Configure policy settings for Windows LAPS

Supported policy roots

Although we don't recommend it, you can administer a device by using multiple policy management mechanisms. To support this scenario in an understandable and predictable way, each Windows LAPS policy mechanism is assigned a distinct registry root key:

Expand table

Policy name	Policy registry key root
LAPS CSP	`HKLM\Software\Microsoft\Policies\LAPS`
LAPS Group Policy	`HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\LAPS`
LAPS Local Configuration	`HKLM\Software\Microsoft\Windows\CurrentVersion\LAPS\Config`
Legacy Microsoft LAPS	`HKLM\Software\Policies\Microsoft Services\AdmPwd`

Windows LAPS queries all known registry key policy roots, starting at the top and moving down. If no settings are found under a root, that root is skipped and the query proceeds to the next root. When a root that has at least one explicitly defined setting is found, that root is used as the active policy. If the chosen root is missing any settings, the settings are assigned their default values.

Policy settings are never shared or inherited across policy key roots.

Tip

The LAPS Local Configuration key is included in the preceding table for completeness. You can use this key if necessary, but the key primarily is intended to be used for testing and development. No management tools or policy mechanisms target this key.

Supported policy settings by BackupDirectory

Windows LAPS supports multiple policy settings that you can administer via various policy management solutions, or even directly via the registry. Some of these settings only apply when backing up passwords to Active Directory, and some settings are common to both the AD and Microsoft Entra scenarios.

The following table specifies which settings apply to devices that have the specified BackupDirectory setting:

Expand table

Setting name	Applicable when BackupDirectory=Microsoft Entra ID?	Applicable when BackupDirectory=AD?
AdministratorAccountName	Yes	Yes
PasswordAgeDays	Yes	Yes
PasswordLength	Yes	Yes
PassphraseLength	Yes	Yes
PasswordComplexity	Yes	Yes
PostAuthenticationResetDelay	Yes	Yes
PostAuthenticationActions	Yes	Yes
ADPasswordEncryptionEnabled	No	Yes
ADPasswordEncryptionPrincipal	No	Yes
ADEncryptedPasswordHistorySize	No	Yes
ADBackupDSRMPassword	No	Yes
PasswordExpirationProtectionEnabled	No	Yes

Setting name	Applicable when BackupDirectory=MicrosoftEntra ID?	Applicable when BackupDirectory=AD?
AutomaticAccountManagementEnabled	Yes	Yes
AutomaticAccountManagementTarget	Yes	Yes
AutomaticAccountManagementNameOrPrefix	Yes	Yes
AutomaticAccountManagementEnableAccount	Yes	Yes
AutomaticAccountManagementRandomizeName	Yes	Yes

If BackupDirectory is set to Disabled, all other settings are ignored.

You can administer almost all settings by using any policy management mechanism. The Windows LAPS configuration service provider (CSP) has two exceptions to this rule. The Windows LAPS CSP supports two settings that aren't in the preceding table: ResetPassword and ResetPasswordStatus. Also, Windows LAPS CSP doesn't support the ADBackupDSRMPassword setting (domain controllers are never managed via CSP). For more information, see the LAPS CSP documentation.

Windows LAPS Group Policy

Windows LAPS includes a new Group Policy Object that you can use to administer policy settings on Active Directory domain-joined devices. To access the Windows LAPS Group Policy, in Group Policy Management Editor, go to **Computer Configuration** > **Administrative Templates** > **System** > **LAPS**. The following figure shows an example:

Image not found or type unknown

Screenshot of the Group Policy Management Editor that shows the Windows LAPS policy settings.

The template for this new Group Policy object is installed as part of Windows at `%windir%\PolicyDefinitions\LAPS.admx`.

Group Policy Object Central Store

Important

The Windows LAPS GPO template files are NOT automatically copied to your GPO central store as part of a Windows Update patching operation, assuming you have chosen to implement that approach. Instead you must manually copy the LAPS.admx to the GPO central store location. See Create and Manage Central Store.

Windows LAPS CSP

Windows LAPS includes a specific CSP that you can use to administer policy settings on Microsoft Entra joined devices. Manage the Windows LAPS CSP by using Microsoft Intune.

Apply policy settings

The following sections describe how to use and apply various policy settings for Windows LAPS.

BackupDirectory

Use this setting to control which directory the password for the managed account is backed up to.

Expand table

Value	Description of setting
0	Disabled (password isn't backed up)
1	Back up the password to Microsoft Entra-only
2	Back up the password to Windows Server Active Directory only

If not specified, this setting defaults to 0 (Disabled).

