## Introduction

This guide will help you understand the permissions required for Right Click Tools to function, and how these permission groups relate to one another.

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Overview of Permissions:</td>
<td>3</td>
</tr>
<tr>
<td>Client Actions</td>
<td>4</td>
</tr>
<tr>
<td>Security Tools: AD LAPS Password</td>
<td>6</td>
</tr>
<tr>
<td>Security Tools: AD BitLocker Recovery Keys</td>
<td>7</td>
</tr>
<tr>
<td>Security Tools: BitLocker Status</td>
<td>8</td>
</tr>
<tr>
<td>Security Tools: MBAM BitLocker Recovery Keys</td>
<td>9</td>
</tr>
<tr>
<td>Console Tools: AD Security Groups</td>
<td>12</td>
</tr>
<tr>
<td>Console Tools: Connect to C$</td>
<td>14</td>
</tr>
<tr>
<td>Console Tools: Delete Devices from AD</td>
<td>17</td>
</tr>
<tr>
<td>Console Tools: Delete Device(s) from ConfigMgr</td>
<td>19</td>
</tr>
<tr>
<td>Console Tools: Group Policy Update</td>
<td>21</td>
</tr>
<tr>
<td>Console Tools: Interactive Command Prompt</td>
<td>22</td>
</tr>
<tr>
<td>Console Tools: Interactive PowerShell Prompt</td>
<td>24</td>
</tr>
<tr>
<td>Console Tools: Local Group Members</td>
<td>26</td>
</tr>
<tr>
<td>Console Tools: Manage Computer</td>
<td>27</td>
</tr>
<tr>
<td>Console Tools: Open Regedit</td>
<td>28</td>
</tr>
<tr>
<td>Console Tools: Ping System(s)</td>
<td>29</td>
</tr>
<tr>
<td>Console Tools: Run PowerShell Script</td>
<td>31</td>
</tr>
<tr>
<td>Console Tools: Running Processes</td>
<td>32</td>
</tr>
<tr>
<td>Console Tools: System Information</td>
<td>33</td>
</tr>
<tr>
<td>Running on a Single Device:</td>
<td>33</td>
</tr>
</tbody>
</table>
**Running on Multiple Devices:**

- Console Tools: Wake On LAN ................................................................. 35
- Console Tools: Cancel Pending Restart or Shutdown ..................................... 41
- Console Tools: Schedule Shutdown or Restart ............................................... 42
- Client Tools: Add Device(s) to Collection .................................................... 43
- Client Tools: Change Cache Size .................................................................. 44
- Client Tools: Clear Cache ............................................................................. 45
- Client Tools: Client Information .................................................................... 46
- Client Tools: Install Missing Software Updates .............................................. 48
- Client Tools: Open Client Installation Log File Folder .................................. 50
- Client Tools: Open Client Log File Folder .................................................... 53
- Client Tools: Refresh Updates Compliance State ......................................... 56
- Client Tools: Rerun Deployment .................................................................. 58
- Client Tools: Restart SMS Agent Host .......................................................... 60
- Client Tools: Run Client Check .................................................................... 61
- Client Tools: Stop ConfigMgr Client Activities ............................................. 62
- Client Tools: Show Collections Advanced .................................................... 63
- Client Tools: Repair Client .......................................................................... 64
- Client Tools: Uninstall SCCM Client ............................................................ 65
- User Tools: Change Password ...................................................................... 66
- User Tools: Enable or Disable Account .......................................................... 67
- User Tools: Run PowerShell Script ............................................................... 68
- User Tools: Security Groups ........................................................................ 69
- User Tools: Unlock Account ......................................................................... 71
- User Tools: User Devices ............................................................................. 72
- User Collection Tools: Add Users to Collection(s) ....................................... 73
- User Collection Tools: Remove Users From Collection(s) ............................ 74
Overview of Permissions:

Recast RCT uses a role-based permissions model. Permissions are assigned to roles, which are then assigned to users. Each permission corresponds to one or more actions that can be run in Recast RCT. Permissions are categorized into different groups, listed below.

