An Overview of Windows LAPS

What is Windows LAPS?

Windows LAPS (Local Administrator Password Solution) automatically manages a local administrator account's password: changing the password when it expires (using password length and complexity settings) and backing up the password to Active Directory so it is available for authorized users to retrieve.

Windows LAPS was made available with the April 2023 Cumulative Update for the following Operating Systems:

- Windows 11 22H2
- Windows 11 21H2
- Windows 10 (those editions still supported by Microsoft)
- Windows Server 2022
- Windows Server 2019

Windows LAPS is not available for Windows Server 2016, but you can continue to use legacy LAPS with it.

Windows LAPS is a whole new solution for managing the local administrator password and is not just an update of the legacy LAPS solution that was originally released in 2015. It includes much of the same functionality of legacy LAPS, and also includes a couple of new things:

- Supports encrypting passwords stored in AD
- Can store password history in AD (for encrypted passwords only)
- Supports saving the password to Azure AD instead of Windows Server (on-prem) AD

Comparing Windows LAPS and Legacy LAPS

Comparing Windows LAPS and Legacy LAPS		
	Windows LAPS	**Legacy LAPS**

Password-management bits	Included with the April 2023 Cumulative Update for Windows	The client-side extension must be installed on each computer.
Frequency of processing the LAPS policy cycle	This is hard-coded in Windows to 1 hour The Invoke-LapsPolicyProcessing PowerShell cmdlet can be used to trigger processing in addition to gpupdate /force.	Since this was a Group Policy Client-side extension, this was done at the same time as a group policy refresh. gpupdate /force will force the processing of Group Policy
Configuration options	Group Policy Configuration Service Provider (such as Intune)	Group Policy
Group Policy settings location	Computer Configuration – Policies – Administrative Templates – System – LAPS	Computer Configuration – Policies – Administrative Templates – LAPS
Where is the password stored in AD	All Windows LAPS attributes are confidential attributes: msLAPS-PasswordExpirationTime: This is a regular attribute that stores the date and time that the LAPS password will expire / when it will be reset, calculated by adding the value of the *Password Age (Days)* setting to the time the password was last set msLAPS-Password: A clear-text string that contains the name of the managed account, the timestamp of the password update, and the current password msLAPS-EncryptedPassword: The encrypted current password msLAPS-EncryptedPasswordHistory: Contains the encrypted previous passwords (it will store as many of the previous passwords as it is configured to, which allows for a maximum of 12) msLAPS-EncryptedDSRMPassword: This setting only pertains to Domain Controllers. msLAPS-EncryptedDSRMPasswordHistory: This setting only pertains to Domain Controllers.	ms-mcs-AdmPwd: This is a confidential attribute where the password is stored ms-mcs-AdmPwdExpirationTime: This is a regular attribute that stores the date and time that the LAPS password will expire / when it will be reset, calculated by adding the value of the *Password Age (Days)* setting to the time the password was last set
Where can the password be backed up to?	Active Directory or Entra ID.	Active Directory only.

Is the password encrypted when backed up to AD/Entra ID?	Active Directory: It depends on the LAPS policy in use when the password is saved in AD. Entra ID: Yes, the password is always encrypted.	No.
Who can access the password in AD	• When backed up to AD: If the password is not encrypted (msLAPS-Password) you must have access to the confidential attribute in AD.If the password is encrypted (msLAPS-EncryptedPassword, msLAPS-EncryptedPasswordHistory) you must have access to the confidential attribute in AD AND be an authorized password decryptor (refer to the *Windows LAPS Policy Settings* section below).Note that each encrypted password in the password history can/may have a different decryptor. • When backed up to Entra ID: By default only members of the following roles: Global Administrator, Cloud Device Administrator, Intune Administrator	You must have access to the confidential attribute in AD.

Prerequisites for Using Windows LAPS

1. The computer object must have permission to write its password to itself in Active Directory.
2. The computer must be running an Operating System for which Windows LAPS is available.
3. The computer must be updated with the April 2023 Cumulative Update for Windows or later.
4. The computer must have a Windows LAPS policy assigned to it.

