Quest® Nova

Getting Started Guide for Delegation and Policy Control for Delegated Administrators

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Legend

CAUTION: A caution icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, NOTE, TIP, MOBILE OR VIDEO: An information icon indicates supporting information.

Quest® Nova
Updated March 2025

Contents

Introduction to Delegation and Policy Control **4**

Roles in Nova DPC **5**

Delegated Administration **7**

Manage **9**

- Users 9
- Contacts 11
- Mailboxes 13
- Groups 14
- Teams 16
- Devices 18
- Custom PowerShell 19

Policy Examples **20**

- Reset a User's Password 20
- Set an Out of Office message 20
- Create a new Team Channel 21

1

Introduction to Delegation and Policy Control

Quest Nova provides granular Delegation and Policy Control for Microsoft 365, enabling you to assign pre-defined roles and responsibilities to specific users, such as help desk operators, country-level administrators, or end-users. Nova also includes policy-based automation for authorization, service configuration and license assignment.

This guide to help you get started with Delegation and Policy Control as a delegated administrator. This includes:

- overviews of the Manage and Manage Administration tabs
- examples of actions that can be completed by a delegated administrator

For a more in-depth guide on using Quest Nova, please click here to view the Nova technical documents. In the *Quest Nova User Guide*, you will see more information on:

- Custom PowerShell execution and delegation
- additional policy examples
- more actions for delegated administrators

It is recommended that you undertake Nova training before using the application to get a better understanding of the platform. To sign up to Nova learning, click here.

To access Delegation and Policy Control, you will need a subscription to Nova that includes support for management, and support will provision your organization during the on-boarding process.

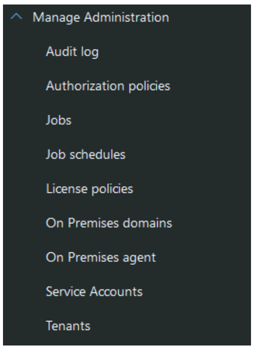
2

Roles in Nova DPC

Users of the Nova application can be assigned one or more roles. Each role provides functionality in the Nova application itself. Roles can be combined. The following is a list of the roles, and what they give access to:

Account Administrator

This gives access to be able to create and manage policies in Delegation and Policy Control. In addition, audit logs can be viewed to see how the policies have been used by delegated administrators. There are several other administrative functions which are shown in this screenshot:



Auth Policy Admin

This gives users the ability just to manage authorization policies within Nova. The option to get into Authorization Policies will be enabled in the **Manage Administration** menu.

Auth Policy administrators also have the ability to delegate certain subsets of custom PowerShell commands to selected users, which can be organized in an organization unit hierarchy. It is advised that Auth Policy Admins create dedicated organizational units exclusively for PowerShell scripts.

Autopilot Classic

This role is most appropriate to assign to a delegated administrator. This gives access to be able to perform allowed actions against users, mailboxes, groups, contacts and Microsoft Teams. What the user will be able to do is governed by the policies which are applied to them and were configured by someone with at least the Account Administrator role.

Config Policy Admin

This gives users the ability just to manage configuration policies within Nova. The option to get into Configuration Policies will be enabled in the **Manage Administration** menu.

IT Administrators

This gives a user the ability to use Nova, but restricts them from changing the configuration or security of Nova itself.

License Admin

This gives people the ability to create and maintain License Policies. The option will be available on the **Manage Administration** menu.

Organizational Unit Admin

This gives users the ability to maintain virtual organizational units. The Tenants option will be available on the **Manage Administration** menu.

System Administrator

This role gives access to the Tenant Management System, and does not give any direct access to the Nova application (unless it is combined with other roles).

Examples of combining roles

If a user needs to be able to create authorization policies, and perform actions on customer tenants (such as password resets, maintaining groups, adding Microsoft Teams etc.), then they should be assigned these roles:

- Account Administrator
- Autopilot Classic

If someone needs to be able to access reporting data, and perform actions on customer tenants (such as password resets, maintaining groups, adding Microsoft Teams, and so on) then they should be assigned these roles:

- Autopilot Classic
- Radar Classic

Granting Account Administrator

The following should be considered when assigning roles

- The Account Administrator roles does not work on it is own. It needs to be combined with the Autopilot Classic role.