- **Active Directory** - These actions interact with your Active Directory environment. Actions include AD queries, getting BitLocker and LAPS information, resetting user passwords, or changing group memberships.
- **Administration** - Actions in this plugin will make changes to your Recast RCT environment. They include permissions to modify roles, adding users to Recast, or changing settings.
- **BitLocker** - BitLocker actions will make changes to BitLocker encrypted drives on remote computers.
- **Composite Action** - These actions are created by RCT Builder and run by RCT Runner. These permissions will allow you to determine which users are allowed to launch RCT Builder and RCT Runner, and which RCT Builder actions they’re allowed to run.
- **ConfigMgr Client** - These permissions are for interacting with the ConfigMgr client on remote devices. Actions include the client actions (machine policy, software updates scan, etc), changing cache size, and repairing or uninstalling the client.
- **ConfigMgr Server** - Permissions in this group will give access to actions that interact with your ConfigMgr environment. Actions include retrieving content status, distributing content, and changing collection membership.
- **Filesystem** - Permissions for actions that interact with the remote filesystem, such as deleting a folder or creating a file.
- **Installed Software** - Permissions include listing software installed on a device or uninstalling a piece of software.
- **Lab Management** - Permissions related to the Lab Manager feature of Recast RCT
- **Local Actions** - Actions in this category are not run from within Recast RCT. Anything that is launched in a locally installed application will show up here, including Interactive Command Prompt, Interactive PowerShell Prompt, Manage Computer, etc.
- **MBAM** - Actions for interacting with your MBAM server. This includes looking up BitLocker recovery keys or TPM hashes.
- **Network** - Currently this houses the Ping Computer action.
- **PowerShell** - Permissions for running PowerShell scripts from within Recast RCT.
- **Registry** - Permissions in this plugin determine which remote registry actions a user is allowed to perform. These actions include creating subkeys and writing or reading values.
- **Scheduler** - Scheduler actions allow you to view or cancel jobs running in Recast RCT. This plugin has to do with the real time actions running on the server, not actions that have been scheduled to run in the future
- **Services** - These are permissions related to interacting with service on remote devices
- **System Information** - Miscellaneous actions that can be performed on remote devices.
- **Task Scheduler** - Permissions related to scheduling tasks to be run in the future in Recast RCT. This plugin will let you schedule Recast RCT actions to be run in the future.
- **Windows Task Scheduler** - These actions will let you schedule and delete tasks in Windows Task Scheduler on remote devices
- **WMI** - Permissions relevant to running WMI queries and WMI methods on remote devices
Client Actions

Permissions

Each client action has its own permission in the Client Tools plugin. For example, to give a user access to perform the Machine Policy Retrieval and Evaluation Cycle action, they would need to have the permission below.
Prerequisites

Client actions require that the device you're targeting has a working ConfigMgr client installed. Additionally, the user running the ConfigMgr console will need to have administrator access to the remote device (if using Recast RCT Community or a Recast Server in impersonation mode), and the remote WMI ports will need to be allowed through the firewall. If the "Ping Computer Before Running Tools" option is set, ICMP Echo will also need to be allowed through the firewall. If using a Recast Server with a service account, the service account will need administrator permissions on the remote device.
Security Tools: AD LAPS Password

### Permissions

AD LAPS Password requires the Get LAPS Passwords permission in the Active Directory plugin.

### Prerequisites

The AD LAPS Password tool requires the user running the action have permissions to the ms-MCS-adminpwd and ms-Mcs-AdmPwdExpirationTime attributes on the AD computer objects. This permission can be given using the AdmPwd.PS PowerShell module. If using a Recast server with a service account, the service account will need permissions to read those attributes.
Security Tools: AD BitLocker Recovery Keys

Permissions
The AD BitLocker Keys tool requires the List BitLocker Keys permission in the Active Directory plugin.

Prerequisites
The AD BitLocker Keys tool requires that the user running the action have permissions to view BitLocker information for the device in Active Directory. If a Recast Server is used with a service account, then the service account needs permission to view BitLocker keys on the AD object.
Security Tools: BitLocker Status

Permissions
This tool requires the BitLocker Status permission in the BitLocker plugin. The right click options within the tool require the corresponding server action (for example, Suspend BitLocker Volume is required for the Suspend BitLocker action).