5. The computer must be able to reach a Domain Controller in order to backup the password to AD.
6. The domain functional level must be Windows Server 2016 or later in order to support encrypting the password backed up to AD.

Windows LAPS Policy Settings

The following settings are located in **Computer Configuration – Policies – Administrative Templates – System – LAPS**:

Setting	Description

Password Settings	If enabled, you can configure the following aspects of the password that is generated: **Password Complexity**: Determines what type of characters are used to generate the password. The available options are: • Large letters • Large letters + small letters • Large letters + small letters + numbers • Large letters + small letters + numbers + specials • Large letters + small letters + numbers + specials (improved readability) *This option is only available starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* With this option, the following letters are not used: l O Q l o With this option, the following numbers are not used: 0 1 With this option, only the following symbols are used: ! # % + @ : = ? * • Passphrase (long words) *This option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* • Passphrase (short words with unique prefixes) *This option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* • Passphrase (short words) *This option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* **Password Length**: Determines how many characters the password will be in length. This must be a number from 8 – 64. The default value is 14. **Password Age (Days)**: This is the number of days that will be used to set the password expiration time. This must be a number from 1 – 365. The default value is 30. **Passphrase Length (words)**: This is the number of words that will be used in the passphrase (when Password Complexity is set to a passphrase option). This must be a number from 3 – 10. The default value is 6. *This option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).*

Name of administrator account to manage	The name of the local administrator account whose password is managed. Only set this if you want Windows LAPS to manage an account other than the built-in Administrator. The default, when not specified, is the built-in Administrator (by its well-known RID). Notes: If you specify a disabled account, the password will be managed by the account will not be enabled by LAPS. If you specify an account that does not exist, . If you specify an account that is not a member of the local Administrators group it will not be added to the local Administrators by LAPS.
Configure automatic account management	*This option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* *When enabled, this takes precedence over the Name of administrator account to manage setting.* If enabled, you can configure the following aspects of the managed account: **Specify the target account to manage**: Two options are available: • Manage a custom admin account A custom account will be managed by Windows LAPS. • Manage the built-in admin account The Built-in Administrator account will be managed by Windows LAPS (by its well-known RID). **Automatic account name (or name prefix)**: The name of the account that Windows LAPS will manage the password for (or the prefix on the name of the account if *Randomize the name of the managed account* is checked.) **Enable the managed account** (checkbox): If checked, the account will be enabled by LAPS. If unchecked, the account will be disabled by LAPS. **Randomize the name of the managed account** (checkbox): If checked, the Automatic account name (or name prefix) will be treated as a prefix; a suffix of eight random numbers will be added to it. The name will also be randomized every time the password is changed. If unchecked, the Automatic account name (or name prefix) will be treated as the account name.
Enable password encryption	If enabled, the password is encrypted before it is backed up to AD. If disabled, the password is not encrypted before it is backed up to AD. If not configured, the default value is Enabled. *This setting is only applicable when backing up the password to Active Directory.*

Enable password backup for DSRM accounts	If enabled, the Domain Controller’s DSRM account password will be managed and backed up to AD. If not configured, the default value is Disabled. *This setting is only applicable to Domain Controllers.*
Do not allow password expiration time longer than required by policy	If enabled, LAPS will adhere to the computer’s password settings policy and the password will be reset when the password has expired based on the computer’s password settings policy. The new expiration is then set so it adheres to the computer’s password settings policy. If disabled, the expiration of the password set by LAPS could exceed the requirement of the computer’s password settings policy. If not configured, the default value is Enabled.
Configure size of encrypted password history	If enabled, you can specify how many older encrypted passwords to store in AD. This must be a number from 0 – 12. This setting only applies when encrypted passwords are being backed up to AD. This setting may help out when reverting to a VM snapshot where an older password was in use at the time the snapshot was taken. The default value, if not configured, is 0.
Configure password backup directory	Determines where the password is backed up to. Options: • 0: Disabled • 1: Entra ID only • 2: Windows Server (on-prem) AD only The default value when not specified is 0 (the password will not be backed up).
Configure authorized password decryptors	When enabled, you will specify the user or group that is authorized to decrypt the encrypted password in AD. You must provide one of the following as the decryptor • The SID of the group or user • The name of the group or user in the following format: AUSTIN\<name> Warning: If the device cannot resolve the SID or name provided, the password will not be backed up. This setting only applies when encrypted passwords are being backed up to AD. The default value when not specified is the Domain Admins group. *This setting is only applicable when backing up the password to Active Directory.*

