

Quest® Nova
User Guide



© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

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

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 October 2024

Contents

Delegation & Policy Control	6
Service Accounts for DPC	6
Microsoft permissions for DPC	8
Virtual Organizational Units	13
Creating a Virtual Organizational Unit	14
Adding a user or group to a Virtual Organizational Unit	14
Deleting a Virtual Organizational Unit	14
User assignment rule	15
Group assignment rule	15
Authorization policies	16
Creating and modifying authorization policies	16
Configuring Nova to grant permissions for OneDrive	18
Examples of authorization policies	18
Exporting and importing policies	19
Policy properties	20
Configuration policies	20
Creating and modifying configuration policies	21
Configuration policy examples	22
Device compliance policies	22
License policies	23
Custom Powershell	24
Delegated administration	31
Resetting a user password	33
Set an out of office message	33
How To...	34
Configure Nova DPC to use OAuth	34
Invite guest users to a tenant	34
Search for external users or guests in a tenant	35
Take an action on all members of a Microsoft Entra ID security group	35
Use the jobs page	36
DPC trial mode	37
Reporting	39
Using the on-boarding wizard	40
Microsoft permissions for Reporting	41
Dashboards	46
Interacting with the data	47
Creating a custom chart widget	49
Adding a card widget	51
Nova Report Center	51
Report Center terminology	53
Customize and organize reports	55
Creating a custom report	57

Creating a custom chart or pivot section	57
Creating a custom table section	62
Creating a custom timeline section	66
Creating a custom map section	68
Creating a custom metric section	68
Creating a custom card section	70
Using text	72
Filtering and sorting	72
Filtering table data	74
Schedule Center	77
Notification Center	80
Custom Alert Center	83
How To...	84
Add a logo to your report	85
Combine multiple charts	85
Describe reports and sections	86
Pin reports to the navigation bar	88
View extra columns in a table report section	88
Tenant Management System	90
Configuring certificate-based authentication	91
SharePoint API permissions	95
Nova administration	96
Contact Center	96
Cross-tenant reporting	97
Deprovision data collection	99
Invitation to access Nova	100
License types	101
On-premises agent	101
Persona menu	103
Subscription overview	104
User detail	105
Using the audit log	110
Virtual Business Boundaries	112
Creating a boundary	113
How to add new users	114
Adding additional service accounts	117
Remove a user from your tenant	118
Creating a group and Team prefix	119
Identify when jobs are not running	119
What are the roles within Nova?	120
Settings	123
Service accounts for Nova	123
Application settings menu	123
Rule sets	124
Copyright	126

About	128
Contacting Quest	128
Technical Support Resources	128

Delegation & 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 even end-users – setting boundaries far more precise than native delegation. Nova also includes policy-based automation for authorization, service configuration and license assignment.

Service Accounts for 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](#).

Microsoft permissions for DPC

To be granted access to Nova DPC, you need to accept Microsoft permissions during the onboarding process of connecting your tenant. The following are Microsoft's permissions:

Permission	Permission Description
Manage Exchange As Application	Allows the app to manage the organization's Exchange environment without any user interaction. This includes mailboxes, groups, and other configuration objects. To enable management actions, an admin must assign the appropriate roles directly to the app.
Use Exchange Web Services with a full access to all mailboxes	Allows the app to have full access via Exchange Web Services to all mailboxes without a signed-in user.
Read all usage reports	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Microsoft 365 and Microsoft Entra ID.
Manage apps that this app creates or owns	Allows the app to create other applications, and fully manage those applications (read, update, update application secrets and delete), without a signed-in user. It cannot update any apps that it is not an owner of.
Read calendars in all mailboxes	Allows the app to read events of all calendars without a signed-in user.
Read and write calendars in all mailboxes	Allows the app to create, read, update, and delete events of all calendars without a signed-in user.
Read contacts in all mailboxes	Allows the app to read all contacts in all mailboxes without a signed-in user.
Read and write contacts in all mailboxes	Allows the app to create, read, update, and delete all contacts in all mailboxes without a signed-in user.
Read all devices	Allows the app to read your organization's devices' configuration information without a signed-in user.
Read and write devices	Allows the app to read and write all device properties without a signed in user. Does not allow device creation, device deletion or update of device alternative security identifiers.