<table>
<thead>
<tr>
<th>Role Permissions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Plugin</td>
</tr>
<tr>
<td>BitLocker Status</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Add TPM Key Protector</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Resume BitLocker Volume</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Suspend BitLocker Volume</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Decrypt Volume</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Encrypt Volume</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Backup Key Protector to Active Directory</td>
<td>BitLocker</td>
</tr>
<tr>
<td>Add Numerical Password Key Protector</td>
<td>BitLocker</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires local administrator permissions on the remote device. If using a Recast Server with a service account, the service account will need administrator permissions on the remote device.
Security Tools: MBAM BitLocker Recovery Keys

Permissions
This tool requires the "Get Recovery IDs for Device" and "Get Recovery Key" permissions in the MBAM plugin.

<table>
<thead>
<tr>
<th>Name</th>
<th>Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get Recovery IDs for Device</td>
<td>MBAM</td>
</tr>
<tr>
<td>Get Recovery Key</td>
<td>MBAM</td>
</tr>
</tbody>
</table>
Prerequisites
This tool requires read access to the MBAM Recovery and Hardware database as well as permission to request recovery keys from the MBAM web service. If using a Recast Server with service account, the service account will need read permissions to the MBAM Recovery and Hardware database as well as permission to request recovery keys from the MBAM web service. You must configure the relevant MBAM Plugin Settings in order for this action to work. If using Recast Server, this can be configured in the Recast Control Panel.
If using Recast Desktop Standalone, you can configure it in Configure Recast RCT.

Configure your Recast tools to optionally query the ConfigMgr SQL database directly for some actions. This should help with some WMI quota violation issues and may speed up some of the actions.

- SQL Server:
- SQL Database:

Configure your Recast tools to access to your MBAM Recovery and Hardware database to query RecoveryKeyIDs linked to a device for use in requesting recovery keys from the MBAM Administration Web Service.

- MBAM Administration URI: https://recast-mbam.recastsoftware
- SQL Server: recast-mbam.recastsoftware.local
- MBAM Recovery and Hardware DB: MBAM Recovery and Hardware
- MBAM Compliance Status DB: MBAM Compliance Status
Permissions
The AD Security Groups Tool requires the Query AD permission in the Active Directory plugin. Additionally, it requires the Add or Remove Account from Group permission in the Active Directory plugin if it’s desired to use the Add New Direct Group or Remove from Group features of the tool.
Prerequisites
The AD Security Groups tool requires that the user running the tool has permissions to look at the group memberships for the object in Active Directory. The user will also need permissions to modify the memberships of group objects in Active Directory if using that part of the tool. If using a Recast Server with a service account, the service account will need the permissions listed instead of the user running the tool.
Console Tools: Connect to C$

Permissions
The Connect to C$ tool requires the Open C$ Share permission in the Local Actions plugin.
Prerequisites
The Connect to C$ tool requires that the user running the console have permissions to browse the c$ share on the remote device. Typically this means the user requires administrator permissions on the remote device. Note that this is the case even if using a Recast Server with a service account because this action launches an application outside of Recast. If the user does not have permission, a prompt will open asking for a username and password to try to successfully connect to the remote device.

TCP445 needs to be allowed from the device running the ConfigMgr console to the device being connected to in order for this tool to function.

Additional information
This action is affected by the Windows Explorer setting in Configure Recast RCT. Specifying an alternative explorer shell will cause this tool to launch that application instead of Windows Explorer when trying to connect to the remote filesystem. When using the alternative shell Recast will not prompt for credentials if it detects the user does not have permission, it will let the alternative shell handle this scenario.
You can specify an alternate explorer shell to use when launching tools that connect to C$ shares or content tools. This can be useful to avoid UAC prompts when you launch the ConfigMgr console as a different user.