Post-authentication actions	Specify an action that will be triggered after the successful authentication of the account whose password is being managed. The available actions are: • Take no actions • Reset the password • Reset the password and logoff the managed account • Reset the password and reboot the device • Reset the password, logoff the managed account, and terminate any remaining processes *This fifth option is only applicable starting with 24H2 operating systems (Windows 11 24H2 and Server 2025).* Set the grace period to the time you want it to wait after the authentication before the action is triggered. The grace period must be set greater than 0; if set to 0 the action will not be triggered. The default behaviour, when this setting is disabled or not configured, is to reset the password and logoff the managed account after 24 hours. If you want it to take no action, enable this setting and select Take no actions.

Retrieving a LAPS Password from Active Directory

There are several methods to retrieve the LAPS password.

Using the Active Directory Users and Computers (ADUC) Console

1. Open the Properties for the computer.
2. Select the LAPS tab.
   loading.gif

   On the LAPS tab of the computer's Properties page:

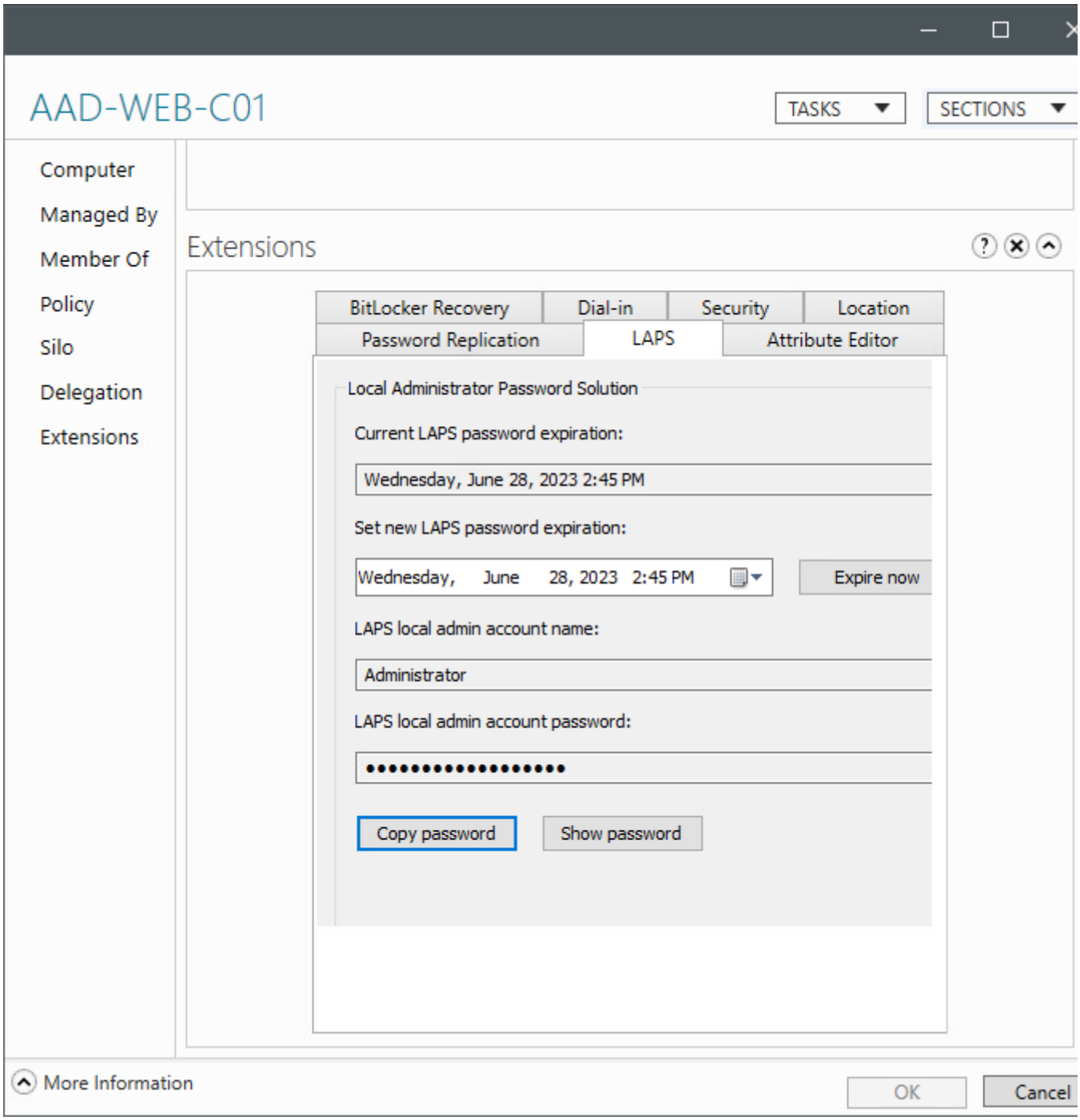
   - The Current LAPS password expiration is displayed.
   - You can specify a new password expiration.
     After specifying the new expiration click OK or Apply.