Permission	Permission Description
Read Microsoft Intune apps	Allows the app to read the properties, group assignments and status of apps, app configurations, and app protection policies managed by Microsoft Intune, without a signed-in users.
Read and write Microsoft Intune apps	Allows the app to read and write the properties, group assignments and status of apps, app configurations and app protection policies managed by Microsoft Intune, without a signed-in user.
Read Microsoft Intune device configuration and policies	Allows the app to read properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups, without a signed-in user.
Read and write Microsoft Intune device configuration and policies	Allows the app to read and write properties of Microsoft Intune-managed device configuration and device compliance policies and their assignment to groups, without a signed-in user.
Perform user-impacting remote actions on Microsoft Intune devices	Allows the app to perform remote high impact actions such as wiping the device or resetting the passcode on devices managed by Microsoft Intune, without a signed-in user.
Read Microsoft Intune devices	Allows the app to read the properties of devices managed by Microsoft Intune, without a signed-in user.
Read and write Microsoft Intune devices	Allows the app to read and write the properties of devices managed by Microsoft Intune, without a signed-in user. Does not allow high impact operations such as remote wipe and password reset on the device's owner.
Read Microsoft Intune RBAC settings	Allows the app to read the properties relating to the Microsoft Intune Role-Based Access Control (RBAC) settings, without a signed-in user.
Read and write Microsoft Intune RBAC settings	Allows the app to read and write the properties relating to the Microsoft Intune Role-Based Access Control (RBAC) settings, without a signed-in user.
Read Microsoft Intune configuration	Allows the app to read Microsoft Intune service properties including device enrollment and third party service connection configuration, without a signed-in user.

Permission	Permission Description
Read and write Microsoft Intune configuration	Allows the app to read and write Microsoft Intune service properties including device enrollment and third party service connection configuration, without a signed-in user.
Read directory data	Allows the app to read data in your organization's directory, such as users, groups and apps, without a signed-in user.
Read and write directory data	Allows the app to read and write data in your organization's directory, such as users, and groups, without a signed-in user. Does not allow user or group deletion.
Read and write domains	Allows the app to read and write all domain properties without a signed in user. Also allows the app to add, verify and remove domains.
Read files in all site collections	Allows the app to read all files in all site collections without a signed in user.
Read and write files in all site collections	Allows the app to read, create, update and delete all files in all site collections without a signed in user.
Read all groups	Allows the app to read group properties and memberships, and read the calendar and conversations for all groups, without a signed-in user.
Read and write all groups	Allows the app to create groups, read all group properties and memberships, update group properties and memberships, and delete groups. Also allows the app to read and write group calendar and conversations. All of these operations can be performed by the app without a signed-in user.
Read all user mailbox settings	Allows the app to read user's mailbox settings without a signed-in user. Does not include permission to send mail.
Read and write all user mailbox settings	Allows the app to create, read, update, and delete user's mailbox settings without a signed-in user. Does not include permission to send mail.
Read mail in all mailboxes	Allows the app to read mail in all mailboxes without a signed-in user.
Read and write mail in all mailboxes	Allows the app to create, read, update, and delete mail in all mailboxes without a signed-in user. Does not include

