Quest® Nova

Getting Started Guide for Delegation and Policy Control for Administrators

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
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

Quest, Quadrotech Nova by Quest, and the Quest are trademarks and registered trademarks of Quest Software Inc. and its affiliates. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are the property of their respective owners.

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 2024

Contents

Introduction to Delegation and Policy Control **4**

Service Accounts for Nova DPC **5**

Roles in Nova DPC **7**

Virtual Organizational Units **9**

Authorization Policies **13**

Use case: Delegating rights to a level 1 helpdesk 14

Use case: Delegating password resets to users in the UK 15

Configuration Policies **16**

Use case: Setting a users United States location details 17

Use case: Assigning a manager 18

License Policies **19**

Use case: Delegating Exchange, SharePoint and Teams licenses 20

Manage **21**

Users 21

Contacts 23

Mailboxes 25

Groups 26

Teams 28

Devices 30

Custom PowerShell 31

Manage administration **32**

Using the audit log 32

Compliance Policies 34

Jobs 35

Jobs schedules 37

On premises agent & On premises domain 38

1

Introduction to Delegation and Policy Control

Quest Nova provides granular Delegation and Policy Control for Office 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 is to help you get started with Delegation and Policy Control as an administrator. This includes:

- how to set up service accounts
- how to create Virtual Organizational Units (vOUs)
- how to create authorization, configuration and license policies, including helpful use cases
- overviews of the Manage and Manage Administration tabs

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

> **CAUTION:** DPC gives the ability to control license management, device management and other sensitive actions, so select your administrators and delegated administrators with care.

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

Service Accounts for Nova DPC

Nova Delegation and Policy Control (DPC) uses service accounts to manage tenants and to perform actions on behalf of delegated administrators. Service accounts are also used to pull the data from the account to perform actions upon in DPC.

You can review and manage these accounts on the **Manage Administration,** then the **Service Accounts** page.

On the Service accounts tab, you can:

- **Refresh**: Update the list of service accounts for the tenant.
- **Add**: Add a service account to the tenant. Instructions on how to do that are below.
- **Edit:** Change the service account. You will need the account's credentials to access.
- **Delete:** Remove the service account from the tenant.
- **Authorize Management:** Learn more about this below.

There are two steps to configure and setup Nova DPC for the tenant. They are:

1. Allowing permissions for Nova DPC

Nova DPC requires an administrator to allow Microsoft permissions to retrieve data for the tenant. To do this:

1. On the **Manage administration** tab, click **Service accounts.**
2. Click **Authorize Management.**
3. Sign in using an administrative account.
4. Review the list of permissions. Once you are happy with this, click **Accept.** This will then take you back to Nova.

2. Adding a service account to the tenant

You then need to add the service account to pull the data from to perform actions on. To do this:

1. On the **Manage administration** tab, click **Service accounts.**
2. Select the tenant to add the service account to.

3. Enter the global administrative account's email to the Admin username box.
4. Enter the password of the global administrator.
5. Click **Save.** The service account will then be provisioned.

Pre-requisites for service accounts

- The service account needs to be a global administrator in the tenant. The global administrator account will also need to be mail enabled to receive an email invitation. A global administrator account is required as:
    i. this allows for delegated actions to be completed by Nova users, without needing to grant these users full administrator permissions.
    ii. an account with global administrator permissions are able to perform actions that may not be available via Microsoft Graph.
- Single Sign On (SSO) is the preferred method of signing in. This will need to be authorized in each tenant.
- Multi-factor authentication should not be enabled on the account (it is used to programmatically run PowerShell sessions, and therefore cannot be multi-factor authentication enabled). Application passwords are not supported for the service account.
- It must be free from any policies that would restrict its access in the tenant (for example, a Conditional Access Policy that limits basic authentication attempts from internal IP addresses only).
- It should be dedicated for use with Nova DPC.

> **NOTE:** If the password of the service account is changed, it must also be changed in Nova DPC.

Permissions

A list of the APIs/permissions required can be found here.

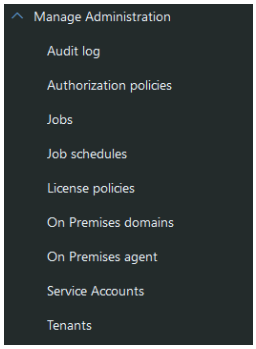
3

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.

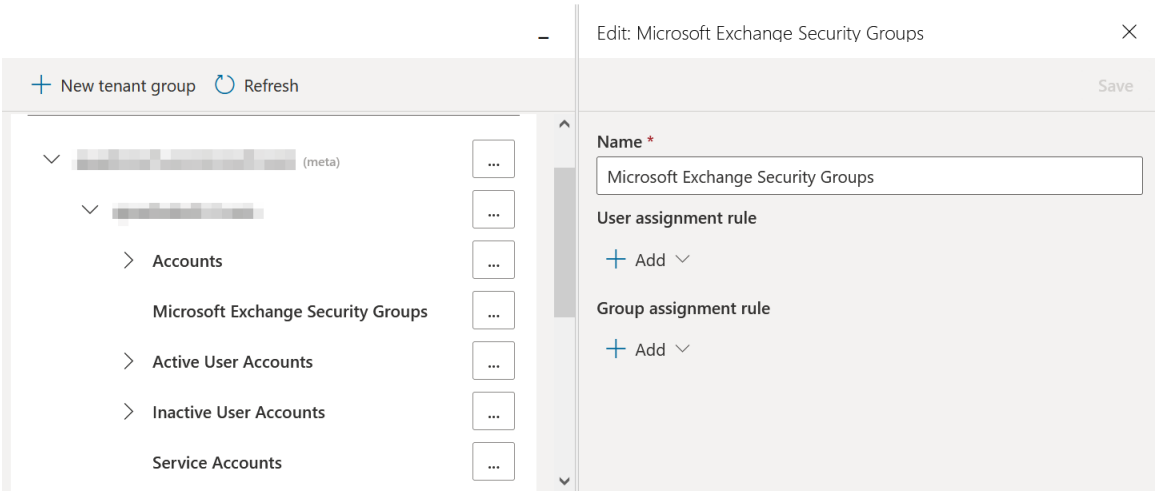
4

Virtual Organizational Units

A virtual organizational unit (vOU) is a manually built dynamic list of users tailored to group users by a specific attribute. For example, vOUs can be built to group users by their location, department, company or another attribute. These help administrators to group users to assign authorization, configuration and license policies to them.