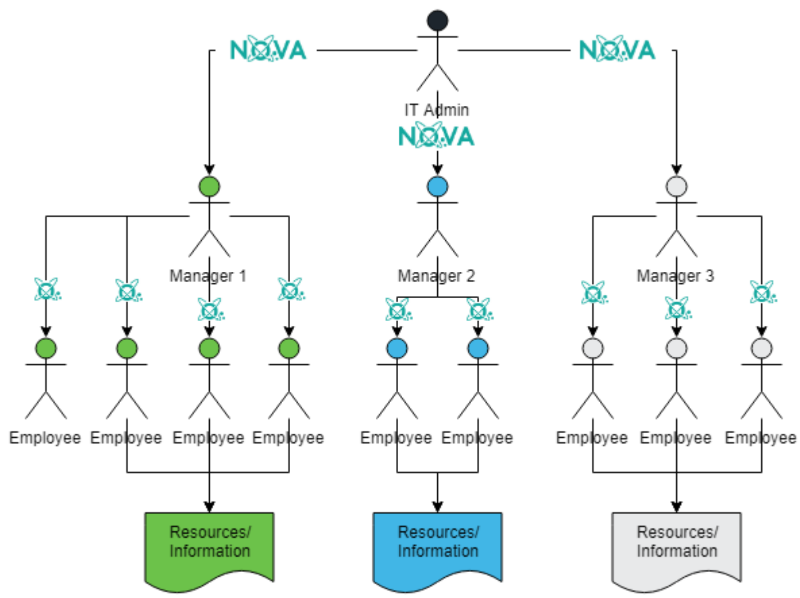
Delegated Administration

An administrator can authorize others within the organization to have specific delegated administrative rights. This section describes some ways rights might be delegated within an organization.

Managing direct reports

For example, an administrator could give sales managers the ability to manage certain attributes and/or rights of the individual sales team members without any additional rights granted either on-premises or in Microsoft 365 for those sales managers. Here is how it looks:

Example 1: IT Admin gives managers access to Nova to manage their direct reports

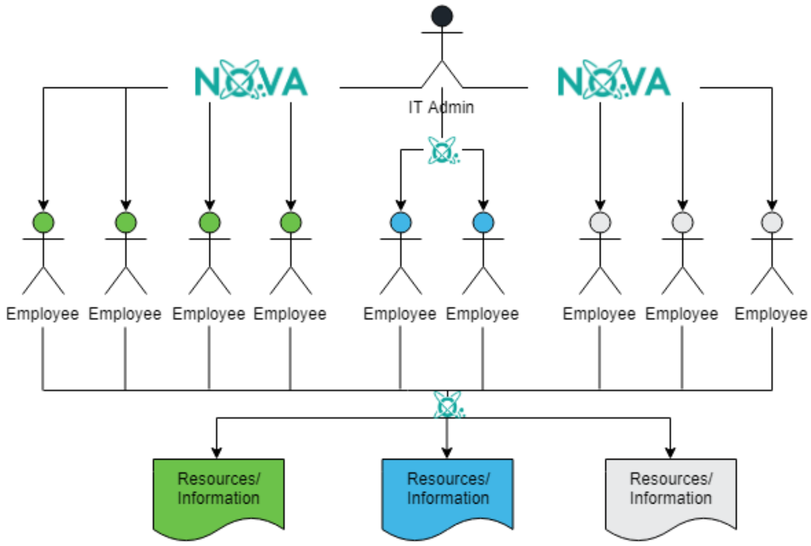


Self service

An administrator might want to give certain users the ability to manage some of their own access or information. For example, some executives might be able to log in to Nova and grant themselves access to resources/information without calling the helpdesk to get access.

Similarly, you might configure a policy that enables all employees to use Nova to update some of their basic information (for example, their phone number and address). This is called the "self service" option, here is how it looks:

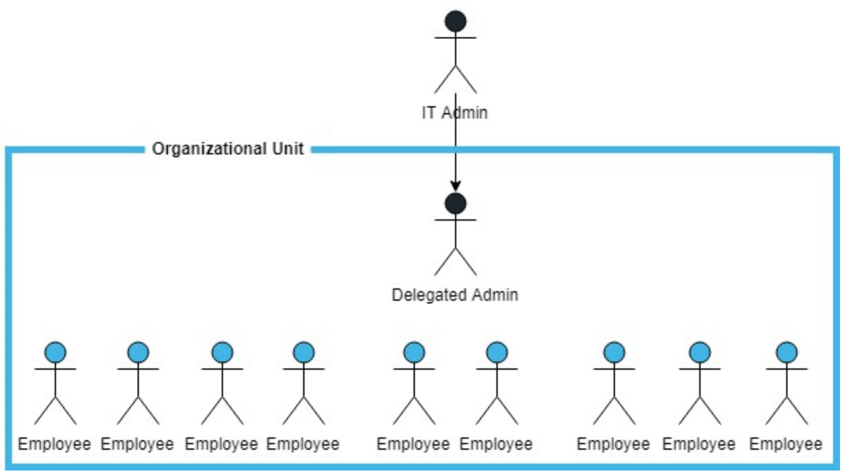
Example 2: IT Admin uses "self service" option, which gives users the ability to access Nova to manage some of their own information/resources



Delegated administration within an organizational unit

Finally, an administrator might want to set up someone within an organizational unit to manage access of others within that organizational unit. For example, you might have an organizational unit containing employees who work in a certain office location. You might assign administrative rights to the site manager or administrative assistant. It could look like this:

Example 3: IT Admin delegates administrative rights to someone within an organizational unit



4

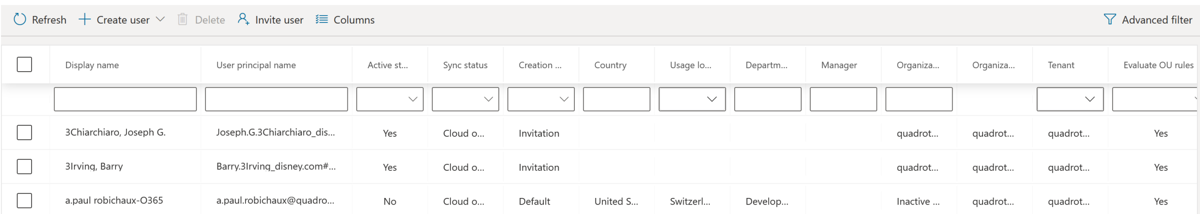
Manage

The Manage tab is accessible by administrators and delegated administrators to view and edit certain objects in their Microsoft 365 environment, including its:

- Users
- Contacts
- Mailboxes
- Groups
- Teams
- Devices
- Custom PowerShell

Users

The Users page shows a list of users in the tenant that you have permission to view. Depending on authorization policies in place, you can create new users and perform actions on existing users.



Display name	User principal name	Active st...	Sync status	Creation ...	Country	Usage lo...	Departm...	Manager	Organiza...	Organiza...	Tenant	Evaluate OU rules
3Chiarchiaro, Joseph G.	Joseph.G.3Chiarchiaro_dis...	Yes	Cloud o...	Invitation					quadrot...	quadrot...	quadrot...	Yes
3Irving, Barry	Barry.3Irving_disney.com#...	Yes	Cloud o...	Invitation					quadrot...	quadrot...	quadrot...	Yes
a.paul robichaux-O365	a.paul.robichaux@quadro...	No	Cloud o...	Default	United S...	Switzerl...	Develop...		Inactive ...	quadrot...	quadrot...	Yes

On the Users page, which you can access by going to **Manage,** then **Users**, you can perform the following actions:

- **Refresh:** This refreshes the users list.
- **Create user:** Here you can create an on-premises user or a cloud user. Details on that are below.
- **Delete:** Delete a user.
- **Invite user:** You can invite a user to the tenant by selecting the organizational unit to insert them into, and entering their email. They will then receive an invitation email to join the tenant.
- **Columns:** You can add and remove columns from the table.
- **Advanced Filter**: Find a user by their personal details or account details.

On the User Profile page you can see information about the user who is logged in to Nova. If there is a default self-service policy in place, then some or all of the information on the page relating to the user account can also be edited. There are a multitude of tabs that have user information, including:

- **Detail:** This includes display names, email addresses, departments, managers, and locations.
- **Licenses:** This is the licenses that the user has access to.
- **OneDrive:** Details on the user's OneDrive account, including information on the drive type, when it was created and last modified, as well as space used and space remaining.
- **Authentication:** This gives information on multi factor authentication status. Administrators have rights to reset password, revoke the user token so the user will have to sign back into their device, disable MFA or add an authentication method for the user. This includes authenticating using a phone number or email.
- **Group membership:** From here, you can add the user to a group by clicking on the group and clicking **Add.**
- **Intune Devices: T**his lists the number of devices registered to the user in Microsoft Intune. You can perform similar actions as seen in this section.