Permission	Permission Description
	permission to send mail.
Send mail as any user	Allows the app to send mail as any user without a signed-in user.
Read all hidden memberships	Allows the app to read the memberships of hidden groups and administrative units without a signed-in user.
Read all OneNote notebooks	Allows the app to read all the OneNote notebooks in your organization, without a signed-in user.
Read and write all OneNote notebooks	Allows the app to read all the OneNote notebooks in your organization, without a signed-in user.
Read online meeting details	Allows the app to read online meeting details in your organization, without a signed-in user.
Read and create online meetings	Allows the app to read and create online meetings as an application in your organization.
Read all users' relevant people lists	Allows the app to read any user's scored list of relevant people, without a signed-in user. The list can include local contacts, contacts from social networking, your organization's directory, and people from recent communications (such as email and Skype).
Read all usage reports	Allows an app to read all service usage reports without a signed-in user. Services that provide usage reports include Microsoft 365 and Microsoft Entra ID.
Have full control of all site collections	Allows the app to have full control of all site collections without a signed in user.
Create, edit, and delete items and lists in all site collections	Allows the app to create or delete document libraries and lists in all site collections without a signed in user.
Read items in all site collections	Allows the app to read documents and list items in all site collections without a signed in user.
Read and write items in all site collections	Allows the app to create, read, update, and delete documents and list items in all site collections without a signed in user.

Permission	Permission Description
Invite guest users to the organization	Allows the app to invite guest users to the organization, without a signed-in user.
Read all users' full profiles	Allows the app to read user profiles without a signed in user.
Read and write all users' full profiles	Allows the app to read and update user profiles without a signed in user.
Access the directory as the signed-in user	Allows the app to have the same access to information in the directory as the signed-in user.
Read directory data	Allows the app to read data in your company or school directory, such as users, groups, and apps.
Read and write directory data	Allows the app to read and write data in your company or school directory, such as users, and groups. Does not allow user or group deletion.
Read all groups	Allows the app to read basic group properties and memberships on behalf of the signed-in user.
Read and write all groups	Allows the app to create groups on behalf of the signed-in user and read all group properties and memberships. Additionally, this allows the app to update group properties and memberships for the groups the signed-in user owns.
Read hidden memberships	Allows the app to read the memberships of hidden groups and administrative units on behalf of the signed-in user, for those hidden groups and administrative units that the signed-in user has access to.
Sign in and read user profile	Allows users to sign in to the app, and allows the app to read the profile of signed-in users. It also allow the app to read basic company information of signed-in users.
Read all users' full profiles	Allows the app to read the full set of profile properties of all users in your company or school, on behalf of the signed-in user. Additionally, this allows the app to read the profiles of the signed-in user's reports and manager.
Read all users' basic profiles	Allows the app to read a basic set of profile properties of all users in your company or school on behalf of the signed-in user. Includes display name, first and last name, photo, and

Permission	Permission Description
	email address. Additionally, this allows the app to read basic info about the signed-in user's reports and manager.
Read and write all applications	Allows the app to create, read, update and delete applications and service principals without a signed-in user. Does not allow management of consent grants.
Manage apps that this app creates or owns	Allows the app to create other applications, and fully manage those applications (read, update, update application secrets and delete), without a signed-in user. It cannot update any apps that it is not an owner of.
Read and write domains	Allows the app to read and write all domain properties without a signed in user. Also allows the app to add, verify and remove domains.
Read all hidden memberships	Allows the app to read the memberships of hidden groups and administrative units without a signed-in user.

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 Microsoft 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.

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 > Tenants**.
2. Expand the organizational units until you find the one whose users you want to see.
3. Click the desired organizational unit ellipses button (...) and select **Users** or **Groups** to see a list of users or groups that were added to the group within Nova.

Creating a Virtual Organizational Unit

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

i | **NOTE:** Any organizational units set up in Nova are not pulled into Microsoft Entra ID.

1. In the left menu, select **Manage Administration > Tenants**.
2. 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 > Tenants**.
2. Expand the 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 select **Users**.
4. Select the checkbox next to the desired user or group and click **Move**.
5. Expand the tree until you find the desired target organizational unit, and then select it and click **Save**.

i | **NOTE:** You cannot have a specific user across more than one vOU. For example, you cannot have a user in a United States vOU and a Sales vOU.