If you are familiar with on-premises Microsoft Entra ID, then you will already be familiar with organizational units. The problem is that Microsoft Entra ID and Office 365 do not have this concept. These users are stored in a flat list, which can make working with multiple geographies and multiple departments much more difficult. Nova has modified this premise, redefined as 'virtual organizational units'. You can create a hierarchy of these just like you would in an on premises Microsoft Entra ID environment.

NOTE: These organizational units are exclusive to Nova, and are not pulled into Microsoft Entra ID.



Creating a new Virtual Organizational Unit

Follow the steps below to set up a virtual organizational unit.

1. In the left menu, select **Manage Administration**, then **Tenants**.
2. Then, either:
   - Click the ellipsis button (...) next to a tenant and select **New**.

- Or, create a virtual organizational unit that's nested under an existing one by expanding the tenant, finding the organizational unit you will create one under, clicking the ellipsis button (...) next to it, and selecting **New**.

3. Enter a name for the new organizational unit and click **Save**.

Adding a User or Group to a Virtual Organizational Unit

Complete the steps below to add a user or group to a virtual organizational unit.

1. In the left menu, select **Manage Administration**, then **Tenants**.
2. Expand organizational units until you find the one to which you will add a new user or group.
3. Click the desired organizational unit's ellipses (...) button and:
   a. if you would like to add one or multiple users, click **Users.**
   b. if you would like to add one or multiple groups, click **Groups**.
4. Select the checkbox next to the desired user or group and click the Move button.
5. Expand the tree until you find the desired target organizational unit, and then select it and click **Save**.

Viewing Users and Groups Assigned to a Virtual Organizational Unit

Follow the steps below to see a list of users and groups currently assigned to a virtual organizational unit.

1. In the left menu, select **Manage Administration,** then **Tenants**.
2. Expand the organizational units until you find the one whose users you want to see.
3. Click the desired organizational unit is ellipses button (...) and select Users & Groups to see a list of users and groups that were added to the group within Nova.

NOTE: You can see other objects as well, such as mailboxes and contacts.

User Assignment Rule

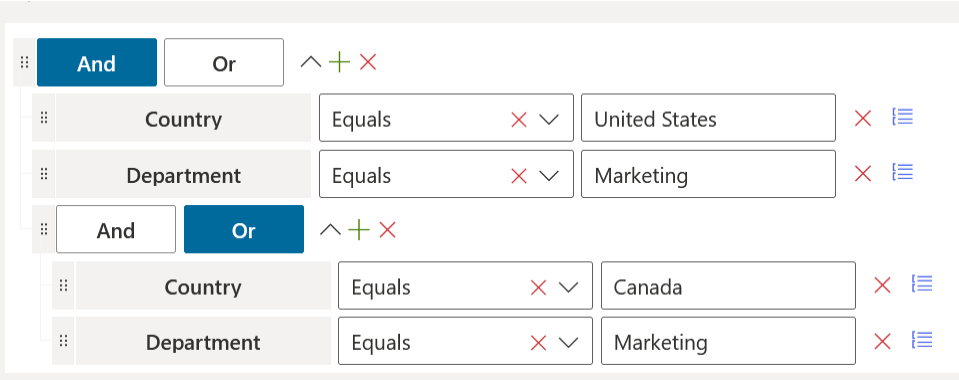
The user assignment rule automatically adds users to a vOU based on one or more properties already assigned to those users. For example, you can set up a policy that adds United Kingdom users operating in Sales. Below are the steps to do that:

1. Go to your vOU and click on the ellipses button, then click **Edit**.
2. Under **User assignment rule,** click **Add,** then **Group.**
3. Click the + icon, then **Property.**
4. Click **Choose property**, then from the drop down menu, click **Country.**

5. For **Choose operator**, click **Equals,** then type United Kingdom into the text field.
6. Click the + icon again, and select **Property.**
7. Click **Choose property**, then from the drop down menu, click **Department.**
8. For **Choose operator,** select **Equals,** then type Sales in the text field.
9. Click **Save.**

Users with these attributes already assigned will now be automatically assigned to this vOU.

Another example is creating a vOU for the marketing department assigned in the United States or Canada. Applying the steps above in this scenario, the rule should look like the image below:



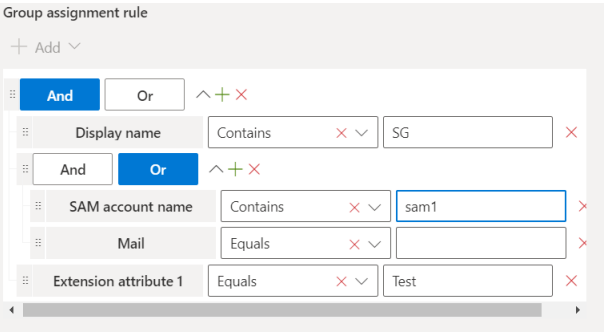
Group Assignment Rule

Administrators also have the ability to automatically assign group management delegation based on properties of the group or group owner. This allows you to delegate responsibilities to localized IT support without granting them excessive access to your tenant(s).

