



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

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

NAME

Get-LapsAADPassword

SYNOPSIS

Queries Microsoft Entra ID for the Windows Local Administrator Password Solution (LAPS) credentials on a specified Microsoft Entra device.

SYNTAX

Get-LapsAADPassword [-AsPlainText] -DeviceIds <System.String[]> [-IncludeHistory] [-IncludePasswords]
[<CommonParameters>]

DESCRIPTION

The `Get-LapsAADPassword` cmdlet allows administrators to retrieve LAPS passwords and password history for a Microsoft Entra joined device. This is implemented by sending queries to Microsoft Graph over the deviceLocalCredentials collection.

The `Get-LapsAADPassword` cmdlet supports two basic modes when querying LAPS passwords:

The first mode queries for non-sensitive metadata, for example time the password was backed up to Azure and the expected expiration time of a password. This mode

requires that the client be granted the Microsoft Graph ``DeviceLocalCredential.ReadBasic.All`` permission.

The second mode queries for all password information including both the metadata information described above and the clear-text form of the password(s). This mode

requires that the client be granted the Microsoft Graph ``DeviceLocalCredential.Read.All`` permission.

The `DeviceIds` parameter accepts either device names or device IDs, but the underlying Microsoft Graph queries only supports querying by device ID. To support this

query, the cmdlet maps a device name input to its corresponding device ID by issuing a separate Microsoft Graph query. This extra query requires the ``Device.Read.All``

permission. If the target is a Microsoft Managed Desktop device, the ``DeviceManagementManagedDevices.Read.All`` permission may also be required.

> [!TIP] > If there are multiple devices in the tenant with the same name, the cmdlet fails. The workaround > is to input the device ID directly.

> [!IMPORTANT] > The ``Get-LapsAADPassword`` cmdlet is implemented as a wrapper around the Microsoft Graph PowerShell > library, which must be manually installed on the

device before ``Get-LapsAADPassword`` can work. > Additional configuration steps are required in your Microsoft Entra tenant to enable authentication to > Microsoft

Graph and to grant the necessary Microsoft Graph permissions. For more information, see > Get started with Windows LAPS and Microsoft Entra ID

(<https://go.microsoft.com/fwlink/?linkid=2233704>)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

-DeviceIds <System.String[]>

Specifies the device name or device ID to query LAPS credentials.

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

-IncludeHistory <System.Management.Automation.SwitchParameter>

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

Required? false
Position? named
Default value False
Accept pipeline input? False
Accept wildcard characters? false

-IncludePasswords <System.Management.Automation.SwitchParameter>

Specifies whether to return password information.

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

System.Object

NOTES

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

Connect-MgGraph -TenantId b20f5886-bddf-43bb-ae6-dda0c87c5fa2 -ClientId 9fa98e34-277f-47fa-9847-e36bdf6bca1f
Get-LapsAADPassword -DeviceIds LAPSAAD

DeviceName DeviceId PasswordExpirationTime

----- -----

This example shows how to query basic LAPS password metadata information for the target device that is specified by device name.

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

```
Connect-MgGraph -TenantId b20f5886-bddf-43bb-ae6-dda0c87c5fa2 -ClientId 9fa98e34-277f-47fa-9847-e36bdf6bca1f
Get-LapsAADPassword -DeviceIds dfc6d5f0-225a-4b46-adcf-73a349a31e70 -IncludePasswords
```

```
DeviceName      : LAPSAAD
DeviceId        : dfc6d5f0-225a-4b46-adcf-73a349a31e70
Account         : LapsAdmin
Password        : System.Security.SecureString
PasswordExpirationTime : 4/22/2023 8:45:29 AM
PasswordUpdateTime   : 4/11/2023 8:45:29 AM
```

This example shows how to query the full LAPS password information for the target device that is specified by device ID.

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

```
Connect-MgGraph -TenantId b20f5886-bddf-43bb-ae6-dda0c87c5fa2 -ClientId 9fa98e34-277f-47fa-9847-e36bdf6bca1f
Get-LapsAADPassword -DeviceIds dfc6d5f0-225a-4b46-adcf-73a349a31e70 -IncludePasswords -AsPlainText
```

```
DeviceName      : LAPSAAD
DeviceId        : dfc6d5f0-225a-4b46-adcf-73a349a31e70
Account         : LapsAdmin
Password        : g4q22s[Xz8}!T32[4;Z#0M}v35udF[xB0}iB;P@xk%9E9Tgw,W]7)vx9O!-
PasswordExpirationTime : 4/22/2023 8:45:29 AM
PasswordUpdateTime   : 4/11/2023 8:45:29 AM
```

This example shows how to query the full LAPS password information for the target device that is specified by device ID, and displaying the password in clear-text form.

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

Connect-MgGraph -TenantId b20f5886-bddf-43bb-ae6-dda0c87c5fa2 -ClientId 9fa98e34-277f-47fa-9847-e36bdf6bca1f
Get-LapsAADPassword -DeviceIds lapsAAD -IncludePasswords -AsPlainText -IncludeHistory

DeviceName : LAPSAAD
DeviceId : dfc6d5f0-225a-4b46-adcf-73a349a31e70
Account : LapsAdmin
Password :]5j)1fi]Rv&Pj+IMiAzq1R9b+yJ.@Q,80#01U541vsC8\$Vv\${hac8TJlkT8
PasswordExpirationTime : 4/22/2023 8:55:20 AM
PasswordUpdateTime : 4/11/2023 8:55:21 AM

DeviceName : LAPSAAD
DeviceId : dfc6d5f0-225a-4b46-adcf-73a349a31e70
Account : LapsAdmin
Password : t&.1P%9891]24l0X4AA4O22a30R1lz(ar7N9{tTf349.lz{L82O6v{!+,gg
PasswordExpirationTime :
PasswordUpdateTime : 4/11/2023 8:55:16 AM

DeviceName : LAPSAAD
DeviceId : dfc6d5f0-225a-4b46-adcf-73a349a31e70
Account : LapsAdmin
Password : g4q22s[Xz8]!T32[4;Z#0M}v35udF[xB0]iB;P@xk%9E9Tgw,W]7)vx9O!-
PasswordExpirationTime :
PasswordUpdateTime : 4/11/2023 8:45:29 AM

This example shows how to query the full LAPS password information for the target device that is specified by device name, requesting password history, and displaying the passwords in clear-text form.

RELATED LINKS

Online

Version:

https://learn.microsoft.com/powershell/module/laps/get-lapsaadpassword?view=windowsserver2022-ps&wt.mc_id=ps-gethel

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

Get started with Windows LAPS and Microsoft Entra ID <https://go.microsoft.com/fwlink/?linkid=2233704>