Right Click Tools Roles

Last Modified on 05.22.24

Right Click Tools with Recast Management Server lets you set up role-based permissions that use Active Directory users or groups to grant or limit access to specific actions.

Administrator Role

You can grant users and groups Recast permissions by assigning an administrator role. Your Recast software must be connected to Recast Management Server to set up role-based permissions.

Add Active Directory User or User Group

To add an AD user or user group:

1. In your Recast Management Server, navigate to **Administration** > **Permissions**.

2. In the main window, click **Add User** or **Add Group**.

3. In the window that opens, search for your AD name or AD user group and click the **Add** button.

NOTE: You can include a **wildcard (*)** to facilitate your search.

Wildcard examples:

- **John Connor** returns strings that match exactly
- **John C*** returns strings beginning with 'John C', such as '**John C**onnor', '**John C**onnors', and '**John C**ranston'
- ***Connor** returns strings ending with 'Connor', such as 'John **Connor**' and 'Carol O'**Connor**'
- ***Support*** returns strings that include 'Support' plus whatever is on the left and right, such as 'Customer **Support** Team' and 'Enterprise **Support** Group'

Assign User a Role

A user must be assigned at least one role.

To assign a user an administrator's role:

1. On the **Permissions** page, click the Edit icon to the right of the user.

2. Under **Role Assignments**, select **Administrators**.

3. To limit the user's permissions to a set of devices, enable **Limit this user to specific objects** and select a **Service Connection**.

4. If desired, set a specific **Refresh Interval** for repopulating scopes. A longer interval uses fewer resources but also detects new users and devices less frequently.

5. Click **Save**.

Read Only Access Role

Read-only access lets users view Right Click Tools actions, console dashboards, web dashboards and trends, and the audit log, without the ability to make changes to any devices. Users given this role will not see permissions, routes, or scopes in the Recast Management Server interface. For the full permission list, see below.

You can add a permissions template to Recast Management Server by running a simple SQL query against your RecastManagementServerDB.

Template (updated November 9, 2023): RMS Read-Only Role Query.txt

Video Walkthrough

Read-Only Role Permission List

Active Directory	Active Directory Cleanup Tool
	Get AD Computer
	Get AD Computer With LAPS Data
	Get AD Computers

	Get AD Computers BitLocker Status
	Get AD Computers In Group
	Get AD Containers
	Get AD Group
	Get AD Groups
	Get AD Groups In Group
	Get AD OUs
	Get AD User
	Get AD Users
	Get AD Users In Group
	Get Account Group Membership
	Get BitLocker Recovery Data
	Get Group Members
	Get Primary Group For Account
	Is Account Enabled
	Search AD Computers
	Search AD Groups
	Search AD Users
Administration	Get All Settings
	Get Action Execution Group
	Get Active Directory Service Connection
	Get Execution History
	Get Execution History For Job ID
	Get MEMCM Service Connection
BitLocker	Get BitLocker Status
	Get Recovery Password From Device
ConfigMgr Client	Get Configuration Baselines
	Get Deployed Programs
	Get Deployed Task Sequences
	Get Device ID
	Get Service Windows
	Get User Policy Endpoint
	Missing Software Updates
	Package Information

ConfigMgr Server	Get Accounts
	Get Active Alerts
	Get Active Directory Forests
	Get Administrative Users
	Get Alert Subscriptions
	Get All Alerts
	Get All Collections
	Get All Content Status
	Get All Deployment Types
	Get All Device Collections
	Get All Devices
	Get All Devices In OU
	Get All Distributed Content
	Get All Software Updates
	Get All User Collections
	Get All Users
	Get Application By Model ID
	Get Application Revisions
	Get Applications
	Get Applications Deployed To Users
	Get Approval Requests
	Get Asset Intelligence Catalog
	Get Asset Intelligence Hardware Requirements
	Get Asset Intelligence Inventoried Software
	Get Automatic Deployment Rules
	Get Baseboard Information
	Get Boot Images
	Get Boundaries
	Get Boundary Groups
	Get Category Instance By ID
	Get Certificates
	Get Chassis Information
	Get Client Operations
	Get Client Settings
	Get Collection Folder Information
	Get Collection Variables for Device

Get Collections for Device
Get Collections for User
Get Compliant Update Statuses
Get Component Status
Get Computer System Information
Get Computer System Product Information
Get Computer Warranty
Get Computers With X64 Laps Client
Get Computers With X86 Laps Client
Get Computers Without Laps Client
Get Configuration Baselines
Get Configuration Items
Get Conflicting Records
Get Content Status
Get DP Group Task Sequence Content
Get DP Groups With Members
Get Deployed Applications For User
Get Deployment Packages
Get Deployment Types For Application
Get Deployments
Get Device Collection Folders
Get Device Collection Information for Device
Get Device Collection Members
Get Device Collections in Folder
Get Device Count For Licensing
Get Devices By Creation Date
Get Devices By MAC Address
Get Devices By Sm Bios Guid
Get Devices In Collection Scope
Get Devices In Site Scope
Get Discovery Methods
Get Distributed Software Updates
Get Distribution Point Configuration Status
Get Distribution Point Content
Get Distribution Point Group Status
Get Distribution Point Group Status for Package
Get Distribution Point Groups