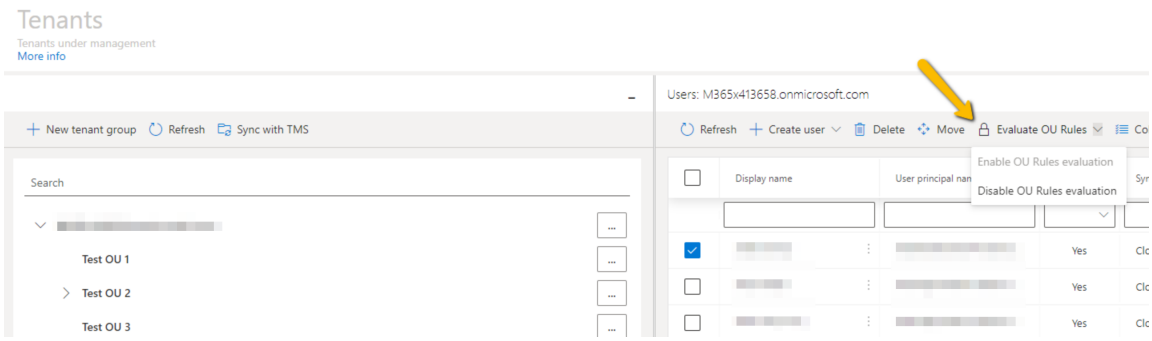
To automate group management delegation:

1. From the Nova dashboard, go to **Manage Administration**, then **Tenants**.
2. Click on the ellipsis next to your desired tenant, and click **New**.
3. Click **Add** under Group Assignment Rule.

From here, provide your required group and/or properties, then save your organizational unit with this group assignment rule. View the image below for an example.



You can also enable or disable OU rules for each user by selecting the user from your chosen tenant, then selecting Evaluate OU Rules, then either enabling or disabling these rules.



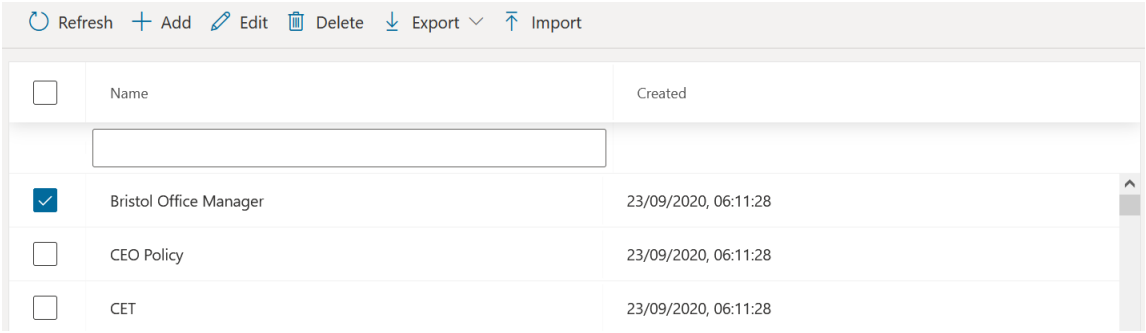
5

Authorization Policies

Authorization policies allow administrators to grant permissions to chosen delegated administrators to perform actions on one or multiple users, groups, virtual organizational units or across the tenant. Permissions that are granted in Nova are also granted in Office 365.

Actions include creating, modifying and deleting users and groups, setting out of office statuses, resetting user passwords, setting multi-factor authentication and more. You can create multiple authorization policies to grant some users additional or less permissions than others, useful for multi-regional helpdesk operators.

Another example is for tenants that retain employee information in Office 365, team managers in different departments can be granted permissions to update some details in a user's profile, but not able to update some specific details, such as an address, and hide some others. This is useful to comply with an organization's company policy.



On the Authorization policies tab, you can:

- **Refresh:** Update the authorization policies to present the most recent additions.
- **Add:** Create an authorization policy.
- **Edit:** Change the authorization policy, including who gets access, the users/groups that the policy applies to, and the actions of the policy.
- **Delete:** Remove the policy from the list.
- **Export**: You can export a policy to a .json file. You may:
  - export all of your policies
  - export a select number of policies
  - export the audit log to a .csv file
- **Import:** Import a .json file of an exported authorization policy.

For more on exporting and importing policies, go to the *Quest Nova User Guide.*

How to create an Authorization Policy

The steps below detail how to create a generic authorization policy.

1. From Nova, go to **Manage Administration**, then **Authorization Policies**.
2. Give the policy a unique name.

> **NOTE:** Under **Settings**, you will see three options: **Default user policy, self service** and **Is template.** You can learn more about these in the *Quest Nova User Guide*.q

3. On the **Delegate to** tab, select the user(s) and/or groups you would like to delegate the permissions to.
4. On the **Managed objects** tab, select the user(s). group(s) and/or organizational units you would like the delegated administrators to perform the action(s) on.
5. Then select **Actions,** and select the actions you would like the delegated user to have access to.

> **NOTE:** Click **Add** after selecting each action.

6. In the **Properties** tab, choose which properties you would like the manage objects to read and/or write.

Once you are happy with the policy, click **Add,** and your authorization policy is set up.

Use case: Delegating rights to a level 1 helpdesk

Below are steps that outline how to create an authorization policy that would be appropriate to assign users working in a level 1 helpdesk.

1. From Nova, go to **Manage Administration**, then **Authorization Policies**.
2. Give the policy a unique name.
3. On the **Delegate to** tab, select the user(s) and/or groups you would like to delegate the permissions to.
4. On the **Managed objects** tab, select the user(s). group(s) and/or organizational units you would like the delegated administrators to perform the action(s) on.
5. Then select **Actions.** For a level 1 helpdesk, we recommend selecting the following options.

> **NOTE:** Click **Add** after selecting each action.

   a. Create On-Premises User
   b. Create Cloud User
   c. Update On-Premises User

d. Update Cloud User

e. Graph Set Out Of Office

f. Reset User Password on Next Login

g. Reset Mailbox Permissions

h. Add Group Member

i. Set Cloud User Manager

2. In the **Properties** tab, choose which properties you would like the manage objects to read and/or write.

Once you are happy with the policy, click **Add,** and your authorization policy is set up.

Use case: Delegating password resets to users in the UK

In this example, we will go over the steps to allow a manager to reset passwords for users based in the UK.

