

| DomainName | UserPrincipalName | EmailAddress | CN | OU | O | DC}] [-Thumbprint <String>] [-ValidationCriteria] [<CommonParameters>]

New-NetIPsecAuthProposal [-User] [-Cert] [-AccountMapping] -Authority <String> [-AuthorityType {Invalid | Root | Intermediate}] [-ExcludeCAName] [-ExtendedKeyUsage

<String[]>] [-FollowRenewal] [-SelectionCriteria] [-Signing {Invalid | RSA | ECDSA256 | ECDSA384}] [-SubjectName <String>] [-SubjectNameType {None | DomainName |

UserPrincipalName | EmailAddress | CN | OU | O | DC}] [-Thumbprint <String>] [-ValidationCriteria] [<CommonParameters>]

New-NetIPsecAuthProposal [-Anonymous] [<CommonParameters>]

New-NetIPsecAuthProposal [-Machine] [-Kerberos] [-Proxy <String>] [<CommonParameters>]

New-NetIPsecAuthProposal [-User] [-Kerberos] [-Proxy <String>] [<CommonParameters>]

New-NetIPsecAuthProposal [-Machine] [-Ntlm] [<CommonParameters>]

New-NetIPsecAuthProposal [-Machine] [-PreSharedKey] <String> [<CommonParameters>]

New-NetIPsecAuthProposal [-User] [-Ntlm] [<CommonParameters>]

DESCRIPTION

The New-NetIPsecAuthProposal cmdlet creates a single authentication proposal to be used in IPsec main mode negotiations. An authentication proposal describes a single

authentication method that the computer would accept as valid proof of the identity of the peer. This cmdlet is also used to authenticate the identity of the local

user, so that a peer computer would accept the proof.

Multiple network IPsec authentication proposal fields are grouped into a single network IPsec phase 1 authentication set or network IPsec phase 2 authentication set.

Each set is a list of proposals in order of preference. A phase 1 authentication is generally used for computer authentication, and a phase 2 authentication is used

for user authentication or computer health certification. See the New-NetIPsecPhase1AuthSet and New-NetIPsecPhase2AuthSet cmdlets for more information. The

authentication method, such as Kerberos v5, Certificate, or pre-shared key authentication, is provided by a network IPsec authentication proposal, specified through a

network IPsec phase 1 authentication set, is required for a successful main mode security association. See the Get-NetIPsecMainModeSA and Get-NetIPsecQuickModeSA

cmdlets for more information.

PARAMETERS

-AccountMapping [<SwitchParameter>]

Specifies the enabled state for the IPsec certificate-to-account mapping. In certificate-to-account mapping, the Internet Key Exchange (IKE) and AuthIP protocols

associate, or map, a user or computer certificate to a user or computer account in an Active Directory (AD) domain or forest, and then retrieves an access token,

which includes the list of user security groups. This process ensures that the certificate offered by the IPsec peer corresponds to an active user or computer

account in the domain, and that the certificate is one that should be used by that user or computer.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Anonymous [<SwitchParameter>]

Specifies anonymous authentication. Anonymous authentication means no authentication is performed. This method does not require identity to authenticate. It is

equal to no authentication. This provides end-to-end security between hosts, but does not provide any authentication or authorization for which users and

computers can connect. This method can be used for both phase 1 and phase 2 authentication.

Required? true

Position? 1

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Authority <String>

Specifies, for certificate authentication, the strong name, or X.509 string, of the Certification Authority (CA) that has issued the client certificates. This

parameter is used for certificate authentication.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-AuthorityType <CertificateAuthorityType>

Specifies that certificates issued by intermediate CAs should be accepted. This parameter is used for certificate authentication. The acceptable values for this

parameter are:: Root or Intermediate. The default value is Root. This parameter is supported in Windows Serverr 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Cert [<SwitchParameter>]

Specifies that certificate authentication is used. The Authority and AuthorityType parameters specify the certification authentication methods.

Required? true

Position? 2

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ExcludeCAName [<SwitchParameter>]

Specifies that CA names are excluded. This can only be specified for phase 1 authentications.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ExtendedKeyUsage <String[]>

Specifies list of object identifiers (OIDs) that would be used on the extended key usage (EKU) field of a certificate. When a CA issues a certificate, then the

EKU specifies the intended purposes of the certificate. For instance, there are specific OIDs for client-server communications as well as secure email and code

signing. An IPsec certificate can be selected or validated by EKU OID. There is a limit of `100` EKUs. This parameter is supported in Windows Server 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-FollowRenewal [<SwitchParameter>]

Specifies that certificate signing is automatically renewed. When the certificate is auto-renewed, the IPsec policy will not need to be updated. This parameter

only works for authentication methods that define a thumb print with the Thumbprint parameter. This parameter only works, and is appropriate, for certificate

selection methods. The default value is False. This parameter is supported in Windows Server 2012.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Health [<SwitchParameter>]

Specifies that the certificate is a health certificate. For phase 2 authentications, if the authentication method is only valid for computer certificates.

Required? false

Position? 2

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Kerberos [<SwitchParameter>]

Specifies that Kerberos is used. This method authenticates the identity of user or computer accounts by using Kerberos Protocol Extensions

(https://msdn.microsoft.com/library/cc233855.aspx).

Required? true

Position? 2

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Machine [<SwitchParameter>]

Specifies that the computer principal should be authenticated rather than the user.

Required? true

Position? 1

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Ntlm [<SwitchParameter>]

Specifies that NTLM authentication is used.

Required? true

Position? 2

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-PreSharedKey <String>

Specifies that the given pre-shared key is used for authentication. The use of a pre-shared key is strongly discouraged, and is provided for interoperability and

for conformance to IPsec standards. The pre-shared key is stored in plain text. The use of a more secure authentication method is strongly recommended.