Deleting a Virtual Organizational Unit

When deleting a virtual organizational unit containing users, those users can be moved to another vOU. Here is how to do it:

1. In the left menu, select **Manage Administration > Tenants**.
2. Expand organizational units until you find the one you want to delete.
3. Click the desired organizational unit's ellipses (...) button and select **Delete**.
4. In the left frame, find and select the vOU to which you will move any users from the deleted vOU, and then click **OK** to apply the changes.

Here is a [video](#) showing the steps above.

User assignment rule

When creating a virtual organizational unit, as well as giving the vOU a name, you can enter a User Assignment Rule. With this feature users will be automatically moved to this virtual organizational unit, based on the rule that you specify. 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:

The screenshot shows a user assignment rule configuration interface. It features a logical expression builder with the following structure:

- Top level: A blue button labeled "And" and a white button labeled "Or". To the right are icons for adding (+), removing (-), and toggling (X).
- First clause: A property dropdown set to "Country", an operator dropdown set to "Equals", and a text field containing "United States".
- Second clause: A property dropdown set to "Department", an operator dropdown set to "Equals", and a text field containing "Marketing".
- Third clause: A sub-expression enclosed in brackets, starting with a blue "And" button and followed by:
 - A property dropdown set to "Country", an operator dropdown set to "Equals", and a text field containing "Canada".
 - A property dropdown set to "Department", an operator dropdown set to "Equals", and a text field containing "Marketing".

Group assignment rule

As a Nova administrator, you 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.

Group assignment rule

+ Add

And Or ^ + X

Display name Contains X SG X

And Or ^ + X

SAM account name Contains X sam1 X

Mail Equals X X X

Extension attribute 1 Equals X Test X

You can 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.

Authorization policies

The Delegation and Policy Control (DPC) feature allows administrators to authorize rights and responsibilities to other users within their organization.

Creating and modifying authorization policies

Nova facilitates Role-Based Access Control (RBAC). That means you use it to grant permission for someone to do something, against something. For example, an administrator might grant permission for people to access a certain application. Or, an office manager might grant access for others in the office to use certain resources.

A Nova administrator configures authorization policies to specify who can perform certain actions within a tenant, and the conditions associated with those actions.

There are four pieces to an authorization policy:

- **Tenant:** Authorization policy is applied to a certain tenant. For example, North America.
- **Delegate:** The person to which rights are granted. They can do something with the tenant. For example, VP of Operations.
- **Action:** The activity the person can perform. For example, update user.
- **Conditions of the action:** Any conditions related to the delegate performing the action. For example, when the VP of Operations updates a user's information, you can specify whether they can see/update all of the user's attributes or only some of them.

When an authorization policy grants someone rights to perform a certain action, that person logs in to Nova to perform the action.

For example, a manager can perform certain actions (like setting out of office messages and granting access to SharePoint resources) to the users on their team. The manager uses single sign-on (via their Microsoft Entra ID credentials) to log in to Nova and perform the actions. Actions performed by the manager are pushed to other applications (for example, Exchange

Online). It is important to note the manager's Nova instance only shows options that are relevant to the activities they can perform in the application.

A video overview of authorization policies can be seen [here](#).

Setting up a new authorization policy

Follow the steps below to create an authorization policy.

1. In the left menu, select **Manage Administration > Authorization policies**.
2. Click **Add**.
3. Enter a name for the policy.
4. Specify settings, if desired:
 - **Default user policy:** Select this option if the policy applies to all organizational units in a tenant. For example, select this option if you want the helpdesk to be able to update all users in the organization.
 - **Self service:** Select this option if you want a user to be able to perform a certain specific action on their own user object when they log in. For example, select this option if you want a user to be able to update their own phone number and address.
 - **Is template:** Select this option if you want to create a template policy that you will use across tenants.
6. Using the **Delegate to** tab, assign the policy to users.
7. Using the **Managed objects** tab, specify where the delegated rights are assigned.
8. Using the **Actions** tab, add tasks you are delegating.
9. Using the **Properties** tab, add any conditions to the policy. For more information, [click here](#).
10. Click **Save** to create the authorization policy.