Creating a cloud user

Below are steps on how to create a cloud user.

1. Click **Create user**, then **Create cloud user**.
2. Select the vOU to insert the user into.
3. Enter the display name, and if the account should be enabled or not.
4. Enter the username of the email address of the user and select the domain name from the drop-down menu.
5. Enter the password for the user, and if the user should be forced to changed their password on the next sign in.
6. Enter the user's exchange alias.
7. Enter the location of the user from the drop down menu.
8. Optionally, add the details of the user, including display name, manager, department and additional location details.
9. Click **Save.**

Creating an on-premises user

Below are steps on how to create an on-premises user.

1. Click **Create user,** then **Create on-premises user**.
2. Select the vOU to insert the user into.

3. Enter the display name, and if the account should be enabled or not.
4. Enter the username of the email address of the user, and select the domain name from the drop down menu.
5. Enter the password for the user, and if the user should be forced to change their password on the next sign in.
6. Enter the SAM account name of the user.
7. Optionally, add the details of the user, including manager and display name.
8. Click **Save.**

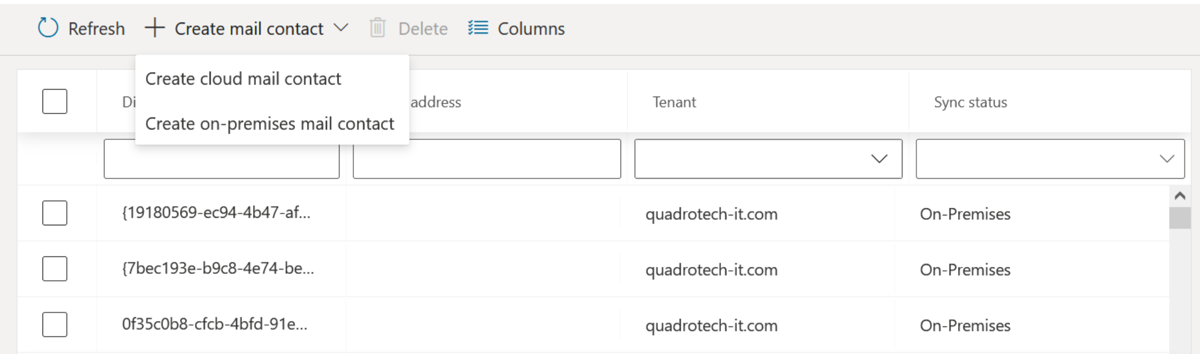
Add authentication method

Below are steps on adding a new authentication method for each individual user:

1. Click on the desired user.
2. Click **Authentication**.
3. Click **Add authentication method**.
4. Under **Choose label**, select either **Email** or **Phone number**.
5. Enter the desired parameters into the boxes, and click **Save**. A job will then run for each authentication method.
6. Your desired authentication method will appear under the Authentication tab for the user.

Contacts

This page shows you a list of mail contacts for a certain Microsoft 365 tenant.



On this page, you can:

- **Refresh:** Update the page to get the most up-to-date contacts.
- **Create Mail Contact:** You can add an on-premises contact or a cloud contact. Instructions on how to do that are below.
- **Delete:** Delete a contact from the list.

- **Columns:** You can add and remove columns from the table.

Creating a cloud mail contact

Below is how to create a mail contact stored in the cloud.

1. Click **Create mail contact**, then **Create cloud mail contact**.
2. Select the vOU to insert the user into.
3. Enter the email address of the chosen contact.
4. Enter the contact name of the user.
5. Enter the display name of the user.
6. Optionally, add the first name, last name and initials of the user.
7. Click **Save.**