**Local Path:**

[Button: Browse]
Permissions
The Delete Device(s) from AD tool requires the Delete Account permission in the Active Directory plugin.
**Prerequisites**
This tool requires that the user has permissions to delete the object in Active Directory. If using a Recast Server with a service account, the service account will need permissions to delete the object in Active Directory.
Console Tools: Delete Device(s) from ConfigMgr

Permissions
The Delete Device(s) from ConfigMgr tool requires the Delete Device permission in the ConfigMgr Server plugin.
**Prerequisites**
The user running the tools will need the Delete Resource permission in ConfigMgr. If using a Recast Server with a service account, the service account will need the Delete Resource permission in ConfigMgr.
Console Tools: Group Policy Update

Permissions
The Group Policy Update tool requires the Group Policy Update permission in the System Information role.

Prerequisites
The user running this action will need to be an administrator of the remote device. If using a Recast Server with a service account, the service account will need to be an administrator of the remote device. This tool relies on remote WMI to start the Group Policy Update process.

Other Notes
Using the Update User Policy option will cause the users to see a command prompt pop up while the policy is updated.
Console Tools: Interactive Command Prompt

Permissions
This action requires the Interactive Command Prompt permission in the Local Actions plugin.

Prerequisites
This action requires local administrator permissions on the remote device for the user running the console. This action will not use the Recast Server service account. The Interactive Command Prompt tool requires you to download PsExec and configure your tools to point to it in Configure Recast RCT.
Interactive Command Prompt relies on PsExec to run. Please download it and find the file with the browse button. If you already have it downloaded, you can just browse for it.

Local Path: [Browse]
Console Tools: Interactive PowerShell Prompt

Permissions
This action requires the Interactive PowerShell Prompt permission in the Local Actions plugin.

Prerequisites
This action requires you have administrator permissions on the remote device. This action will not use the Recast Server service account when using a Recast Server.

Other Notes
This tool requires PSRemoting be enabled on the remote device. If PSRemoting is not enabled, the tool will prompt to enable it.
Enable PSRemoting?

PSRemoting is not enabled on NM-RECAST2
Do you want to enable PSRemoting?

[Yes] [No]
Permissions
This action requires the Read Only permission in the System Information plugin. If the user needs to update the group membership from within this tool, they will also need the Update Local Group Membership permission from the System Information plugin.

Prerequisites
This tool requires administrator permissions on the remote device. If using a Recast Server with a service account, the service account will need administrator permissions on the remote device.
Console Tools: Manage Computer

Permissions
This action requires the Manage Computer permission in the Local Actions plugin.

Prerequisites
You must be a local administrator on the remote device to run this tool. The action will not use the Recast Server service account.
Console Tools: Open Regedit

Permissions
This action requires the Open Regedit permission in the Local Actions plugin.

Prerequisites
The action requires local administrator permissions on the remote device. Additionally, it requires that the remote registry service be enabled. This action does not use the Recast Server service account.
Console Tools: Ping System(s)

Ping System(s)

Recast

Complete!

2 Successful

0 Unsuccessful

<table>
<thead>
<tr>
<th>Computer Name</th>
<th>Host Name</th>
<th>Reply F</th>
</tr>
</thead>
<tbody>
<tr>
<td>NM-RECAST2</td>
<td>NM-RECAST2.nowmico.local</td>
<td>10.6.1.6</td>
</tr>
<tr>
<td>NM-RECAST1</td>
<td>NM-RECAST1.nowmico.local</td>
<td>10.6.1.6</td>
</tr>
</tbody>
</table>

Log

<table>
<thead>
<tr>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/10/2018 11:08:04 AM</td>
<td>Started</td>
</tr>
<tr>
<td>4/10/2018 11:08:05 AM</td>
<td>NM-RECAST2 was successful</td>
</tr>
<tr>
<td>4/10/2018 11:08:05 AM</td>
<td>NM-RECAST1 was successful</td>
</tr>
<tr>
<td>4/10/2018 11:08:05 AM</td>
<td>Complete!</td>
</tr>
</tbody>
</table>

What's the difference between RCT Free and RCT Enterprise?
Permissions
Ping System(s) requires the Ping Computer permission in the Network plugin.