1. From Nova, go to **Manage Administration**, then **Authorization Policies**.
2. Give the policy a unique name.
3. On the **Delegate to** tab, select the user(s) and/or groups you would like to delegate the permissions to.
4. On the **Managed objects** tab, select the user(s). group(s) and/or organizational units you would like the delegated administrators to perform the action(s) on.
5. Then select **Actions.** To delegate password resets, select the following actions:

NOTE: Click **Add** after selecting each action.

a. Reset User Password on Next Login

b. Update User Password

c. Revoke Microsoft Entra ID User All Refresh Token (this prompts users to add their new password sooner)

Once you are happy with the policy, click **Add,** and your authorization policy is set up.

6

Configuration Policies

Configuration policies bring standardization to your virtual organizational units and allows you to automate changes to users. Instead of manually assigning a license type, or updating Microsoft Entra ID attributes one by one, configuration policies allow you to apply these across your chosen vOUs.

For example, you may manage two tenants. One contains people working in the United States, and the other contains people working in the United Kingdom. You can create configuration policies to give users in the United States a Country attribute of US, and and another configuration policy gives users within the United Kingdom a Country attribute of UK.

- **Refresh:** Update the configuration policies to present the most recent additions.
- **Add:** Create a configuration policy.
- **Edit:** Change the configuration policy, including who gets access, the filters that the policy applies to, and the actions of the policy.
- **Delete:** Remove the policy from the list.

How to create a configuration policy

Below are steps on how to create a generic configuration policy.

1. In the menu on the left side of the screen, select **Manage administration**, then **Configuration policies**.
2. Click **Add**.
3. Enter a unique Name for the policy.
4. With the **Policy Scope** tab selected, click **Add**, and then select the organizational unit(s) and/or group(s) to which the policy will apply. These are the users that the policy will apply to.
5. Optionally, with the **User filters** tab selected, click **Add**, and then select the groups or attributes used to filter the users. This defines the filter used to select users from the scope to apply the policy to.
6. Select the **Actions** tab, click **Add**, and then select the actions you want to include in the policy. These actions are:
    a. **Add User to Groups**: add a user to a group.
    b. **Assign User License**: Manage Office 365 licenses.
    c. **Graph Set Out of Office**: Set user's out of office status.
    d. **Set Cloud User Manager**: Set a user's manager.

e. **Set Mailbox Primary SMTP Address**: Set a user's primary email address.

f. **Set Mailbox Primary SMTP Address for Synchronized Users:** Sets primary SMTP address for on-premises user and their cloud mailbox.

g. **Set User Multi-factor authentication**: Set a user's MFA status.

h. **Update Cloud User**: Update Office 365 user attributes.

i. **Update On-Premises User**: Update on-prem user attributes.

7. Click **Save,** and your configuration policy will have been created.

Use case: Setting a users United States location details

In this use case, you will be assigning a user to change a vOU's location details to the United States.

> **NOTE:** You will to have previously created a virtual organizational unit containing all users known to currently operate in the United States. This configuration policy will apply Microsoft Entra ID attributes to these users, including new users that you may add to this vOU.

1. In the menu on the left side of the screen, select **Manage administration**, then **Configuration policies**.
2. Click **Add**.
3. Enter a unique Name for the policy.
4. With the **Policy Scope** tab selected, click **Add**, and then select the organizational unit(s) and/or group(s) to which the policy will apply. For this example, we want to give all users in the United States vOU Usage location and Country settings, so select your previously created United States vOU. Then click **Add.**
5. Optionally, with the **User filters** tab selected, click **Add**, and then select the groups or attributes used to filter the users. This defines the filter used to select users from the scope to apply the policy to.
6. Select the **Actions** tab, click **Add**, and select **Update Cloud User.**
7. Enable the **Usage location** slider, and select **United States** from the drop down menu.
8. Enable the **Country** slider, and enter **United States** into the text field.
9. Click **Save,** and your configuration policy will have been created.

Use case: Assigning a manager

In this use case, you will be assigning a user who can add a manager attribute to an organizational unit.

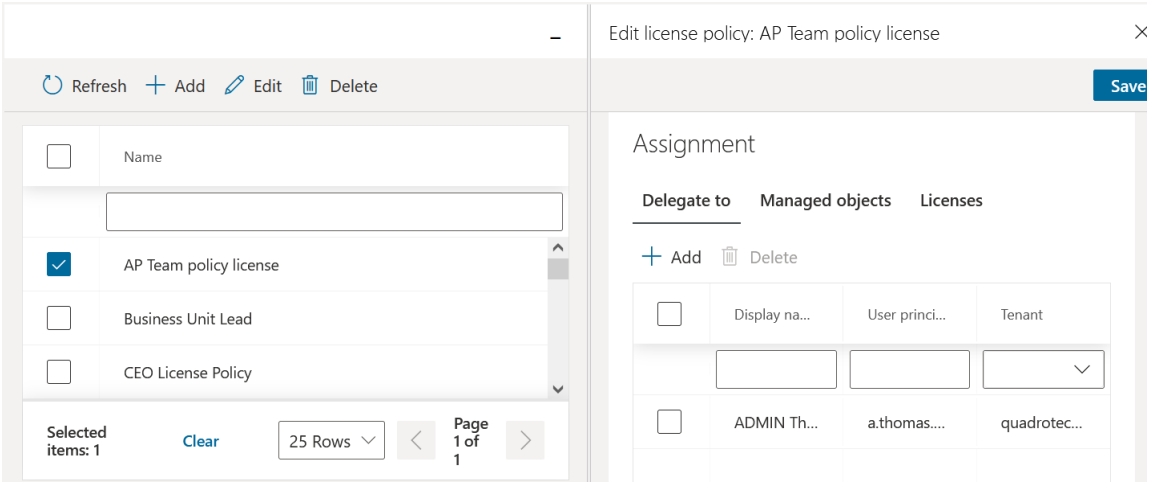
> **NOTE:** You need to have previously created a virtual organizational unit containing all users you would like to assign a manager to.