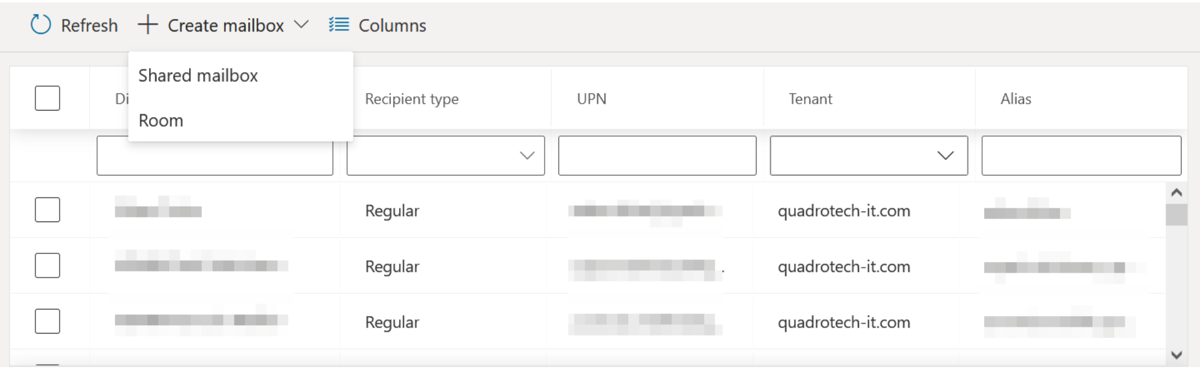
Create on-premises mail contact

Below is how to create a mail contact stored on-premises.

1. Click **Create mail contact**, then **Create on-premises mail contact**.
2. Select the vOU to insert the user into.
3. Choose the user's domain from the drop down menu.
4. Enter the contact name of the user.
5. Enter the display name of the user.
6. Optionally, enter the personal details of the contact. This includes location, department, telephone number and job title.
7. Click **Save.**

Mailboxes

On the Mailboxes page, you can review and manage mailboxes in the Microsoft 365 tenants that you have access to.



You can:

- **Refresh:** Refresh the mailbox list to get the most updated data.
- **Create Mailbox:** You can create either a shared mailbox or a room. Instructions on how to do that are below.
- **Columns:** You can add and remove columns from the table.

You can get details on each mailbox. By clicking on the name of the mailbox, you will see:

- **Detail:** This includes basic mailbox information, including forwarding addresses, recipient type and archive status.
- **Permission owner:** This shows the owner of the mailbox.
- **Recipient permissions:** Allows users to add send as and send on behalf permissions to other mailboxes.
- **Mailbox permissions:** This shows the list of users associated with the mailbox, and their permissions, including access rights.
- **SMTP aliases:** This is the list of email addresses assigned to the mailbox.
- **Folder statistics:** These are statistics associated with the different folders in the mailbox.
- **Mobile devices:** This is the list of devices that have access to the mailbox.
- **Automatic replies:** This is a list of automatic replies created by the users of the mailbox.

Creating a shared mailbox

Below are steps on how to create a shared mailbox.

1. Click **Create mailbox,** then **Shared mailbox.**
2. Select the vOU to insert the user into.
3. Enter this name of the mailbox.

4. Enter the display name of the mailbox.
5. Enter the mailbox's alias.
6. From the drop down menu, select the owner of the mailbox.
7. Click **Save.**

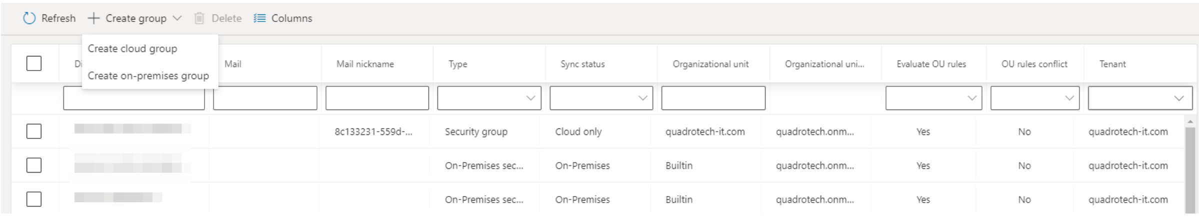
Creating a Room

Below are steps on how to create a room.

1. Click **Create mailbox**, then **Room**.
2. Select the vOU to insert the user into.
3. Enter this name of the room.
4. Enter the room's alias.
5. Optionally, enter the maximum amount of resources this room can have.
6. Optionally, enter the room's office location.
7. Click **Save**.

Groups

On the Groups page, by going to **Manage**, then **Groups,** you can manage Microsoft 365 groups.



You can:

- **Refresh:** Refresh the groups list to get the most updated data.
- **Create group:** you can create either a group in the cloud, or an on-premises group. Details on how to do that are below.
- **Delete:** Delete a group from the list.
- **Columns:** You can add and remove columns from the table.

By clicking on a group, you will see additional information, such as:

- **Detail**: This includes information on the group such as its group type, mail and security enablement and its mail nickname.
- **Owners**: This is a list of the group owners. You are able to add and remove owners if you have the permissions to.