Editing or deleting an authorization policy

To edit or delete an existing authorization policy:

1. In the left menu, select
2. **Manage Administration > Authorization policies**.
3. Locate the policy you want to edit or delete, and select it.
4. Either:
 - Click **Edit**, make desired changes, and click **Save** to apply all the edits.
 - Click **Delete** and confirm the delete action.

Delegating action(s) to an authorization policy

Follow these steps to delegate an action to an authorization policy:

1. In the left menu, go to
2. **Manage Administration > Authorization policies**.
3. Select an existing policy, and then click **Edit**.
4. In the **Assignment** frame, select the **Actions** tab, and then click **Add**.
5. Locate the action(s) you want to add, select it/them, and then click the **Add** button located in the top right corner of the window.
6. Select the **Properties** tab and select any conditions. For more information, [click here](#).
7. Click the **Save** button.

Which policies apply?

After you have set up and assigned policies, [here is](#) how you can see which policies apply to a certain virtual organizational unit.

Configuring Nova to grant permissions for OneDrive

Granting permissions in Nova also grants those permissions in Microsoft 365. Follow the steps below to grant permissions for users for OneDrive.



NOTE: If you are not a System Administrator, ensure that you are in an authorization policy with the actions needed to configure OneDrive.

1. In Nova, under Manage, go to **Users**.
2. Find the user to configure, then go to **OneDrive**, then **Items**.
3. Select Private/Sharing under the Sharing column for a OneDrive item. This will then open a list of users who have permissions on that OneDrive item.
4. Select which users you would like to grant permissions to that item, and click **Grant Access**.
5. On the Grant Access screen, select which type of permission to grant; View Only or Edit. Add recipients to that permission, and click **Save**.

These users' permissions should now be saved in OneDrive as well as Nova.

Examples of authorization policies

Below, you will find some examples of authorization policies in Nova.

Delegating password resets

In [this](#) video we see how to delegate the ability to perform password resets.

Delegating out of office administration

In [this](#) video we see how to delegate the ability to manage out of office (automatic replies) messages.

Delegating management of MFA

In [this](#) video we see how to delegate the ability to manage multi-factor authentication settings for users.

Delegating custom PowerShell scripts

As a System or Account Administrator, you have the ability to delegate the execution of Custom PowerShell scripts to other administrators. Click [here](#) for more information on that. Follow to steps below on how to create an authorization policy to delegate custom PowerShell Scripts.

1. Go to **Manage administration > Authorization Policies**.
2. Click **Add**.
3. Enter a name for your policy.
4. On the **Assignment** section, on the **Delegate to** tab, click **Add**, and add the user(s) and/or OU(s) you would like to delegate the policy to.
5. Then select **Managed Objects** and choose which user(s) and/or OU(s) you would like the delegated administrator to perform the actions on.
6. Then select **Actions** and select **Executes Custom PowerShell Script**, and click the arrow button.
7. Under PowerShell Commands, and add the PowerShell commands that have been created. Once you have selected them, click Close.



NOTE: Go [here](#) to learn more about creating custom PowerShell scripts.

8. Select the [properties](#) you would like to apply to your policy, then click **Close**.
9. Once you are finished creating the policy, click **Save**.

Exporting and importing policies

To ensure the policy does not become lost or corrupted, you might want to export/save the configuration to a safe location.

Exporting an authorization policy or configuration policy

Follow the steps below to export a policy file.

1. From the left menu bar, select **Manage Administration > Authorization policies or Configuration policies** (depending on the type of policy you want to export).
2. Either:
 - Export all policies by selecting **Export > Export All**.
 - Export a specific policy (or policies) by selecting the check box next to any policies you want to export and selecting **Export > Export Selected**.
3. Click **OK**.

A .zip file containing the policy configuration is saved to your **Downloads** folder.

Importing an authorization policy or configuration policy

When you are ready to restore a previously exported policy file, follow the steps below.