AdministratorAccountName

Use this setting to configure the name of the managed local administrator account.

If not specified, this setting defaults to managing the built-in local administrator account.

Important

Don't specify this setting unless you want to manage an account other than the built-in local administrator account. The local administrator account is automatically identified by its well-known relative identifier (RID).

Important

You can configure the specified account (built-in or custom) as either enabled or disabled. Windows LAPS will manage that account's password in either state. If left in a disabled state however, the account must obviously first be enabled in order to be actually used.

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.

Important

This setting is ignored when AutomaticAccountManagementEnabled is enabled.

PasswordAgeDays

This setting controls the maximum password age of the managed local administrator account. Supported values are:

- **Minimum**: 1 day (When the backup directory is configured to be Microsoft Entra ID, the minimum is 7 days.)
- **Maximum**: 365 days

If not specified, this setting defaults to 30 days.

Important

Changes to the PasswordAgeDays policy setting have no effect on the expiration time of the current password. Similarly, changes to the PasswordAgeDays policy setting won't cause the managed device to initiate a password rotation.

PasswordLength

Use this setting to configure the length of the password of the managed local administrator account. Supported values are:

- **Minimum**: 8 characters
- **Maximum**: 64 characters

If not specified, this setting defaults to 14 characters.

Important

Do not configure PasswordLength to a value that is incompatible with the managed device's local password policy. This will result in Windows LAPS failing to create a new compatible password (look for a 10027 event in the Windows LAP event log).

The PasswordLength setting is ignored unless PasswordComplexity is configured to one of the password options.

PassphraseLength

Use this setting to configure the number of words in the passphrase of the managed local administrator account. Supported values are:

- **Minimum**: 3 words
- **Maximum**: 10 words

If not specified, this setting defaults to 6 words.

The PassphraseLength setting is ignored unless PasswordComplexity is configured to one of the passphrase options.

PasswordComplexity

Use this setting to configure the required password complexity of the managed local administrator account, or to specify that a passphrase is created.

Expand table

Value	Description of setting
1	Large letters
2	Large letters + small letters
3	Large letters + small letters + numbers
4	Large letters + small letters + numbers + special characters
5	Large letters + small letters + numbers + special characters (improved readability)
6	Passphrase (long words)

Value	Description of setting
7	Passphrase (short words)
8	Passphrase (short words with unique prefixes)

If not specified, this setting defaults to 4.

Important

Windows supports the lower password complexity settings (1, 2, and 3) only for backward compatibility with legacy Microsoft LAPS. We recommend that you always configure this setting to 4.

Important

Do not configure PasswordComplexity to a setting that is incompatible with the managed device's local password policy. This will result in Windows LAPS failing to create a new compatible password (look for a 10027 event in the Windows LAPS event log).

PasswordExpirationProtectionEnabled

Use this setting to configure enforcement of maximum password age for the managed local administrator account.

Supported values are either 1 (True) or 0 (False).

If not specified, this setting defaults to 1 (True).

Tip

In legacy Microsoft LAPS mode, this setting defaults to False for backward compatibility.

ADPasswordEncryptionEnabled

Use this setting to enable encryption of passwords in Active Directory.

Supported values are either 1 (True) or 0 (False).

Important

Enabling this setting requires that your Active Directory domain is running at Domain Functional Level 2016 or later.

ADPasswordEncryptionPrincipal

Use this setting to configure the name or security identifier (SID) of a user or group that can decrypt the password stored in Active Directory.

This setting is ignored if the password currently is stored in Azure.

If not specified, only members of the Domain Admins group in the device's domain can decrypt the password.

If specified, the specified user or group can decrypt the password stored in Active Directory.

Important

The string that's stored in this setting is either an SID in string form or the fully qualified name of a user or group. Valid examples include:

- `S-1-5-21-2127521184-1604012920-1887927527-35197`
- `contoso\LAPSAdmins`
- `lapsadmins@contoso.com`

The principal identified (either by SID or by user or group name) must exist and is resolvable by the device.

NOTE: the data specified in this setting is entered as-is; for example, do *not* add enclosing quotes or parentheses.

This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.

This setting is ignored when Directory Services Repair Mode (DSRM) account passwords are backed up on a domain controller. In that scenario, this setting always defaults to the Domain Admins group of the domain controller's domain.