- **Members**: This is a list of the group members. You are able to add and remove members if you have the permissions to.

Creating a Cloud Group

Below is how to create a group stored in the cloud.

1. Click **Create group**, the **Create on-premises group**.
2. Select the vOU to insert the user into.
3. Enter this display name of the group.
4. Enter the group's Exchange alias to link the group to.
5. Enter the group type. These are:
    a. Office 365 Group
    b. Security Group
    c. Distribution Group
    d. Mail enabled security group
6. Optionally, add a description to inform other users of the group's purpose.
7. Click **Save**.

Create an On-Premises Group

Below are steps on how to create a group stored on-premises.

1. Click **Create group**, then **Create on-premises group.**

2. Select the vOU to insert the user into.

3. Enter this domain of the group from the drop down list.

4. Enter the group's display name.

5. Enter the group's name.

6. Enter the group's SAM account name.

7. Enter the group's category: **Distribution** or **Security.**

8. Enter the group's scope: **Domain local, Global** or **Universal.**

8. Optionally, add who the group is managed by, a description of the group, the home page of the group and its mail address.

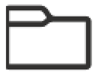
9. Click **Save.**

Teams

On the Teams page, by going to **Manage**, then **Teams**, you can manage your Microsoft 365 Teams. Here, you will see your already created Microsoft Teams, and the groups that they are associated with. These are the icons that you will see in Teams, and what they mean:

This is a channel within a Team.

This is a Team.



This is a group created in Nova to organize Teams and Teams channels.

On this page, you are also able to filter by Archived Teams, and select which tenant you would like to view. By default, the page will show all Teams, both archived and unarchived, from all tenants you have access to.

By clicking on a Team's ellipses, and clicking **Detail,** you will see additional information on a Team, including:

- **Detail:** This is information on a Team, including its description, group type, visibility, and mail and archive enablement.
- **Settings:** This is the list of settings applied to the Team, including member, guest and messaging permissions.
- **Owners:** This is a list of owners for the Team. You can add or remove owners if you have the appropriate permissions.
- **Members:** This is a list of members for the Team. You can add or remove members if you have the appropriate permissions.
- **Channels:** This is a list of channels for the Team. You can add, edit or delete channels if you have the appropriate permissions.

Clicking on the ellipses on a Team also allows you to:

- **Move** the Team into a different folder.
- **Delete** the Team.
- **Create** a new Teams Channel. Clicking on this will take you to a creation section, where you can enter the channel's name and description.

Clicking on the ellipses for a group allows you to:

- Create a new **Teams group.**
- **Edit** the folder to change its name and Team prefix.
- Create a new **Team**. More on this is below.
- **Refresh** the group to update its details.

How to create a new Team

Below are steps on how to create a new Team in Microsoft Teams.

1. Click on the folder ellipses and click **Create Team**.
2. Enter the display name for the Team.
3. Enter the Exchange alias for the Team.
4. Choose the Team's viability. The Team can be either **Public** or **Private.**
5. From the drop down menu, select the Team's owner.
6. Optionally, enter a description for the Team to give more information on its purpose.
7. Optionally, select settings for members, guests and messaging, including the choice to filter any inappropriate material.
8. Click **Save.**

How to create a new Channel

Below are steps on how to create a new Teams channel.

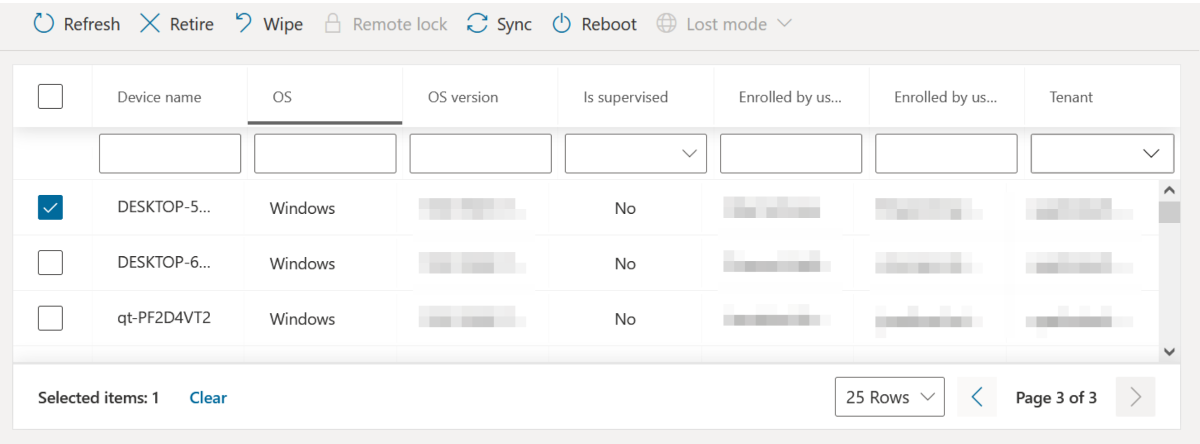
1. Click on the ellipses on the Team you would like to create the channel in, and click **Create Channel**.
2. Enter the display name for the Team.
3. Optionally, enter a description for the channel.
4. Click **Save.**