- You can make the password expire now by clicking on the Expire now button and then clicking on OK or Apply.
  This will set the expiration to the current date and time.
  The password will not actually be changed immediately on the computer, but when it next processes LAPS policy.
- The LAPS local admin account name is displayed.
- The LAPS local admin account password is masked by default
  - Clicking Copy password will put the clear-text password on your clipboard without unmasking it here.
  - Clicking Show password will display the password in clear text here.

Note: You cannot view the password history from here. You must use PowerShell to access the password history.

Using Active Directory Administration Center

1. Open the properties for the computer.
2. Scroll down to the Extensions.
3. Select the LAPS tab.



The LAPS tab is available just as it would appear in ADUC. Refer to the ADUC section above for details.

Using PowerShell

You can retrieve the LAPS password using the Get-LapsADPassword cmdlet.

1. Use the Get-LapsPassword cmdlet

```
PS C:\> Get-LapsADPassword -Identity aad-web-c01


ComputerName        : AAD-WEB-C01
DistinguishedName   : CN=AAD-WEB-C01,OU=Web,OU=AUS-Managed,OU=AAD-Servers,OU=A
Account             : Administrator
Password            : System.Security.SecureString
PasswordUpdateTime  : 6/21/2023 12:42:45 PM
ExpirationTimestamp : 6/28/2023 2:45:24 PM
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : CDS\AUSTIN-Directory-Admins
```

Get-LapsADPassword -Identity <computername>
will return the current password in a Secure String object.The Account property shows the managed account name.The Password property contains the password.The PasswordUpdateTime shows when the password was updated.The ExpirationTimestamp shows when the current password expires/when a new password will be required.The DecryptionStatus property will show Success if you are allowed to decrypt the password. It will show Unauthorized if you are not.The AuthorizedDecryptor property will show the user or group that can decrypt the password.Note: When using tab-completion it is easy to accidentally run the Get-LapsAADPassword instead. This is the cmdlet used to retrieve the password from Azure Active Directory.