Required? true

Position? 2

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Proxy <String>

Specifies the fully qualified domain name (FQDN) of the Kerberos proxy to use when authenticating from a remote network. This parameter is supported in Windows

Server 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SelectionCriteria [<SwitchParameter>]

Specifies that the current certificate authentication proposal should be used to select the certificate as opposed to

remote peers. When using certificate

criteria, exactly one proposal for selection and exactly one proposal for validation are needed. A single proposal can be used for both. If this parameter or the

ValidationCriteria parameter is not specified, then the proposal is used for both. This parameter is supported in Windows Server 2012. The default value is

False. If both this parameter and the ValidationCriteria parameter are set to False, then the configuration is not valid and both flags in a new phase 1

authentication set or phase 2 authentication are set to True.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Signing <CertificateSigningAlgorithm>

Specifies the certificate signing algorithm to accept. The acceptable values for this parameter are: RSA, ECDSA256, or ECDSA384. The default value is RSA.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubjectName <String>

Determines, if it is not null, how the certificate should be validated. A certification authority (CA) could put any string value into the Subject Name or

Alternative Subject Name fields on a certificate, so there are no format requirements for this parameter. However, depending on the value of SubjectNameType,

there are some general formats that are usually followed. Examine the certificates issued by the CA to find the exact formatting to use. If the SubjectNameType

parameter is: - None: The Subject Name field on a certificate must be null.

- DomainName: The Subject Name field on a certificate should generally take the format of a FQDN.

The Alternative Subject Name field will be examined. - UserPrincipalName: The Subject Name field on a certificate should generally take the format of an service

principal name (SPN). The Alternative Subject Name field will be examined. - EmailAddress: An email address, like `username@contoso.com`. The Alternative Subject

Name field on a certificate will be examined. - CN, OU, O, DC: The values from an X.509 strong name. These will be parsed from the Subject Name field on a

certificate. This parameter is supported in Windows Server 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-SubjectNameType <CertificateSubjectType>

Determines how the SubjectName field should be interpreted. The acceptable values for this parameter are: None, DomainName, UserPrincipalName, EmailAddress, CN,

OU, O, or DC. This parameter is supported in Windows Server 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Thumbprint <String>

Specifies the thumbprint hashing to use for certification criteria. This is primarily intended for interoperability server-to-server authentication. This

parameter cannot be combined with the FollowRenewal parameter. This parameter is supported in Windows Server 2012.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-User [<SwitchParameter>]

Specifies that the computer should authenticate as the user account, rather than the computer. This parameter is valid with NTLM, Kerberos, Cert, or Proxy.

Required? true

Position? 1

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-ValidationCriteria [<SwitchParameter>]

For use with certificate criteria. Specifies that the current certificate auth proposal should be used to validate the certificate given by the remote peer. When

using certificate criteria, exactly one proposal for selection and exactly one proposal for validation are needed. A single proposal can be used for both. If this

parameter or the SelectionCriteria parameter is not specified, then the proposal is used for both. This parameter is supported in Windows Server 2012. The

default value is False. If both this parameter and the SelectionCriteria parameter are set to False, then the configuration is not valid and both flags in a new

phase 1 authentication set or phase 2 authentication are set to True.

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

None

OUTPUTS

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

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:\>$cert1Proposal = New-NetIPsecAuthProposal -Machine -Cert -Authority "C=US,O=MSFT,CN=?Microsoft Root Authority?" -AuthorityType Root

PS C:\>$cert2Proposal = New-NetIPsecAuthProposal -Machine -Cert -Authority "C=US,O=MYORG,CN='My Organizations Root Certificate'" -AuthorityType Root

PS C:\>$certAuthSet = New-NetIPsecPhase1AuthSet -DisplayName "Computer Certificate Auth Set" -Proposal $cert1Proposal,$cert2Proposal

PS C:\>New-NetIPSecRule -DisplayName "Authenticate with Certificates Rule" -InboundSecurity Require -OutboundSecurity Request -Phase2AuthSet $certAuthSet.Name

This example creates a rule that requires that incoming connections are authenticated by using either of two computer certificates. The computer also requests

authentication for outbound connections, but allows an outbound connection if authentication is not successful.

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

PS C:\>$mkerbauthprop = New-NetIPsecAuthProposal -Machine -Kerberos

PS C:\>$mntlmauthprop = New-NetIPsecAuthProposal -Machine -NTLM

PS C:\>$p1Auth = New-NetIPsecPhase1AuthSet -DisplayName "First Machine Auth" -Proposal $mkerbauthprop,$mntlmauthprop

PS C:\>$ukerbauthprop = New-NetIPsecAuthProposal -User -Kerberos

PS C:\>$unentlmauthprop = New-NetIPsecAuthProposal -User -NTLM

PS C:\>$anonyauthprop = New-NetIPsecAuthProposal -Anonymous

PS C:\>$p2Auth = New-NetIPsecPhase2AuthSet -DisplayName "Second User Auth" -Proposal $ukerbauthprop,$unentlmauthprop,$anonyauthprop

PS C:\>New-NetIPSecRule -DisplayName "Authenticate Both Computer and User" -InboundSecurity Require -OutboundSecurity Require -Phase1AuthSet $p1Auth.Name

-Phase2AuthSet $p2Auth.Name

This example creates a rule that requires a first, or computer, authentication and attempts an optional second, or user, authentication.

RELATED LINKS

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

Get-NetIPsecMainModeSA

New-NetIPsecPhase1AuthSet

New-NetIPsecPhase2AuthSet

New-NetIPSecRule