Get Distribution Point Status for Package
Get Distribution Points
Get Distribution Points In Distribution Point Group
Get Driver Packages
Get Drivers
Get Endpoint Protection Antimalware Policies
Get Endpoint Protection Firewall Policies
Get Failed Content On Distribution Point
Get Global Conditions
Get Installed Software Updates
Get Machines With Cm Blm Keys
Get Malware Detected
Get Migration Jobs
Get Non Compliant Update Statuses
Get Object Container Items
Get Operating System Images
Get Packages
Get Power Configurations for Computer
Get Queries
Get Required Software Updates
Get Scope Memberships
Get Security Roles
Get Security Scopes
Get Servers and Site System Roles
Get Service Windows for Computer
Get Site Device Collections With Folders
Get Site Status
Get Sites
Get Software Metering Rules
Get Software Update Groups
Get Software Updates In Group
Get Status Message Queries
Get System Bios Information
Get System Console Usage Data
Get System Firmware Status
Get System Operating System Information
Get Systems BitLocker Encryption Status

	Get Task Sequence Content
	Get Task Sequences
	Get Unknown Devices
	Get User Collection Folders
	Get User Collections in Folder
	Get User Devices
	Get User Devices By Username
	Get User State Migrations
	Get Virtual Hard Disks
	Get Warranty Information
Endpoint Insights	Open Recast EI Report Viewer
Filesystem	Get Directory Entries
	Get Directory Entries
	Get Security By Name
Installed Software	List Software
Kiosk Manager	List Profiles
Local Actions	Active Directory Cleanup Tool
MBAM	Get MBAM Compliance
	Get MBAM Compliance For All Machines
	Get Machines With MBAM Keys
	Get Machines With MBAM Keys_v2
	Get Recovery Keys For Device
	Get TPM Hash
	Get TPM Hash For User
Network	Ping Computer
Registry	Get Value
	List Hives
	List Subkeys
	List Values

SCEP	Get Defender Exclusions
	Get Defender Status
Services	List Services
System Information	Get All Local Group Members
	Get Battery Information
	Get Logged In Users
	Get Running Processes
	Get User Sessions
	Read Only
Task Scheduler	Get Task Results
	Get Task Results For Date
Unified Write Filter	Get File Exclusions
	Get Overlay Configuration
	Get Registry Exclusions
	Get Unified Write Filter Feature Status
	Get Write Filter Status
Windows Security	Get All Virtualization Based Security Settings
	Get Credential Guard Settings
	Get Secure Boot Status
	Get System Guard Secure Launch Settings
	Get TPM Status
	Get UEFI Secure Boot Status
	Get Virtualization Based Security Settings
	Get Windows Firewall Profiles
	Get Windows Firewall Rules
Windows Task Scheduler	List Tasks
WMI	Read Only

Custom Role Templates

We've created these role templates as starting point for creating custom permission sets for Right Click Tools users. They are designed to be quickly added in Recast Management Server and can then be adjusted to fit your needs by adding or removing individual permissions.

Add a Permission Template to Recast Management Server

You can add a permission template to your Recast Management Server running a simple SQL query against your RecastManagementServer database.

To add a permission template in RMS:

1. Open SQL Server Management Studio (SSMS).

2. Expand the **Databases** folder.

3. Right-click on **RecastManagementServer**.

4. Select **New Query** from the drop-down menu.

5. Copy the template file (available below) and paste it into the main window in SSMS.

6. **Execute** the action.

In the Recast Management Server interface, the **Permissions** page should display a new Recast Role. You can click **Permissions** to the right of the role to view and/or change the specific permissions associated with the role.

Video Walkthrough

Custom Permission Templates

Read Only Access

This template will create a custom role called "ReadOnly" and grant users read access to all of the tools and Recast Management Server Web Dashboards.

SQLNewRMSReadOnlyAccessRole.txt

Remote Software Center

This template will create a custom role called "RemoteSoftwareCenter" and grant users access to all of the actions within Remote Software Center.

SQLNewRMSRemoteSoftwareCenterRole.txt

Content Distribution Monitor

This template will create a custom role called "ContentDistributionMonitorDashboard" and grant users access to all of the actions within the Content Distribution Monitor.

SQLNewRMSContentDistributionMonitorDashboardRole.txt

Scopes

Recast Scopes are lists of devices. Beginning with Recast Software Version 5.0, scopes are created automatically in the background when you create a route or limit user permissions to a set of devices. A user assigned a role and its associated permissions will automatically be allowed to perform tasks within a specific scope, which may include certain devices, users, AD OUs, or AD groups.