Prerequisites
Ping System(s) requires ICMP echo to be allowed through the firewall.
Console Tools: Run PowerShell Script

Permissions
This action requires the Run Function Against Computers permission in the PowerShell plugin.

Prerequisites
This action will likely require administrator permissions on the remote device, though it depends on the script.

Other Notes
The actions are stored on the Recast Server in the "C:\Program Files (x86)\Now Micro\Recast RCT Server\Server\App_Data\PowerShell\ComputerActions" folder. The functions listed in these scripts should take one or more computer names as input parameters and return a PowerShell command to be executed in parallel on all of the computer names passed in. The "C:\Program Files (x86)\Now Micro\Recast RCT Server\Server\App_Data\PowerShell\Scripts" folder houses functions that may be used by the ComputerActions scripts. Typically, a ComputerActions script will return a function from one of the scripts in the Scripts folder.
Console Tools: Running Processes

Permissions
This action requires the Get Running Process permission in the System Information plugin. It also uses the Kill Process permission in the System Information plugin to run the Kill Process right click option.

Prerequisites
This action uses remote WMI to list the processes and requires that the user running the tool is an administrator on the remote machine. If a Recast Server with a service account is used, the service account will need to have administrator permissions on the remote device.
Console Tools: System Information

Running on a Single Device:

Permissions
This action requires the Read Only permission in the System Information plugin. If the Add / Remove Programs tab is desired, the List Software permission under the Installed Software plugin is needed. If the Services tab is desired, the List Services permission in the Services plugin is needed. If the user needs to modify services, the Change Start Mode and Start / Stop / Restart Service permissions in the Services plugin are required. If the user needs to uninstall software from the Add / Remove Programs tab, the Uninstall Software permission from the Installed Software plugin is required. If the user needs to delete user profiles, the Delete Profile permission from the System Information plugin is required. If the user needs to remove local group members, the Update Local Group Membership from the System Information plugin is required.
Prerequisites
This tool requires local administrator permission on the remote device. If using a Recast Server with service account, the service account needs local administrator permission on the remote device. This action uses remote WMI and remote registry to gather data and perform actions on the remote machine.
Running on Multiple Devices:

Permissions
The System Information tool on multiple devices requires the Read Only permission in the System Information plugin.

Prerequisites
This action requires local administrator permissions on the remote devices. If using a Recast Server with service account, the service account needs local administrator permissions on the remote devices. This tool requires remote WMI access.

Other Notes
This tool can be customized using Configure Recast RCT on the System Information tab.
**Console Tools: Wake On LAN**

---

**Permissions**
This action requires the Wake on LAN permission in the ConfigMgr Server plugin.

---

**Prerequisites**
This action requires some setup in your environment. If using the subnet directed broadcast option, the routers in your environment will need to allow these types of packets from your Recast installations. If using a Recast Server, these packets will need to be allowed from the Recast Server. When using unicast
mode, some switches may need to be configured to forward UDP packets. This site has some details about the tradeoff of each option: https://technet.microsoft.com/en-us/library/bb632911.aspx

Wake on LAN settings can be configured in Configure Recast RCT.
If using a Recast Server, the Wake on LAN settings can be configured in the Recast Control Panel.

Other Notes
The ability to schedule Wake on LAN packets is available in Recast RCT Enterprise.
Scheduling Wake on LAN packets requires the Schedule Task permission in the Task Scheduler plugin.
Console Tools: Cancel Pending Restart or Shutdown

**Permissions**
This action requires the Cancel Shutdown permission in the System Information plugin.

![Successful dialog box](image)

**Prerequisites**
This action requires local administrator permissions on the remote devices. If using a Recast Server with service account, the service account will need local administrator permissions on the remote devices. This tool uses remote WMI.

**Other Notes**
This will only cancel shutdowns / restarts that are imminent. It will not clear shutdown / restart tasks in task scheduler.
Console Tools: Schedule Shutdown or Restart

Permissions
This action requires the Schedule Shutdown permission in the System Information plugin.

