# Get started with Windows LAPS and Windows Server Active Directory

## Domain functional level and domain controller OS version requirements

If your domain is configured below 2016 Domain Functional Level (DFL), you can't enable Windows LAPS password encryption period. Without password encryption, clients can only be configured to store passwords in clear-text (secured by Active Directory ACLs) and DCs can't be configured to manage their local DSRM account.

Once your domain reaches 2016 DFL, you can enable Windows LAPS password encryption. However if you're still running any WS2016 DCs, those WS2016 DCs don't support Windows LAPS and therefore can't use the DSRM account management feature.

It's fine to use supported operating systems older than WS2016 on your domain controllers as long as you're aware of these limitations.

The following table summarizes the various supported-or-not scenarios:

Expand table

| Domain details | Clear-text password storage supported | Encrypted password storage supported (for domain-joined clients) | DSRM account management supported (for DCs) |
|---|---|---|---|
| Below 2016 DFL | Yes | No | No |

| Domain details | Clear-text password storage supported | Encrypted password storage supported (for domain-joined clients) | DSRM account management supported (for DCs) |
|---|---|---|---|
| 2016 DFL with one or more WS2016 DCs | Yes | Yes | Yes but only for WS2019 and later DCs |
| 2016 DFL with only WS2019 and later DCs | Yes | Yes | Yes |

Microsoft strongly recommends customer upgrade to the latest available operating system on clients, servers, and domain controllers in order to take advantage of latest features and security improvements.

# Update the Windows Server Active Directory schema

The Windows Server Active Directory schema must be updated prior to using Windows LAPS. This action is performed by using the `Update-LapsADSchema` cmdlet. It's a one-time operation for the entire forest. This operation can be performed on a Windows Server 2022 or Windows Server 2019 domain controller updated with Windows LAPS, but can also be performed on a non-domain-controller as long as it supports the Windows LAPS PowerShell module.

PowerShell Copy

```
PS C:\> Update-LapsADSchema
```

Tip

Pass the `-Verbose` parameter to see detailed info on what the `Update-LapsADSchema` cmdlet (or any other cmdlet in the LAPS PowerShell module) is doing.

# Grant the managed device permission to update its password

The managed device needs to be granted permission to update its password. This action is performed by setting inheritable permissions on the Organizational Unit (OU) the device is in. The `Set-LapsADComputerSelfPermission` is used for this purpose, for example:

PowerShell Copy

```
PS C:\> Set-LapsADComputerSelfPermission -Identity NewLaps
```

Output Copy

```
Name    DistinguishedName
----    -----------------
NewLAPS OU=NewLAPS,DC=laps,DC=com
```

Tip

If you prefer to set the inheritable permissions on the root of the domain, this is possible by specifying the entire domain root using DN syntax. For example, specify 'DC=laps,DC=com' for the -Identity parameter.

# Remove Extended Rights permissions

Some users or groups might already be granted Extended Rights permission on the managed device's OU. This permission is problematic because it grants the ability to read confidential attributes (all of the Windows LAPS password attributes are marked as confidential). One way to check to see who is granted these permissions is by using the `Find-LapsADExtendedRights` cmdlet. For example:

PowerShell Copy

```
PS C:\> Find-LapsADExtendedRights -Identity newlaps
```

Output Copy

```
ObjectDN                ExtendedRightHolders
--------                --------------------
OU=NewLAPS,DC=laps,DC=com {NT AUTHORITY\SYSTEM, LAPS\Domain Admins}
```

In the output in this example, only trusted entities (SYSTEM and Domain Admins) have the privilege. No other action is required.

# Configure device policy

Complete a few steps to configure the device policy.

# Choose a policy deployment mechanism

The first step is to choose how to apply policy to your devices.

Most environments use Windows LAPS Group Policy to deploy the required settings to their Windows Server Active Directory-domain-joined devices.

If your devices are also hybrid-joined to Microsoft Entra ID, you can deploy policy by using Microsoft Intune with the Windows LAPS configuration service provider (CSP).

# Configure specific policies

At a minimum, you must configure the BackupDirectory setting to the value 2 (backup passwords to Windows Server Active Directory).