1. From the left menu bar, select **Manage Administration > Authorization policies** or **Configuration policies** (depending on the type of policy you want to import).
2. Click **Import**.
3. Specify how you want duplicate policy names to be handled.
4. Browse for the policy file, select it, and click **Open**.
5. Click **Import**.

The restored/imported policy can now be found in your list of policies.

Policy properties

You can edit details related to actions added to authorization policies using the Properties tab (shown below).

After adding actions to a policy, you can select whether delegates can see or edit information related to the assigned actions.

For example, after assigning the Update Tenant User action to an authorization policy, you might edit the policy's properties so delegates (i.e. members of the help desk) cannot read and/or edit certain information.

[Here is](#) a video showing more about properties.

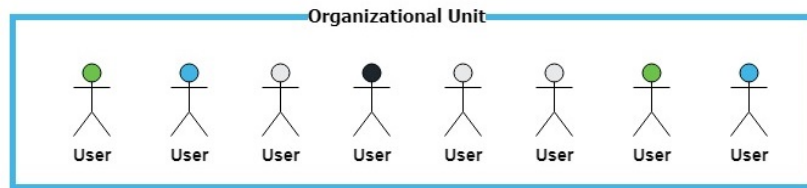
Configuration policies

Configuration policies bring standardization to a particular tenant (organizational unit). For example, you could use a configuration policy to grant access to a certain resource for all users within a tenant.

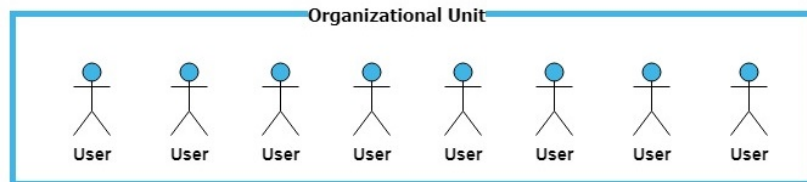
Or, you might manage two tenants. One contains people working in the United States, and the other contains people in the United Kingdom. You can create configuration policies to give users in the United States a Country attribute of US. And, another configuration policy gives users within the United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

Once a configuration policy is assigned to a particular tenant (organizational unit), a job is initiated. The job updates all user objects within the tenant, as shown below.

Organizational Unit BEFORE configuration policy takes effect



Organizational Unit AFTER configuration policy takes effect



After initial setup, any time a new user is added to the tenant (organizational unit), a job runs to ensure the user object matches all of the tenant's configuration policies. For a brief overview, check out the video below:

[Click here](#) to watch an introductory video on configuration policies.

Supported actions

At this time, any of these actions can be added configuration policies:

- **Add User to Groups:** add a user to a group
- **Assign User License:** Manage Microsoft 365 licenses.
- **Graph Set Out of Office:** Set user's out of office status.
- **Set Cloud User Manager:** Set a user's manager.
- **Set Mailbox Primary SMTP Address:** Set a user's primary email address.
- **Set User Multi-factor authentication:** Set a user's MFA status.
- **Update Cloud User:** Update Microsoft 365 user attributes.
- **Update On-Premises User:** Update on-prem user attributes.

Creating and modifying configuration policies

Complete the steps below to set up a new configuration policy.

1. In the menu on the left side of the screen, select **Manage Administration > Configuration policies**.
2. Click **Add**.
3. Enter a **Name** for the policy.
4. With the **Policy Scope** tab selected, click **Add**, and then select the organizational unit to which the policy will apply. This defines the users that the policy *may* be applied to.
5. 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. See below for a list of available actions.

7. Click **Save**.

[Click here](#) to watch a video on how to create a configuration policy.

Editing or deleting a configuration policy

If you want to update or delete an existing configuration policy, follow the steps below.

1. In the menu on the left side of the screen, select **Manage Administration > Configuration policies**.
2. Select the desired policy and either:
 - Click **Edit**, make desired changes, and click **Save**.
 - Click **Delete** and confirm the deletion.

Configuration policy examples

Assign a manager to a vOU

Assigning a manager to a virtual organizational unit is straight forward. This configuration policy allows administrators to automatically assign managers to particular users who may be within a certain department or geographical location. Check out [this](#) video below for a walk through.