Prerequisites
The action requires local administrator permissions on the remote devices. If using Recast Server with a service account, the service account will need local administrator permissions on the remote device. This action uses remote WMI.

Other Notes
This tool will copy an executable to C:\Windows on remote devices when the "Give user a prompt to cancel" option is selected. Some antivirus vendors may block the execution of this application.
Client Tools: Add Device(s) to Collection

Permissions
This tool requires the Get All Device Collections and Add Devices to Collection permissions from the ConfigMgr Server plugin.

<table>
<thead>
<tr>
<th>Name</th>
<th>Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get All Device Collections</td>
<td>ConfigMgr Server</td>
</tr>
<tr>
<td>Add Devices to Collection</td>
<td>ConfigMgr Server</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires that the user running the tools has sufficient ConfigMgr permissions to add the device to the collection. If using a Recast Server with service account, the service account needs to have permissions to add the devices to the relevant collection.

Other Notes
The "Match on name instead of ResourceID" checkbox will query ConfigMgr for the Resource ID that matches the computer name. This is useful when launched from tools that may not have the Resource ID available (such as the ReLAPS or BitLocker Compliance tools).
Client Tools: Change Cache Size

Permissions
This tool requires the Change Cache Size permission in the ConfigMgr Client plugin.

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Clear Cache

Are you sure?

Are you sure you want to clear the cache?

Permissions
This action requires the Clear Cache permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Clear Cache</td>
</tr>
</tbody>
</table>

Prerequisites
This action requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permissions on the remote device. This tool uses remote WMI and connects to the c$ share.
**Client Tools: Client Information**

---

**Permissions**

This action requires the Client Information permission in the ConfigMgr Client plugin. If the user needs to start remote application installs or uninstalls from the Applications tab, this requires the Install Application and Uninstall Application permissions in the ConfigMgr Client plugin. If the user needs to change the cache size from the Cache tab, they will require the Change Cache Size permission in the ConfigMgr Client plugin. If the user needs to delete cache items from Cache tab, they will need the Remove Items From Cache permission in the ConfigMgr Client plugin.
**Prerequisites**

This action requires administrator permissions on the remote device and permission to look up boundaries in ConfigMgr. If using a Recast Server with service account, the service account requires administrator permissions on the remote device and permissions to look up boundaries in ConfigMgr. This tool uses remote WMI. Remote SMB is used when the Open in Explorer right click option is used from the Cache tab.
Permisssions
This action requires the Install Software Updates permission in the ConfigMgr Client plugin.
**Prerequisites**
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Open Client Installation Log File Folder

Permissions
This action requires the Open C$ Share permission in the Local Actions plugin.

Prerequisites
This action requires that the user running the console have permissions to browse the c$ share on the remote device. Typically this means the user requires administrator permissions on the remote device. Note that this is the case even if using a Recast Server with a service account because this action launches an application outside of Recast. If the user does not have permission, a prompt will open asking for a username and password to try to successfully connect to the remote device.
TCP445 needs to be allowed from the device running the ConfigMgr console to the device being connected to in order for this tool to function.

**Additional information**
This action is affected by the Windows Explorer setting in Configure Recast RCT. Specifying an alternative explorer shell will cause this tool to launch that application instead of Windows Explorer when trying to connect to the remote filesystem. When using the alternative shell Recast will not prompt for credentials if it detects the user does not have permission, it will let the alternative shell handle this scenario.
You can specify an alternate explorer shell to use when launching tools that connect to C$ shares or content tools. This can be useful to avoid UAC prompts when you launch the ConfigMgr console as a different user.

Local Path:  

[Browse button]
Client Tools: Open Client Log File Folder

Permissions
This action requires the Open C$ Share permission in the Local Actions plugin.

Prerequisites
This tool requires that the user running the console have permissions to browse the c$ share on the remote device. Typically this means the user requires administrator permissions on the remote device. Note that this is the case even if using a Recast Server with a service account because this action launches an application outside of Recast. If the user does not have permission, a prompt will open asking for a username and password to try to successfully connect to the remote device.
TCP445 needs to be allowed from the device running the ConfigMgr console to the device being connected to in order for this tool to function.