Devices

You are able to add actions to Microsoft Intune configuration policies to your user's mobile devices. For DPC users, this is helpful if you need to modify devices and applications of users you are allowed to manage. The devices screen can be found within the Nova Dashboard by clicking **Manage**, then **Devices**.

Actions include:

- **Refresh:** this refreshes the list of devices in the tenant.
- **Retire:** if the device is no longer in use, you can retire it.
- **Wipe:** you can remote wipe devices immediately.
- **Remote Lock:** you can remotely lock devices immediately.
- **Sync:** Sync your device to get its most up to date information.
- **Reboot:** instantly reboot a device.



To show more details for your device, click on its name. Here, you will find several more tabs, including:

- **Detail:** this gives additional information of the device, including manufacturer, model, last sync date type and encryption state.
- **Owner:** this gives detail on the owner of the device, including email and the tenant the user is in.
- **Users:** this includes a list of users assigned to the device.
- **Group Membership:** if the device is part of a group, they will be listed here.

Also on this Device Detail page, you have the opportunity to remove the passcode (for iOS), and reset passcode (Android 7+ versions only).

Custom PowerShell

The Custom PowerShell page shows a list of PowerShell scripts which have been added to Nova. You can also create your own scripts and run them. For more on this, go to the *Quest Nova User Guide.*

NOTE: Only System Administrators, Account Administrators and delegated administrators who have been given Custom PowerShell rights can access this page and perform actions with custom PowerShell.

5

Policy Examples

Below are some authorization and configuration policy examples that allow delegated administrators to perform certain actions and tasks.

NOTE: Delegated administrators must have the correct permissions in the relevant authorization or configuration policy to perform the following actions. Please contact your Nova administrator if you would like to perform these tasks.

Reset a User's Password

Nova gives the ability to reset a user's password and have them change the password upon their next login. This is helpful if you believe an account has been compromised or to revoke access for a recently terminated employee. To do this:

1. Go to the **Manage** tab, then click **Users**.
2. Click on the user you would like to perform the action on.
3. Go to **Authentication.**
4. Click **Reset password.**
5. Enter the new password to assign to the user.
6. Optionally, check the box to have the user change the password upon their next login.
7. Click **Save.** This will then appear as a running job in the Jobs tab.

Revoke user token/enable Multi Factor Authentication

In the same screen, you can also revoke the user token so the user will have to sign in again, as well as the option to enable or disable multi factor authentication for a user. You can do this by clicking on the relevant button on the **Authentication** tab, and clicking **OK** to proceed.

Set an Out of Office message

Nova gives the ability to set a user's out of office message, with the possibility to set different messages to internal and external users. To do this:

1. Go to the **Manage** tab, then click **Mailboxes**.
2. Locate the user you would like to set an out of office message to.
3. Click **Automatic Replies.**

4. Click **Set Out of Office.**
5. Click the drop down list, and select **Scheduled.**
6. Select the scheduled start and end date and time for the message.
7. Enter the internal and external messages you would like to send to recipients.
8. Click **Save.** This will then appear as a running job in the Jobs tab.

Create a new Team Channel

Nova gives the ability to give delegated administrator's the permissions to create a new channel in a Microsoft Team. To do this:

1. Go to the **Manage** tab, and click **Teams**.
2. Click on the ellipses of the Team you would like to create a channel to, and click **Create channel.**
3. Enter the display name of the channel, and add a description if required.
4. Click **Save.** This will then appear as a running job in the Jobs tab.