ADEncryptedPasswordHistorySize

Use this setting to configure how many previous encrypted passwords are remembered in Active Directory. Supported values are:

- **Minimum** : 0 passwords
- **Maximum**: 12 passwords

If not specified, this setting defaults to 0 passwords (disabled).

Important

This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.

This setting also takes effect on domain controllers that back up their DSRM passwords.

ADBackupDSRMPassword

Use this setting to enable backup of the DSRM account password on Windows Server Active Directory domain controllers.

Supported values are either 1 (True) or 0 (False).

This setting defaults to 0 (False).

Important

This setting is ignored unless ADPasswordEncryptionEnabled is configured to True and all other prerequisites are met.

PostAuthenticationResetDelay

Use this setting to specify the amount of time (in hours) to wait after an authentication before executing the specified post-authentication actions (see PostAuthenticationActions). Supported values are:

- **Minimum** : 0 hours (setting this value to 0 disables all post-authentication actions)
- **Maximum**: 24 hours

If not specified, this setting defaults to 24 hours.

PostAuthenticationActions

Use this setting to specify the actions to take upon expiration of the configured grace period (see PostAuthenticationResetDelay).

This setting can have one of the following values:

Expand table

Value	Name	Actions taken when the grace period expires	Comments

1	Reset password	The managed account password is reset.	
3	Reset password and sign out	The managed account password is reset, interactive sign-in sessions using the managed account are terminated, and SMB sessions using the managed account are deleted.	Interactive sign-in sessions receive a nonconfigurable two-minute warning to save their work and sign out.
5	Reset password and reboot	The managed account password is reset and the managed device is restarted.	The managed device is restarted after a nonconfigurable one-minute delay.
11	Reset password and sign out	The managed account password is reset, interactive sign-in sessions using the managed account are terminated, SMB sessions using the managed account are deleted, and any remaining processes running under the managed account identity are terminated.	Interactive sign-in sessions receive a nonconfigurable two-minute warning to save their work and sign out.

If not specified, this setting defaults to 3.

Important

The allowed post-authentication actions are intended to help limit the amount of time a Windows LAPS password can be used before it's reset. Signing out of the managed account or restarting the device are options that help ensure the time is limited. Abruptly terminating signed-in sessions or restarting the device might result in data loss.

From a security perspective, a malicious user who acquires administrative privileges on a device using a valid Windows LAPS password does have the ultimate ability to prevent or circumvent these mechanisms.

AutomaticAccountManagementEnabled

Use this setting to enable automatic account management.

Supported values are either 1 (True) or 0 (False).

This setting defaults to 0 (False).

AutomaticAccountManagementTarget

Use this setting to specify whether the built-in Administrator account is automatically managed, or a new custom account.

Expand table

Value	Description of setting
0	Automatically manage the built-in Administrator account
1	Automatically manage a new custom account

This setting defaults to 1.

This setting is ignored unless AutomaticAccountManagementEnabled is enabled.

AutomaticAccountManagementNameOrPrefix

Use this setting to specify the name or the name prefix of the automatically managed account.

This setting defaults to "WLapsAdmin".

This setting is ignored unless AutomaticAccountManagementEnabled is enabled.

AutomaticAccountManagementEnableAccount

Use this setting to enable or disable the automatically managed account.

Expand table

Value	Description of setting
0	Disable the automatically managed account

Value	Description of setting
1	Enable the automatically managed account

This setting defaults to 0.

This setting is ignored unless AutomaticAccountManagementEnabled is enabled.

AutomaticAccountManagementRandomizeName

Use this setting to enable randomization of the name of the automatically managed account.

When this setting is enabled, the name of the managed account (determined by the AutomaticAccountManagementNameOrPrefix setting) is suffixed with a random six-digit suffix every time the password is rotated.

Windows local account names have a maximum length of 20 characters, which means the name component must be 14 characters long at most to have sufficient space for the random suffix. Account names specified by AutomaticAccountManagementNameOrPrefix that are longer than 14 characters are truncated.

Expand table

Value	Description of setting
0	Don't randomize the name of the automatically managed account
1	Randomize the name of the automatically managed account

This setting defaults to 0.

This setting is ignored unless AutomaticAccountManagementEnabled is enabled.

See also

- Windows LAPS CSP
- Microsoft Intune

Next steps

- Use event logs for Windows LAPS
- Use Windows LAPS PowerShell cmdlet
- Windows LAPS schema extensions reference

Revision #1
Created 5 January 2024 05:47:26 by ColtM
Updated 12 May 2024 05:12:06 by ColtM