**Additional information**
This action is affected by the Windows Explorer setting in Configure Recast RCT. Specifying an alternative explorer shell will cause this tool to launch that application instead of Windows Explorer when trying to connect to the remote filesystem. When using the alternative shell Recast will not prompt for credentials if it detects the user does not have permission, it will let the alternative shell handle this scenario.
You can specify an alternate explorer shell to use when launching tools that connect to C$ shares or content tools. This can be useful to avoid UAC prompts when you launch the ConfigMgr console as a different user.

<table>
<thead>
<tr>
<th>Local Path:</th>
<th>Browse</th>
</tr>
</thead>
</table>

By Now Micro
Client Tools: Refresh Updates Compliance State

Permissions
This action requires the Refresh Updates Compliance State permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
<th>Plugin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refresh Updates Compliance State</td>
<td>ConfigMgr Client</td>
</tr>
</tbody>
</table>
Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Rerun Deployment

### Packages

<table>
<thead>
<tr>
<th>Package Name</th>
<th>Package ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Manager Client Upgrade Package</td>
<td>NM100003</td>
</tr>
</tbody>
</table>

### Task Sequences

<table>
<thead>
<tr>
<th>Package Names</th>
<th>Task Sequence ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot image (x64)</td>
<td>NM120014</td>
</tr>
<tr>
<td>Now Micro Default Lock Screen</td>
<td></td>
</tr>
<tr>
<td>OSD - OSDBackground</td>
<td></td>
</tr>
<tr>
<td>OSD - TPM Scripts</td>
<td></td>
</tr>
<tr>
<td>Dell Command Update</td>
<td></td>
</tr>
<tr>
<td>OSD - Set Start Menu and Taskbar Layout</td>
<td></td>
</tr>
<tr>
<td>Windows 10 x64 - Media</td>
<td></td>
</tr>
<tr>
<td>Configuration Manager Client Package</td>
<td></td>
</tr>
<tr>
<td>Firmware Updates - Dell Precision 5510</td>
<td></td>
</tr>
<tr>
<td>Now Micro Fonts</td>
<td></td>
</tr>
<tr>
<td>Firmware Configuration - Dell</td>
<td></td>
</tr>
<tr>
<td>Firmware Updates - Dell XPS 15 9560</td>
<td></td>
</tr>
<tr>
<td>OSD - Move Computer To Different OU</td>
<td></td>
</tr>
<tr>
<td>OSD - Reset LAPS Password</td>
<td></td>
</tr>
<tr>
<td>OSD - Windows 10 Unattend</td>
<td></td>
</tr>
<tr>
<td>Firmware Configuration - Lenovo</td>
<td></td>
</tr>
<tr>
<td>Dell XPS 13 9350 Win10 x64</td>
<td></td>
</tr>
</tbody>
</table>
Permissions
This action requires the Rerun Deployment permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Rerun Deployment</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Restart SMS Agent Host

Permissions
This action requires the Restart SMS Agent permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Restart SMS Agent</td>
</tr>
<tr>
<td>Plugin</td>
</tr>
<tr>
<td>ConfigMgr Client</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Run Client Check

Successful!

Successfully ran the client check on NM-RECAST2!

Permissions
This action requires the Run Client Check permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Run Client Check</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Stop ConfigMgr Client Activities

Successfully stopped ConfigMgr client activities on NM-RECAST2

Permissions
This action requires the Stop Client Activities permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Stop Client Activities</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.

Other Notes
Use the Run Client Check tool to revert the client to a working state.
Client Tools: Show Collections Advanced

Permissions
This action requires the Get Device Collection Information for Device permission in the ConfigMgr Server plugin. If the user needs to remove devices from the collection, they will also need the Remove Devices from Collection permission in the ConfigMgr Server plugin.

Prerequisites
This action requires the user has permissions in ConfigMgr console to read properties about collections and remove devices from a collection. If using a Recast Server with service account, the service account will need ConfigMgr console permissions to read properties of the collections and remove devices from the collection.
Client Tools: Repair Client

Successful!