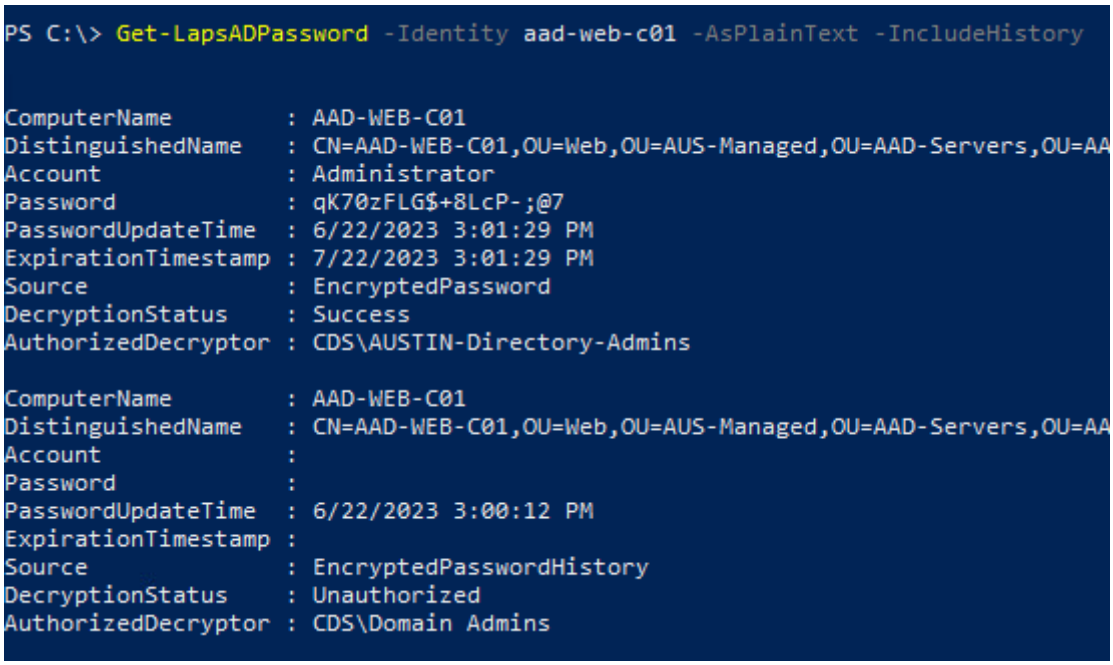
2. Or to get the password in plain text

```
PS C:\> Get-LapsADPassword -Identity aad-web-c01 -AsPlainText


ComputerName        : AAD-WEB-C01
DistinguishedName   : CN=AAD-WEB-C01,OU=Web,OU=AUS-Managed,OU=AAD-Servers,OU=A
Account             : Administrator
Password            : eodpMVV6b)Y%P6@,M7
PasswordUpdateTime  : 6/21/2023 12:42:45 PM
ExpirationTimestamp : 6/28/2023 2:45:24 PM
Source              : EncryptedPassword
DecryptionStatus    : Success
AuthorizedDecryptor : CDS\AUSTIN-Directory-Admins
```

Get-LapsAdPassword -Identity <computername> -AsPlainText
will return the current password in plain text.

3. Or to get the password history in plain text



Get-LapsAdPassword -Identity <computername> -AsPlainText -IncludeHistory
will return the password history in plain text
The number of passwords in the password history depends on the LAPS policy applied and how many times the password has been changed by LAPS.
Each password in the password history can have a different Authorized Decryptor, depending on what was specified in the policy when the password was encrypted and stored in AD.The AuthorizedDecryptor shows who can decrypt the password.
The DecryptiomStatus shows whether the password was successfully decrypted for the user running the cmdlet.In this example, the user running the cmdlet can see the latest password as they are a member of the Authorized Dectryptors. They cannot see the previous password as the Authorized Dectryptors for it is a different group that the user is not a member of.

Windows Event Log

A new Windows Event Log channel has been created for Windows LAPS.

In Event Viewer, navigate to: Application and Services Logs – Microsoft – Windows – LAPS – Operational.

