LAPS Active Directory Tool Permissions

Last Modified on 05.16.23

Indications

When attempting to read the LAPS AD password with the AD LAPS Password Tool, you might receive the error **No LAPS Password Found**, or the LAPS password tool returns no results (the results sections are empty).

Probable Cause

When the LAPS Tool is implemented in your environment, two new attributes are created. ms-mcs-AdmPwd (which contains the Password) and ms-mcs-AdmPwdExpirationTime (which contains the password expiration time).

The AD LAPS Password Tool requires the ability to read the two attributes to identify the password and expiration time, and will need to be able to change the value in ms-mcs-AdmPwdExpirationTime to force a password reset.

Resolution

There are two commands that you should run from an administrative PowerShell prompt. The PowerShell commands are added when you install the LAPS software (full admin install). To start the session you should add the LAPS modules by typing Import-Module AdmPwd.ps

- **Set-AdmPwdReadPasswordPermission -OrgUnit ",OU=Units,DC=ad,DC=uoregon,DC=edu" -AllowedPrincipals**
  Updates the permissions of all computer objects in the target OU to allow entered AD User/Group to read the LAPS attributes of computer objects.

- **Set-AdmPwdResetPasswordPermission -OrgUnit ",OU=Units,DC=ad,DC=uoregon,DC=edu" -AllowedPrincipals**
  Updates the permissions of all computer objects in the target OU to allow the entered AD User/Group to reset the LAPS attributes of computer objects.