Windows PowerShell Get-Help on Cmdlet 'Set-LapsADReadPasswordPermission'

PS:\>Get-HELP Set-LapsADReadPasswordPermission -Full

NAME

Set-LapsADReadPasswordPermission

SYNOPSIS

Configures security on an Active Directory (AD) Organizational Unit (OU) to grant specific users or groups permission to query Windows Local Administrator Password

Solution (LAPS) passwords.

SYNTAX

Set-LapsADReadPasswordPermission -AllowedPrincipals <System.String[]> [-Credential <System.Management.Automation.PSCredential>] [-Domain <System.String>]

[-DomainController <System.String>] -Identity <System.String[]> [-Confirm] [-WhatIf] [<CommonParameters>]

DESCRIPTION

The `Set-LapsADReadPasswordPermission` cmdlet is used by administrators to configure security permissions on an OU to allow specific users or groups to query LAPS

passwords on computers in that OU. Users and groups must be fully qualified with both domain and user name components. The only exception to this is when the

specified name resolves to a built-in principal, such as `Domain Admins`.

PARAMETERS

-AllowedPrincipals <System.String[]>

Specifies the name of the users or groups should be granted the permissions. Users or groups may be specified in either name or SID format. If specified in name

format, the name must always include the identifying domain name portion unless the name maps to a well-known or built-in account.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Credential <System.Management.Automation.PSCredential>

Specifies the credentials to use when updating AD. If not specified, the current user's credentials are used.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Domain <System.String>

Specifies the name of the domain to connect to.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-DomainController <System.String>

Specifies the name of the domain controller to connect to.

Required? false

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Identity <System.String[]>

Specifies the name of the OU to update.

This parameter accepts several different name formats that influence the criteria used in the resultant AD search. The supported name formats are as follows:

- distinguishedName (begins with a `CN=`)

- name (for all other inputs)

Setting permissions on the domain root is only supported using the distinguishedName input format, for example 'DC=laps,DC=com'.

Required? true

Position? named

Default value None

Accept pipeline input? True (ByValue)

Accept wildcard characters? false

-Confirm <System.Management.Automation.SwitchParameter>

Prompts you for confirmation before running the cmdlet.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-WhatIf <System.Management.Automation.SwitchParameter>

Shows what would happen if the cmdlet runs. The cmdlet isn't 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

System.String[]

OUTPUTS

System.Object

NOTES

-------------------------- Example 1 --------------------------

Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals "Domain Admins"

Name DistinguishedName

---- -----------------

LapsTestOU OU=LapsTestOU,DC=laps,DC=com

This example shows how to run the cmdlet with an isolated name that successfully maps to a well-known user or group.

-------------------------- Example 2 --------------------------

Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals @("S-1-5-21-2889755270-1324585639-743026605-1215")

Name DistinguishedName

---- -----------------

LapsTestOU OU=LapsTestOU,DC=laps,DC=com

This example shows how to run the cmdlet specifying a user SID as input.

-------------------------- Example 3 --------------------------

Set-LapsADReadPasswordPermission -Identity 'OU=LapsTestOU,DC=laps,DC=com' -AllowedPrincipals @("laps.com\LapsAdmin1", "LapsAdmin2@laps.com")

Name DistinguishedName

---- -----------------

LapsTestOU OU=LapsTestOU,DC=laps,DC=com

This example shows how to run the cmdlet specifying two fully qualified user names in different formats.

---------- Example 4 ----------

Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals @("LapsAdministratorsGroup")

Set-LapsADReadPasswordPermission : The 'LapsAdministratorsGroup' account appears to be an isolated
name but is not a well-known name. Please use a fully qualified name instead, such as
"LAPSAdmins@contoso.com" or "contoso\LAPSAdmins"
At line:1 char:1
+ Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincip ...
+ ~~~~~~
    + CategoryInfo : InvalidArgument: (:) [Set-LapsADReadPasswordPermission], LapsPowershellException
    + FullyQualifiedErrorId : Invalid principal specified,Microsoft.Windows.LAPS.SetLapsADReadPasswordPermission

This example shows a failure caused by specifying an isolated name that didn't resolve to a well-known or built-in account. The fix for this error would be to add a
domain name qualifier to the input name, for example `LapsAdministratorsGroup@laps.com`.

RELATED LINKS

Online Version: https://learn.microsoft.com/powershell/module/laps/set-lapsadreadpasswordpermission?view=windowsserver2022-ps&wt.mc_id=ps-gethelp

Windows LAPS Overview https://go.microsoft.com/fwlink/?linkid=2233901