1. In the menu on the left side of the screen, select **Manage administration**, then **Configuration policies**.
2. Click **Add**.
3. Enter a unique Name for the policy.
4. With the **Policy Scope** tab selected, click **Add**, and then select the organizational unit you would like to assign a manager to, and click **Add.**
5. Select the **Actions** tab, click **Add**, and select **Set Cloud User Manager.**
6. Choose the manager to assign to the configuration policy from the drop down menu, and click **Save.**
7. Click **Save,** and your configuration policy will have been created.

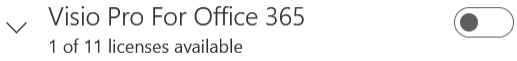
7

License Policies

License policies allow administrators to give delegated users permissions to assign one or multiple licenses to other users and/or groups. You can also get specific and specify which workloads from a license you want users to get. For example, if your organization doesn't use Yammer, you can remove that workload, if desired, before assigning an E5 license to someone. You can also specify how many of a particular license a delegated administrators can assign.



License policies also give you viability into how many licenses are available to distribute.



How to create a license policy

Below are steps on how to create a generic license policy.

1. In Nova, as an administrator, go to **Manage administration**, then **License Policies**.
2. Give the License Policy a unique name.
3. Click the **Delegate to** tab, and select the user(s) you would like to delegate the policy to.
4. In the **Managed objects** tab, select the user(s), group(s) and/or organizational unit(s) you would like the delegated user(s) to give the license(s) to.
5. In the **Licenses** tab, select the tenant containing the licenses you would like to apply.
6. Select the license(s) and workload(s) you would like the delegated user(s) to be able to assign, and click **Add.**

a. You also have the ability to select the number of licenses you would like your delegated user to assign. Select **Unlimited** to give the user access to all selected licenses, or click **Limited** and add the number of licenses to delegate to the user.

7. Click the X button, then **Add.** The license policy will be added to your tenant.

Use case: Delegating Exchange, SharePoint and Teams licenses

In this use case, we will create a license policy that delegates an unlimited number of Exchange Online, SharePoint Online and Microsoft Teams licenses to your chosen delegated users.

1. In Nova, as an administrator, go to **Manage administration**, then **License Policies**.
2. Give the License Policy a unique name.
3. Click the **Delegate to** tab, and select the user(s) you would like to delegate the policy to.
4. In the **Managed objects** tab, select the user(s), group(s) and/or organizational unit(s) you would like the delegated user(s) to give the license(s) to.
5. In the **Licenses** tab, select the tenant containing the Office E3/E5 license.
6. Select the applicable Office E3/E5 license, and click the arrow icon.
7. Select the **Exchange Online, SharePoint Online** and **Microsoft Teams** sliders, and click **Add.** These licenses will appear under the licenses tab.
7. Click the X button, then **Add.** The license policy will be added to your tenant.

8

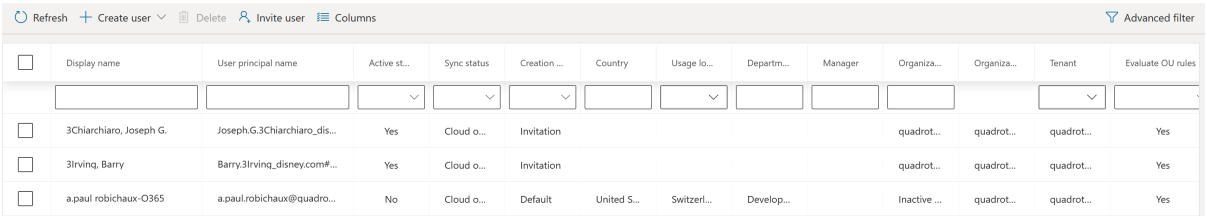
Manage

The Manage tab is accessible by administrators and delegated administrators to view and edit certain objects in their Office 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.



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, and disable MFA.
- **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.**

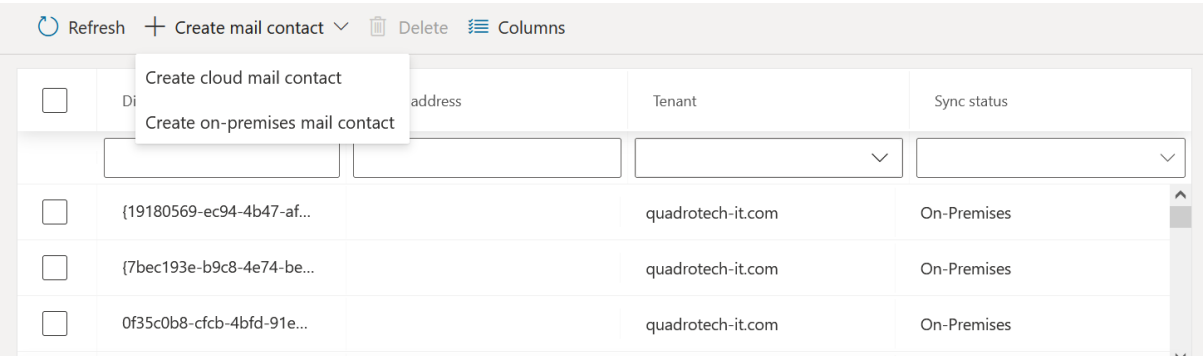
Add authentication method

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 Office 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.**