If you don't configure the AdministratorAccountName setting, Windows LAPS defaults to managing the default built-in local administrator account. This built-in account is automatically identified using its well-known relative identifier (RID) and should never be identified using its name. The name of the built-in local administrator account varies depending on the default locale of the device.

If you want to configure a custom local administrator account, you should configure the AdministratorAccountName setting with the name of that account.

Important

If you configure Windows LAPS to manage a custom local administrator account, you must ensure that the account is created. Windows LAPS doesn't create the account. We recommend that you use the RestrictedGroups CSP to create the account.

You can configure other settings, like PasswordLength, as needed for your organization.

When you don't configure a given setting, the default value is applied - be sure to understand those defaults. For example if you enable password encryption but don't configure the ADPasswordEncryptionPrincipal setting, the password is encrypted so that only Domain Admins can decrypt it. You can configure ADPasswordEncryptionPrincipal with a different setting if you want non-Domain Admins to be able to decrypt.

# Update a password in Windows Server Active Directory

Windows LAPS processes the currently active policy on a periodic basis (every hour) and responds to Group Policy change notifications. It responds based on the policy and change notifications.

To verify that the password was successfully updated in Windows Server Active Directory, look in the event log for the 10018 event:

Image not found or type unknown

Screenshot of the event log that shows a successful Windows Server Active Directory password upd

To avoid waiting after you apply the policy, you can run the `Invoke-LapsPolicyProcessing` PowerShell cmdlet.

# Retrieve a password from Windows Server Active Directory

Use the `Get-LapsADPassword` cmdlet to retrieve passwords from Windows Server Active Directory. For example:

PowerShell Copy

```
PS C:\> Get-LapsADPassword -Identity lapsAD2 -AsPlainText
```

Output Copy

```
ComputerName        : LAPSAD2
DistinguishedName   : CN=LAPSAD2,OU=NewLAPS,DC=laps,DC=com
Account             : Administrator
Password            : Zlh+lzC[0e0/VU
PasswordUpdateTime  : 7/1/2022 1:23:19 PM
ExpirationTimestamp : 7/31/2022 1:23:19 PM
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : LAPS\Domain Admins
```

This output result indicates that password encryption is enabled (see `Source`). Password encryption requires that your domain is configured for Windows Server 2016 Domain Functional Level or later.

# Rotate the password

Windows LAPS reads the password expiration time from Windows Server Active Directory during each policy processing cycle. If the password is expired, a new password is generated and stored immediately.

In some situations (for example, after a security breach or for ad-hoc testing), you might want to rotate the password early. To manually force a password rotation, you can use the `Reset-LapsPassword` cmdlet.

You can use the `Set-LapsADPasswordExpirationTime` cmdlet to set the scheduled password expiration time as stored in Windows Server Active Directory. For example:

PowerShell Copy

```
PS C:\> Set-LapsADPasswordExpirationTime -Identity lapsAD2
```

Output Copy

```
DistinguishedName                    Status
-----------------                    ------
CN=LAPSAD2,OU=NewLAPS,DC=laps,DC=com PasswordReset
```

The next time Windows LAPS wakes up to process the current policy, it sees the modified password expiration time and rotates the password. If you don't want to wait, you can run the `Invoke-LapsPolicyProcessing` cmdlet.

You can use the `Reset-LapsPassword` cmdlet to locally force an immediate rotation of the password.

# See also

- Introducing Windows Local Administrator Password Solution with Microsoft Entra ID
- Windows Local Administrator Password Solution in Microsoft Entra ID (preview)
- RestrictedGroups CSP
- Microsoft Intune

- Microsoft Intune support for Windows LAPS
- Windows LAPS CSP
- Windows LAPS Troubleshooting Guidance

# Next steps

- Configure Windows LAPS policy settings
- Use Windows LAPS event logs
- Use Windows LAPS PowerShell cmdlets
- Key concepts in Windows LAPS

---

Revision #1
Created 5 January 2024 05:47:49 by ColtM
Updated 12 May 2024 05:12:06 by ColtM