PowerShell Module

Below are some helpful cmdlets included in the LAPS PowerShell module.

Cmdlet	Description
Get-LapsAdPassword	Gets the escrowed password(s) from Active Directory. Review the Retrieving a LAPS Password section above for details and examples.
Invoke-LapsPolicyProcessing	Initiates the processing of the current LAPS policy, independent of the hourly processing cycle).
Reset-LapsPassword	Attempts to immediately change the managed account's password (whether or not it has expired).

Frequently Asked Questions

Q1: Can I initiate a password change ahead of the expiration time?

A1: There are a couple of ways to have the managed password changed:

- Use the Reset-LapsPassword cmdlet, which will result in LAPS attempting to reset the password immediately.
- Edit the password expiration for the computer to the current time, which will result in the password being reset the next time LAPS policy is processed on the computer.

Q2: What happens if the computer cannot reach a Domain Controller when the password expires? Will the password be set without the new password being backed up in AD?

A2: As with legacy LAPS, Windows LAPS will first escrow the new password in Active Directory. Only if that is successful with the password actually be changed on the computer.

Q3: Who can decrypt an encrypted password in Active Directory?

A3: This is specified by the user or group set as the authorized password decryptors in the LAPS policy at the time the password was stored in AD.

Is this setting was not set, the decryptors default to the Domain Admins.

Q4: What happens to the password and password expiration stored in Active Directory when Windows LAPS manages the password?

A4: The attributes used by legacy LAPS are not modified by Windows LAPS. After Windows LAPS starts to manage the account's password the legacy LAPS attributes will remain intact. Windows LAPS does not clear out the Legacy LAPS attributes.
This can be confusing, having two sets of password attributes, but you should avoid

programmatically clearing out all of the legacy LAPS attributes on all of your computers without verifying they are no longer valid. You could be clearing out currently-set passwords making them unavailable (Windows LAPS is not available for Windows Server 2016 which will continue to use legacy LAPS if enabled. Windows LAPS may not have changed the password yet if there is no Windows LAPS policy assigned to the computer).

Q5: What will happen if a computer has both a legacy LAPS and Windows LAPS policy applied to it?

A5: Windows LAPS will manage the password.

Q6: Will Windows LAPS save both an unencrypted and encrypted password to AD?

A6: No, Windows LAPS will store only an encrypted password or unencrypted password based on the computer's policy settings.

Q7: What will happen if the account I specify as the Name of administrator account to manage does not exist?

A7: Windows LAPS policy processing will fail. It can not manage an account that does not exist. This scenario can lead you to being locked out of the computer / not having a way to get admin access to it.

Q8: What will happen if the account I specify as the Name of administrator account to manage is disabled?

A8: Windows LAPS policy processing will succeed. It will manage the account's password, but it will not enable the account. The account must be enabled before it can be used. This scenario can lead you to being locked out of the computer / not having a way to get admin access to it.

Q9: What will happen if the account I specify as the Name of administrator account to manage is not a member of the local Administrators group?

A9: Windows LAPS policy processing will succeed. It will manage the account's password, but it will not add it to the Administrators group. This scenario can lead you to being locked out of the computer / not having a way to get admin access to it.

Q10: Can the password of more than one account be managed by Windows LAPS?

A10: No, only one account can be managed.

Q11: Should I remove (delete or unlink) my GPO(s) that configure Legacy LAPS?

A11: To "clean things up", you can unlink or delete any GPOs that configure Legacy LAPS as long as you do not have any computers running an operating system that Windows LAPS is not available on. If you need to keep using Legacy LAPS for older operating systems, you can optionally use filtering (security filtering or WMI filtering) on the GPO to have it only apply to these computers – although you do not need to do anything as Windows LAPS will manage the password in the

scenario where Windows LAPS and Legacy LAPS are both enabled.

Revision #3
Created 2025-03-26 16:54:29 UTC by Ryan
Updated 2025-03-26 16:57:21 UTC by Ryan