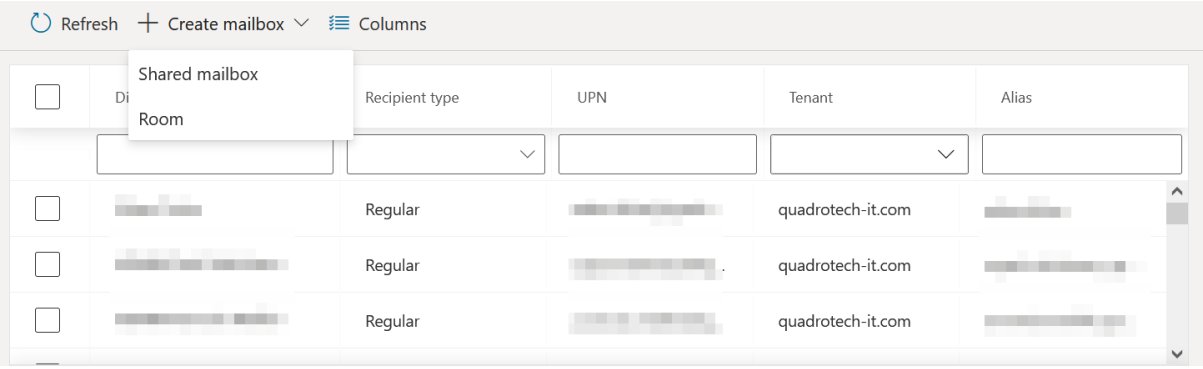
Create on-premises mail contact

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 Office 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.**

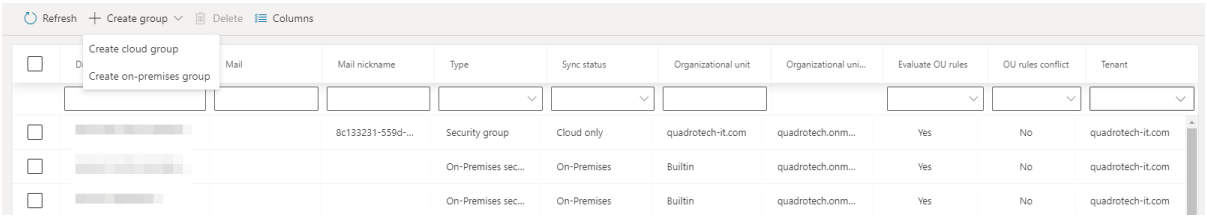
Creating a Room

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 Office 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 Office 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.

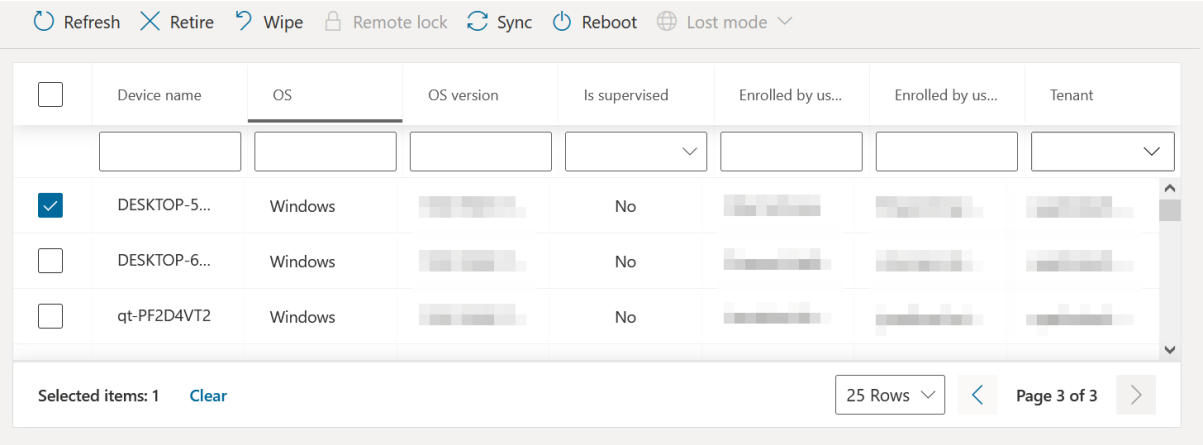
1. Click on the ellipses on the Team you would like to create the channel in, and click **Create Channel**.
2. Enter the display name for the Team.
3. Optionally, enter a description for the channel.
4. Click **Save.**

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.

9

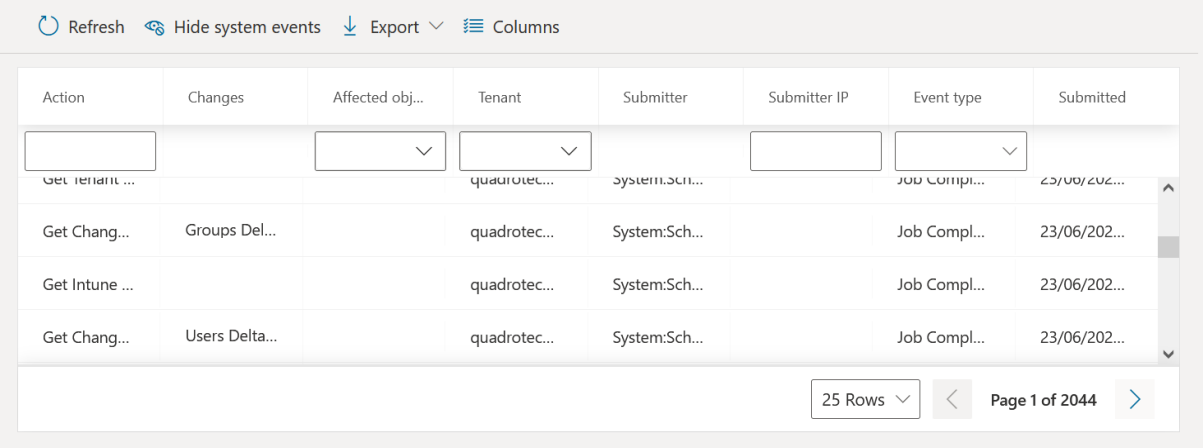
Manage administration

The Manage administration tab gives administrators and delegated administrators the rights to assign users, groups and/or virtual organizational units access to a range of actions in Office 365, as well as actions on service accounts and devices. This tab includes:

- Audit log
- Authorization policies
- Compliance policies
- Configuration policies
- Jobs
- Job schedules
- License policies
- On premises agent & On premises domains
- Service accounts
- Tenants (creating Virtual Organizational Units)

Using the audit log

You will find an audit log under the Manage Administration service that shows who performed what actions against which object. Here is how it looks:

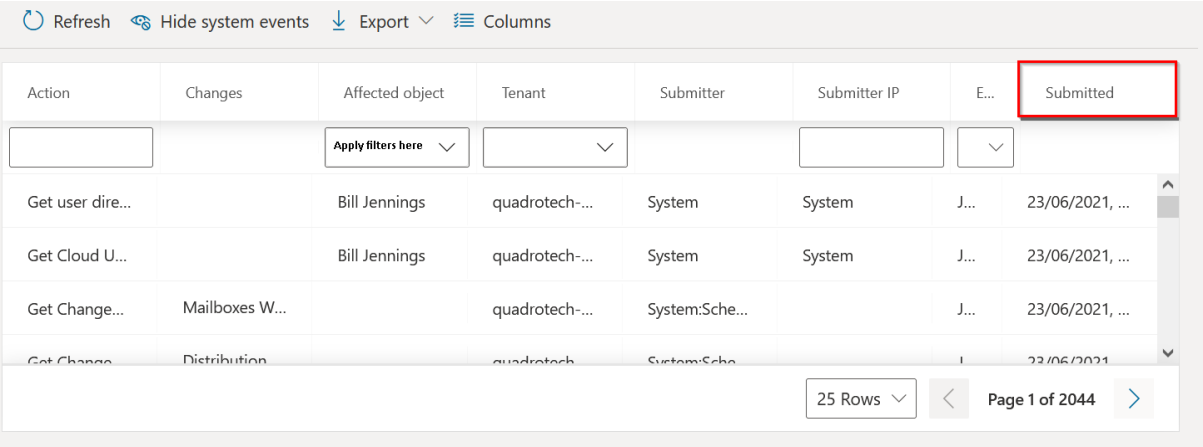


Actions you can complete on the Audit Log are:

- **Refresh:** Update the audit log to receive the most recent data.
- **Hide/Show system events:** this hides/shows system data, and will show/hide only data relating to Submitter IPs.
- **Export**: this exports data into a .csv file. Here, you can:
  - **Export all:** this exports all data collected.
  - **Export page:** this exports data in the page you are currently viewing. You can adjust the amount of rows in the table, then click **Export page** to export those amount of rows.
- **Columns:** You can add and remove columns from the table.

Filtering and sorting the audit log

Apply filters to the log using fields in the top row.
You can also sort the data by clicking on a column name. If the audit log is currently being sorted by a certain column, a line displays above the column name (shown below). Click the column name again to reverse the filter.



A **Hide/Show System Events** button displays above the audit log. Click this button to filter for only user-generated events.

Audit log contents

Here is a description of the contents of each column:

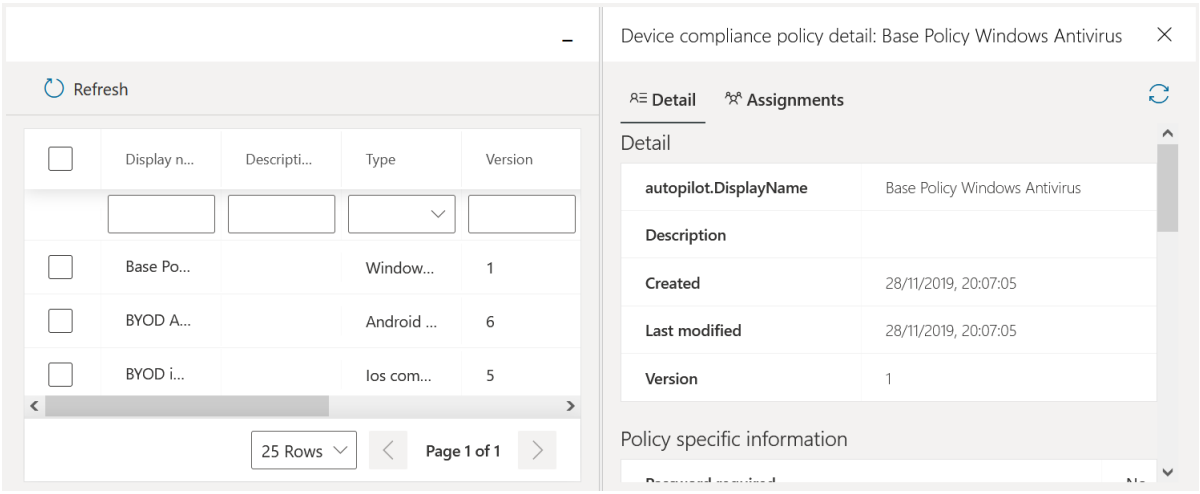
Field	Description
Action	The action that was performed
Changes	Shows details of what was changed. For example, showing a phone number changed from 555-5555 to 444-4444.
Affected object	The resource the changes were performed against
Tenant	The tenant affected by the changes

Field	Description
Submitter	The user who initiated the event
Submitter IP	The IP address of the user who initiated the event
Event type	Shows whether the job is completed, errored, running, etc.
Submitted	Date and time the job was initiated

Click here to watch a video on the audit log.

Compliance Policies

Device compliance policies give an overview of the device compliance policies that have been applied to your registered devices. Instant information regarding these policies include the type of policy (Windows, Mac, Android etc), the version of the policy and when the policy was last created and modified.



