

Permissions

Last Modified on 11,27,25

Create role-based permissions for Privileged Access.

Assign Administrator Role

Before an administrator can manage access rights using Privileged Access, they'll need to be added as a user in Recast Management Server and assigned a Recast role.

Add an 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 Recast Users section, click Add User or Add Group.

Recast Users



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

NOTE: By default, the search is limited to the users or groups in the same domain as your Recast Management Server.

Using 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 Connor', 'John Connors', and 'John Cranston'
- *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 a User a Role

Each user must be assigned at least one role.

To assign a user a role:

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



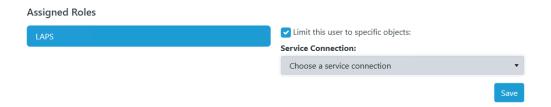
Recast Users

				Add	User Add Gr	oup
Name	•	Identifier T	Is Group	T	Actions	
Administrators		1-1-1-21-WHITHING-WIGHER TOUTS THE	True		/ 📋	^
Low Permission User		1/1-1/27-49931668-19921678-1297431130-1292	False		/	
н н н						

2. In the Role Assignments window that opens, under Roles, select a role to assign to the user/group.

To learn about the individual permissions granted by a role, see View or Edit User Role Permissions.

3. Under Assigned Roles, enable Limit this user to specific objects and select a Service Connection to add a limiting rule that restricts user permissions to a set of devices (optional). To learn more, see Limiting Rules.



4. Click Save.

NOTE: Beginning with Recast Software Version 5.9.2502.2105, you no longer have to set a **Refresh Interval** to repopulate your limiting rules (formerly known as scopes). The scheduled Discovery Sync will keep your service connection data up to date.

View Administrator Permissions

You can view the full set of permissions granted to users assigned an Administrator role for Privileged Access.

To view Privileged Access admin role permissions:

- 1. On the Permissions page, click Permissions to the right of the Administrators role.
- 2. In the Role Permissions window, expand the Privileged Access (previously Privilege Manager) section.

Full list of admin role permissions: Privileged Access Role Permissions.pdf @

API Permissions

Set up the following Application permissions in the Microsoft Graph API to access all Right Click Tools Privileged Access features:



Λ	nn	lication	narm	100	ione
$\overline{}$	\sim	lication	DELLI	100	10113

- Device.Read.All
- GroupMember.Read.All
- User.Read.All

For	instructions	on adding	API	permissions,	see Set U	Jp I	Entra I	D	for	Privil	eged	Access.
-----	--------------	-----------	-----	--------------	-----------	------	---------	---	-----	--------	------	---------

For the full list of Graph API permissions required for features in the Right Click Tools suite, see API Permissions by Product/Add-On.