Set a user's usage location and country details

Setting a user's location settings is a straightforward process with Nova. Setting a configuration policy allows you to instantly change a user's usage location and country settings when placed within a virtual organizational unit. See how to do that [here](#).

Device compliance policies

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).

License policies

License Policies in Nova give an administrator (or delegated administrator) the ability to assign/remove licenses, as needed, all from within Nova. Plus, Nova gives visibility into exactly how many licenses are used and how many are available.

The Nova license policies and reports provide:

- The ability to apply licenses according to what has been budgeted and what is required for a specific role
- The ability to show and hide particular licenses to include (or exclude) them from the report page shown above.
- Accurate license intelligence when it comes time for budgeting and Microsoft 365 renewal.
- Delegated license management activities

Similar to other Nova policies, with a license policy you specify who can assign what licenses within a tenant or group. For example, a license policy might enable the Director of Engineering to manage Azure DevOps licenses assigned to users within the Engineering virtual organizational unit.

You can get really granular and specify which workloads from a license you want users to get. For example, if your organization does not 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 delegated administrators can assign.

To set up a license policy

1. In Nova, go to **Manage administration > License policies**.
2. Click **Add**.
3. Enter a **Name** for the policy.
4. In the Assignment section, with the Delegate to tab selected, click **Add**.

5. Select user(s) to whom you will delegate the ability to assign licenses according to the policy, and then click **Add**.
6. Select the Managed objects tab, and then click **Add**.
7. Use the Select type drop-down menu to choose whether the licenses can be applied to certain users, groups, and/or organizational units.
8. Locate any users/groups/organizational units containing users to which the licenses can be assigned, select them, and click **Add**.
9. Select the Licenses tab, and then click **Add**.
10. Select the tenant containing licenses you will add to the policy.
11. Select the licenses (and specify the maximum number of licenses) and workloads you want those delegated the policy to be able to assign, and then click Add.

After completing these steps, your policy is configured and the user(s) who are delegated the license policy can assign licenses to users specified in the policy.

To hide licenses

You can hide selected licenses from the licenses report, if desired, by clicking the **Hide Licenses** button.

You can also show/hide any hidden licenses by using the toggle option located in the top left of the list.

Custom Powershell

The Custom PowerShell functionality allows almost any PowerShell scripts to be executed to perform custom tasks within your tenant organizations.

This accessibility of this function is dependent on the user's role:

- **System Administrator** and **Account Administrator** roles will have access to Refresh, Add, Edit, Delete and Run command functions.
- **Autopilot Classic** roles will be able to Refresh and Run command actions.
- **Auth Policy admins** will be able to delegate PowerShell commands to other users. Click [here](#) to see how to create an authorization policy to delegate custom PowerShell commands.



NOTE: Custom PowerShell scripts can run for up to 600 seconds (five minutes), after which the script will timeout.

More details on the scripts, validation and parameters can be found [here](#).

Creating a new custom script

Follow the steps below to add a new custom script:

1. In the left menu, select **Manage > Custom PowerShell**.
2. Click on 'Add'
3. Give the custom PowerShell script a meaningful name.
4. Select the online PowerShell-type that the script will run against. You can choose one of the following:
 - Exchange Online
 - Microsoft Entra ID
 - MS Online
 - MS Teams
 - SharePoint
6. Enter the PowerShell script that should be executed.
7. Click on **Validate**. (You will need to correct any errors before the final step)
8. **Save** the script.

Here is an example script for setting a retention policy on a mailbox:

```
param( [Parameter(mandatory=$true)] $name, [Parameter(mandatory=$true)]  
$retentionPolicyName )
```

```
set-mailbox "$name" -RetentionPolicy "$retentionPolicyName"
```

To use this script, you would select 'Exchange Online' as the PowerShell type. After validating the script, you will see that two parameters were added to the bottom of the data entry page. More details on the scripts, validation, parameters and so on, can be found [here](#).

