Recast

Permission Issues

Last Modified on 12.02.25

Indications of Insufficient Permissions

Recast permissions, as well as Microsoft permissions, determine a user's access to Right Click Tools actions as well as their ability to run an action within a given limiting rule. Recast permissions will not override Microsoft permissions.

> If a user has **insufficient Recast permissions** to run an action, the tool will be greyed out.
> If a user has the required Recast permissions, but **insufficient Microsoft permissions**, to run an action, the tool will appear to be available (not greyed out) but the action won't run successfully.

For more information, see Insufficient Recast Permissions.

LAPS Active Directory Tool Permissions

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.

MBAM Active Directory Tool Permissions

Recast

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 without 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.

Windows Defender Attack Surface Reduction Exclusions Required

Indications

You may see an error message similar to this:

"ASR rule 'Block process creations originating from PSExec and WMI commands' is enabled and can block this tool from performing network validation if no exclusion is set"

Probable Cause

Windows Defender ATP (ASR) can sometimes prevent Right Click Tools from functioning as intended.

Resolution

Add the following items to the list of exclusions for Windows Defender ASR

- C:\Windows\System32\schtasks.exe
- C:\windows\System32\wbem\WmiPrvSE.exe
- C:\Windows\System32\msiexec.exe
- %ProgramFiles(x86)%\Recast Software\Recast Agent\recastagent.exe
- %ProgramFiles(x86)%\Recast Software\Recast RCT\Right Click Tools Desktop.exe

Recast

Zscaler Implementation Without Recast Agents

A default Zscaler implementation will not work correctly with Right Click Tools.

To use Right Click Tools with Zscaler from a user-configured ZPA to ZPA connection, and without deploying Recast Agents, you'll need to modify the Client Hostname Validation setting in your Zscaler portal.

To configure Zscaler to work with Right Click Tools:

1. In your Zscaler portal, navigate to **Administration** > **Application Segments**.

2. Click **Client Hostname Validation**.

3. On the page that opens, update your regular expression to **.*.<yourdomain.com>** and save your changes.