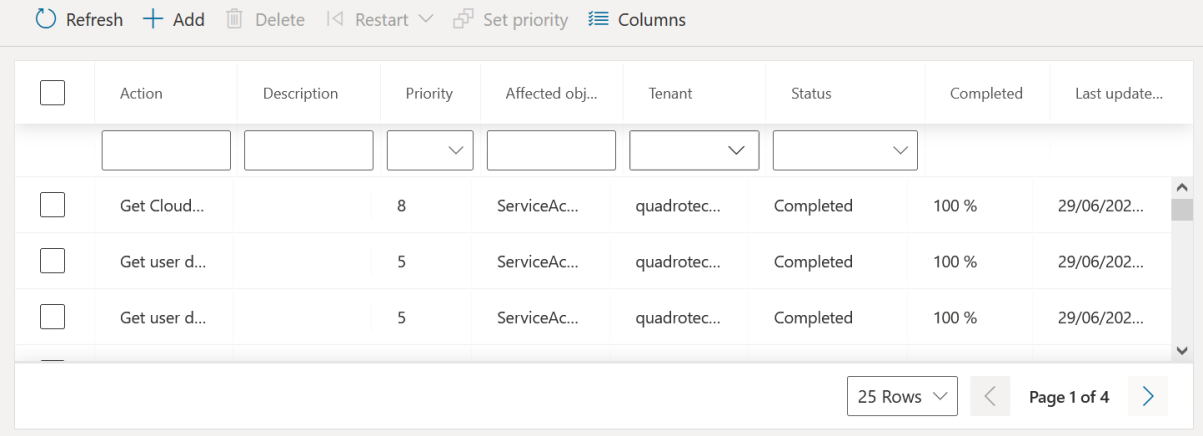
Click on a policy to see policy specific information, including:

- if a passcode is required
- the minimum length of the passcode
- the number of minutes before a device is locked
- the minimum and maximum iOS (if applicable)

By clicking on **Assignments**, you can add and remove groups to be applied to this policy.

Jobs

DPC actions are completed via jobs. The Jobs page shows all Nova jobs, in various statuses.



The list of jobs that are performed are:

Add Cloud Group Member Add a user to a group	Add Distribution Group Member	Add Distribution Group Owner	Add Domain	Add Group Owner Add an owner to a group.
Add Group Recipient Permission Sets the SendAs permission in Exchange Online that allows users to send messages that appear to come from the specified group	Add Mailbox Folder Permission Adds folder-level permissions for users and mail enabled security groups in mailboxes.	Add Mailbox Permission	Add Proxy Email Addresses	Add Mailbox Recipient Permission Sets the SendAs permission in Exchange Online that allows users to send messages that appear to come from the specified mailbox.
Add OneDrive Item's Permissions	Add On-Premises Group Member Adds member to On-Premises group.	Adds On-Premises User Proxy Addresses Adds proxy addresses for on-premises user.	Add User to Groups	Archive Team
Assign User License Manage Office 365 licenses.	Clear Mobile Device	Create a sharing link for a OneDrive item	Create Channel	Create Cloud Group Create a new group as specified; this could be an Office 365 group, dynamic group, security group or team.
Create Cloud Mail Contact	Create Cloud User	Create Distribution Group	Create Mail-Enabled Security Group	Create On-Premises Group

On the jobs page, you can:

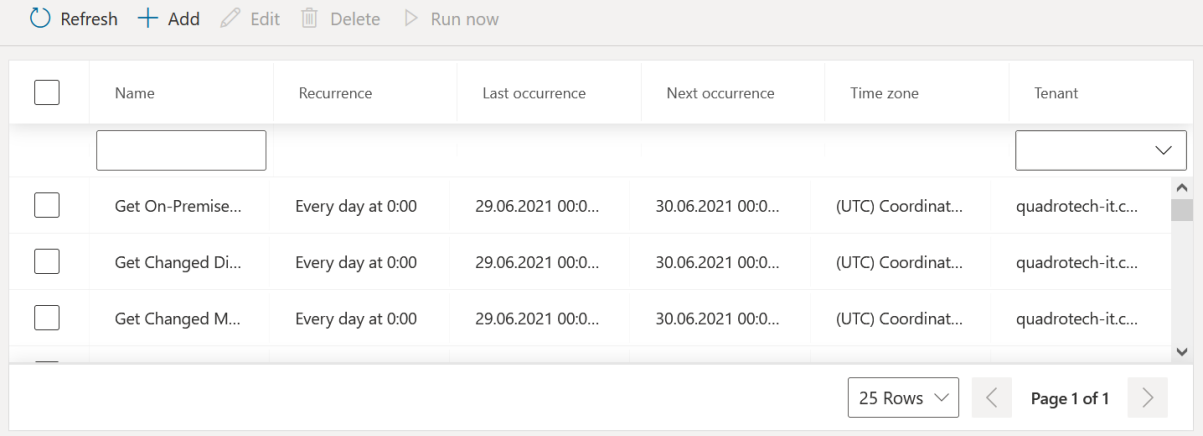
- **Refresh:** this refreshes the list of devices in the tenant.
- **Add:** You can add a job to be completed. Select the tenant, and job you would like to be performed.
- **Delete** a job.
- **Restart** a job with either normal or advanced logging.
- **Set the priority** of a job if there are multiple running.

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

Some jobs need to be performed more than once. For example, you might want the Get Mailboxes job to recur, so it checks regularly to see if new mailboxes are added to your environment. Use the Job Schedules page to schedule recurring jobs, change the frequency at which they occur, and see when a recurring job was last performed.

Jobs schedules

Delegation & Policy Control (DPC) performs several actions from time-to-time, on a schedule. Use the Job Schedule page to: review the jobs, create new ones, and edit existing ones.



You can:

- **Refresh:** Refresh the jobs schedules list to get the most updated data.
- **Add** a job schedule. Find out how to do that below.
- **Edit** a job schedule. Here you can change the time and recurrence of the job, and the time zone.
- **Delete** a job schedule.
- **Run** the job schedule now.

Create a new job schedule

Below is how you can create a new job schedule.

1. Select the tenant to run the job on.
2. Set the schedule to run for every hour, every day, once a week or once a month.
3. Select the time to run the job.
4. Select the time zone to set the time of the job in.
5. Click **Save.**

On premises agent & On premises domain

In a hybrid Office 365 environment, where some resources remain on premises inside a customer organization, Nova can deploy an agent to collect metadata and perform administration. By going to **Manage administration**, then **On premises agent**, you can install the agent. Once installed the agent will be automatically kept up to date by Nova.

With the On premises domain, which you can view by going to **Manage administration,** then **On premises domains**, you can see information about the on premises domains that have been discovered by the on premises Nova agent.

To find out more about the On Premises Agent and the On Premises domain, go to the *Quest Nova User Guide.*