Successfully started the client repair on NM-RECAST2!

Permissions
This action requires the Repair Client permission in the ConfigMgr Client plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Repair Client</td>
</tr>
</tbody>
</table>

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
Client Tools: Uninstall SCCM Client

Permissions
This action requires the Uninstall Client permission in the ConfigMgr Client plugin.

Prerequisites
This tool requires administrator permission on the remote device. If using a Recast Server with service account, the service account needs administrator permission on the remote device. This tool uses remote WMI.
User Tools: Change Password

Permissions
This action requires the Reset Password permission in the Active Directory plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Reset Password</td>
</tr>
</tbody>
</table>

Prerequisites
This action requires reset user password permissions on the Active Directory object. If using a Recast Server with service account, the service account needs the reset user password permissions on the AD object.
User Tools: Enable or Disable Account

Are you sure?

SMS-TestUser-1019 is disabled. Do you want to enable the account?

Permissions
This action requires the Enable or Disable Account permission in the Active Directory plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Plugin</td>
</tr>
<tr>
<td>Enable or Disable Account</td>
</tr>
</tbody>
</table>

Prerequisites
This action requires permissions to enable or disable the Active Directory object. If using a Recast Server with service account, the service account needs permission to enable or disable the AD object.
User Tools: Run PowerShell Script

Permissions
This action requires the Run Function Against Users permission in the PowerShell plugin.

Prerequisites
This action will require the user has permissions to do the actions in the script. If using a Recast Server with service account, the service account will need to have permissions to run the actions in the script.

Other Notes
The actions are stored on the Recast Server in the "C:\Program Files (x86)\Now Micro\Recast RCT Server\Server\App_Data\PowerShell\UserActions" folder. The functions listed in these scripts should take one or more user names as input parameters and return a PowerShell command to be executed in parallel on all of the user names passed in. The "C:\Program Files (x86)\Now Micro\Recast RCT Server\Server\App_Data\PowerShell\Scripts" folder houses functions that may be used by the UserActions scripts. Typically, a UserActions script will return a function from one of the scripts in the Scripts folder.
User Tools: Security Groups

Permissions
This action requires the Query AD permission in the Active Directory plugin. Additionally, it requires the Add or Remove Account from Group permission in the Active Directory plugin if it's desired to use the Add New Direct Group or Remove from Group features of the tool.
Prerequisites
This action requires that the user running the tool has permissions to look at the group memberships for the object in Active Directory. The user will also need permissions to modify the memberships of group objects in Active Directory if using that part of the tool. If using a Recast Server with a service account, the service account will need the permissions listed instead of the user running the tool.
User Tools: Unlock Account

Success

Successfully unlocked account

Permissions
This action requires the Unlock permission in the Active Directory plugin.

<table>
<thead>
<tr>
<th>Role Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Unlock Account</td>
</tr>
</tbody>
</table>

Prerequisites
This action requires unlock account permissions on the Active Directory object. If using a Recast Server with service account, the service account needs the unlock account permissions on the AD object.
User Tools: User Devices

Permissions
This action requires the Get User Devices permission in the ConfigMgr Server plugin.

Prerequisites
This action requires the user have permissions in the ConfigMgr console to read the SMS_UserMachineRelationship and SMS_G_System_Console_User in WMI. The built-in Read-only analyst role in ConfigMgr has all of the permissions required to perform this action.
User Collection Tools: Add Users to Collection(s)

Permissions
This tool requires the "Add Users to Collection" permission in the ConfigMgr Server plugin.

Prerequisites
This tool requires permission to modify the memberships of the selected collections. If using a Recast Server with service account, the service account needs permission to modify the memberships of those collections.
**User Collection Tools: Remove Users From Collection(s)**

![User Collection Tools](image)

**Permissions**
This tool requires the "Remove Users from Collection" permission in the ConfigMgr Server plugin.

![Role Permissions](image)

**Prerequisites**
This tool requires permission to modify the memberships of the selected collections. If using a Recast Server with service account, the service account needs permission to modify the memberships of those collections.