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

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

NAME

Get-LapsADPassword

SYNOPSIS

Queries Windows Local Administrator Password Solution (LAPS) credentials from Active Directory (AD) on a specified AD computer or domain controller object.

SYNTAX

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-Credential <System.Management.Automation.PSCredential>] [-DecryptionCredential <System.Management.Automation.PSCredential>] [-IncludeHistory] [<CommonParameters>]

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-Credential <System.Management.Automation.PSCredential>] [-DecryptionCredential <System.Management.Automation.PSCredential>] -Domain <System.String> [-IncludeHistory] [<CommonParameters>]

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-Credential <System.Management.Automation.PSCredential>] [-DecryptionCredential <System.Management.Automation.PSCredential>] -DomainController <System.String> [-IncludeHistory] [<CommonParameters>]

[<CommonParameters>]

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-Credential <System.Management.Automation.PSCredential>] [-DecryptionCredential <System.Management.Automation.PSCredential>] [-DomainController <System.String>] [-IncludeHistory] -Port <System.Nullable`1[System.Int32]> [<CommonParameters>]

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-IncludeHistory] -Port <System.Nullable`1[System.Int32]> -RecoveryMode [<CommonParameters>]

Get-LapsADPassword [-Identity] <System.String[]> [-AsPlainText] [-IncludeHistory] -RecoveryMode [<CommonParameters>]

DESCRIPTION

The `Get-LapsADPassword` cmdlet allows administrators to retrieve LAPS passwords and password history for an Active Directory computer or domain controller object.

Depending on policy configuration, LAPS passwords may be stored in either clear-text form or encrypted form. The `Get-LapsADPassword` cmdlet automatically decrypts

encrypted passwords.

The `Get-LapsADPassword` cmdlet may also be used to connect to a mounted AD snapshot.

The Verbose parameter may be used to get additional information about the cmdlet's operation.

PARAMETERS

-AsPlainText <System.Management.Automation.SwitchParameter>

Specify this parameter to return the LAPS passwords in clear-text format. The default behavior is to return the LAPS passwords wrapped in a .NET SecureString

object.

> [!IMPORTANT] > Using this parameter exposes the returned clear-text password to casual viewing and may pose a >

security risk. This parameter should be used

with caution and only in support or testing > situations.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Credential <System.Management.Automation.PSCredential>

Specifies a set of credentials to use when querying AD for the LAPS credentials. 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

-DecryptionCredential <System.Management.Automation.PSCredential>

Specifies a set of credentials to use when decrypting encrypted LAPS credentials. 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? true

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, or the remote server on which an AD Snapshot Browser is running.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-Identity <System.String[]>

Specifies the name of the computer or domain controller object to retrieve LAPS credentials from.

This parameter accepts several different name formats that influence the criteria used when searching AD for the target device. The supported name formats are as

follows:

- distinguishedName (begins with a `CN=`)

- samAccountName (begins with a '$")

- dnsHostName (contains at least one '.' character)

- name (for all other inputs)

Required? true

Position? 0

Default value None

Accept pipeline input? True (ByPropertyName, ByValue)

Accept wildcard characters? false

-IncludeHistory <System.Management.Automation.SwitchParameter>

Specifies that any older LAPS credentials on the computer object should also be displayed.

Required? false

Position? named

Default value False

Accept pipeline input? False

Accept wildcard characters? false

-Port <System.Nullable`1[System.Int32]>

Specifies the AD Snapshot Browser port to connect to.

Required? true

Position? named

Default value None

Accept pipeline input? False

Accept wildcard characters? false

-RecoveryMode <System.Management.Automation.SwitchParameter>

This parameter provides a last-ditch option when it's no longer possible to decrypt a given LAPS credential via the normal mechanisms. For example, this might be

necessary if a LAPS credential was encrypted against a group that has since been deleted.

>[!IMPORTANT] > When specifying this parameter, you must be logged-in locally as a Domain Administrator on a > writable domain controller.

Required? true

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 ----------

Get-LapsADPassword LAPSCLIENT

ComputerName : LAPSCLIENT

DistinguishedName : CN=LAPSCLIENT,OU=LapsTestOU,DC=laps,DC=com

Account : Administrator

Password : System.Security.SecureString

PasswordUpdateTime : 4/9/2023 10:03:41 AM

ExpirationTimestamp : 4/14/2023 10:03:41 AM

Source : CleartextPassword

DecryptionStatus : NotApplicable

AuthorizedDecryptor : NotApplicable

This example demonstrates querying the current LAPS password for the `LAPSCLIENT` computer in the current domain. The password was stored in AD in clear-text form and

didn't require decryption. The password was returned wrapped in a SecureString object.

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

Get-LapsADPassword -Identity LAPSCLIENT -DomainController lapsDC -AsPlainText

ComputerName : LAPSCLIENT

DistinguishedName : CN=LAPSCLIENT,OU=LapsTestOU,DC=laps,DC=com

Account : Administrator

Password : k8P]Xl5T-ky!aj4s21el3S#.x44!e{8+,{L!M

PasswordUpdateTime : 4/9/2023 10:03:41 AM

ExpirationTimestamp : 4/14/2023 10:03:41 AM

Source : CleartextPassword

DecryptionStatus : NotApplicable

AuthorizedDecryptor : NotApplicable

This example demonstrates querying the current LAPS password on a specific domain controller (`lapsDC`), for the `LAPSCLIENT` computer, requesting that the password

be displayed in clear-text form. The password was stored in AD in clear-text form and didn't require decryption. The password was returned in clear-text form.

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

Get-LapsADPassword -Identity LAPSCLIENT2 -Domain laps.com -AsPlainText -IncludeHistory

ComputerName : LAPSCLIENT2

DistinguishedName : CN=LAPSCLIENT2,OU=LapsTestEncryptedOU,DC=laps,DC=com

Account : Administrator

Password : q64!7KI3BOe/&S%buM0nBaW{B]261zN5L0{;{

PasswordUpdateTime : 4/9/2023 9:39:38 AM

ExpirationTimestamp : 4/14/2023 9:39:38 AM

Source : EncryptedPassword

DecryptionStatus : Success

AuthorizedDecryptor : LAPS\LAPS Admins

ComputerName : LAPSCLIENT2

DistinguishedName : CN=LAPSCLIENT2,OU=LapsTestEncryptedOU,DC=laps,DC=com

Account : Administrator

Password : O{P61q6bu(3kZ6&#p2y.&F$cWd;0dm8!]Wl5j

PasswordUpdateTime : 4/9/2023 9:38:10 AM

ExpirationTimestamp :

Source : EncryptedPasswordHistory

DecryptionStatus : Success

AuthorizedDecryptor : LAPS\LAPS Admins

This example demonstrates querying the current LAPS password for the `LAPSCLIENT2` computer, in a specific AD domain (`laps.com`), requesting that the password be

displayed in clear-text form. The password was stored in AD in encrypted form and was successfully decrypted.

> [!NOTE] > ExpirationTimestamp is always empty for any older LAPS passwords returned.

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

Get-LapsADPassword -Identity lapsDC.laps.com -AsPlainText

ComputerName : LAPSDC

DistinguishedName : CN=LAPSDC,OU=Domain Controllers,DC=laps,DC=com

Account : Administrator

Password : 118y$rsw.3y58yG]on$Hii

PasswordUpdateTime : 4/9/2023 10:17:51 AM

ExpirationTimestamp : 4/19/2023 10:17:51 AM

Source : EncryptedDSRMPassword

DecryptionStatus : Success

AuthorizedDecryptor : LAPS\Domain Admins

This example demonstrates querying the current LAPS password for the `lapsDC.laps.com` domain controller, requesting that the password be displayed in clear-text

form. The password was stored in AD in encrypted form and was successfully decrypted.

---------- Example 5 ----------

Get-LapsADPassword LAPSDC

ComputerName : LAPSDC

DistinguishedName : CN=LAPSDC,OU=Domain Controllers,DC=laps,DC=com

Account :

Password :

PasswordUpdateTime : 4/9/2023 10:17:51 AM

ExpirationTimestamp : 4/19/2023 10:17:51 AM

Source : EncryptedDSRMPassword

DecryptionStatus : Unauthorized

AuthorizedDecryptor : LAPS\Domain Admins

This example demonstrates querying the current LAPS password for the `LAPSDC` domain controller when the user doesn't have permissions to decrypt the LAPS DSRM

password.

---------- Example 6 ----------

Get-LapsADPassword LAPSLEGACYCLIENT -AsPlainText

ComputerName : LAPSLEGACYCLIENT

DistinguishedName : CN=LAPSLEGACYCLIENT,OU=LegacyLapsOU,DC=laps,DC=com

Account :

Password : Z#x}&7BluHf3{r+C218

PasswordUpdateTime :

ExpirationTimestamp : 5/14/2023 1:55:39 PM

Source : LegacyLapsCleartextPassword

DecryptionStatus : NotApplicable

AuthorizedDecryptor : NotApplicable

This example demonstrates querying the current LAPS password for the 'LAPSLEGACYCLIENT' machine which is currently running in legacy LAPS emulation mode.

> [!NOTE] > When querying legacy LAPS-style passwords, the Account and PasswordUpdateTime fields are > always unavailable.

---------- Example 7 ----------

Get-LapsADPassword -Identity LAPSCLIENT -Port 50000 -AsPlainText

ComputerName : LAPSCLIENT

DistinguishedName : CN=LAPSCLIENT,OU=LapsTestOU,DC=laps,DC=com

Account : Administrator

Password : H6UycL[vj#zzTNVpS//G2{j&t9aO}k[K5l4)X

PasswordUpdateTime : 4/15/2023 6:51:45 AM

ExpirationTimestamp : 4/20/2023 6:51:45 AM

Source : CleartextPassword

DecryptionStatus : NotApplicable

AuthorizedDecryptor : NotApplicable

This example demonstrates querying an AD Snapshot browser instance for the current LAPS password for the `LAPSCLIENT` machine. This example assumes that that the

snapshot browser has been previously started on the local machine listening on an LDAP port of `50000`.

RELATED LINKS

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

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

Get started with Windows LAPS and Windows Server Active Directory https://go.microsoft.com/fwlink/?linkid=2233705