Editing or deleting existing custom script

To edit or delete a script follow these steps:

1. In the left menu, select
2. **Manage > Custom PowerShell**.
3. Locate the script you want to edit or delete, and select it.
4. Either:
 - Click **Edit**, make desired changes, and click **Save** to apply all the edits.
 - Click **Delete** and confirm the delete action.

Executing a script

To run a script follow these steps:

1. In the left menu, select
2. **Manage > Custom PowerShell**.
3. Locate the script you run and select it.
4. Click on 'Execute command'
5. You must specify:
 - The tenant you wish to execute the script on
 - Any required parameters, including applying authorization policies.



NOTES:

- You may need to scroll down the page in order to see the list of parameters.
- Applying an authorization policy parameter only applies to those with Autopilot Classic roles.

6. Click on the 'Execute' button.

Nova will now submit a job for this script to be executed against the selected tenant. The following section explains how to check if the script ran successfully.

Reviewing the execution of a script

To verify that a script ran, follow these steps:

To run a script follow these steps:

1. In the left menu, select
2. **Manage > Jobs.**
3. Locate the script you ran, and review the status column to see if the script ran successfully or if it generated an error.

You can filter the list of jobs on the job screen in order to make it easier to find the required information.



NOTE: In normal operation, a notification will be generated when the job completes.

Delegated administration for custom PowerShell commands

A delegated administrator can also have access to execute custom PowerShell scripts. For this to occur, an administrator has to assign the delegated admin to an organizational unit containing a custom script commands within an authorization policy. These can be Meta-OU's, Tenant-OU's or regular OUs.



NOTE: As a delegated administrator, you are only allowed to run scripts you have been assigned to. You are forbidden to run any other custom script.

Supported types

The Custom PowerShell command which will be executed must have a param (...) block. The entire command is parsed and validated for **PowerShell 5**. The command must be syntactically correct in order to pass validation.

The following is a list of the supported types:

PowerShell	Field	Notes
-none-	Text	

PowerShell	Field	Notes
[string]	Text	(1)
[byte]	Number	(1)
[sbyte]	Number	(1)
[short]	Number	(1)
[ushort]	Number	(1)
[int]	Number	(1)
[uint]	Number	(1)
[ulong]	Number	(1)
[float]	Number	(1)
[double]	Number	(1)
[decimal]	String	(1)
[bool]	Boolean	(1)
[switch]	Boolean	
-other-	String	

(1) Accepts CLR type name, eg System.String, System.UInt32, System.Boolean, etc

Recognized attributes

[Parameter]

- Mandatory is supported. Mandatory fields must be provided when user tries to execute script. Mandatory [bool] and [switch] parameters should be avoided. While most of values (\$null, 1, "true", ...) can be converted to boolean value, user should use either [Parameter(Mandatory)] or [Parameter(Mandatory = \$true)].
- ParameterSetName is not supported. Multiple parameter sets may cause script to be not executable.
- Other parameters properties are ignored.

[ValidateNotNullOrEmpty]

Parsing and saving

When a command is stored, the parser extracts known validation attributes and stores information in the parameter model. This information is then translated into DTO so the user interface can render the appropriate field.

The parser ignores validation attributes it can not recognize.

Here is example of parameters and corresponding extracted validation.

```
// param ($Foo)
{
    "name": "Foo",
    "isMandatory": false,
    "validateNotNullOrEmpty": false,
    ...
}
// param([Parameter(Mandatory)] [ValidateNotNullOrEmpty] $Foo)
{
    "name": "Foo",
    "isMandatory": true,
    "validateNotNullOrEmpty": true,
    ...
}
```

Triggering execution

The Custom PowerShell commands are execute from the 'Execute Command' button in the user interface.

Mandatory and required fields

Text fields

isMandatory	validate Not Null Or Empty	parameters value (execute request)	request is valid	Notes
false	false	{ }	true	
false	false	{ "Foo" : "" }	true	
false	false	{ "Foo" : null }	true	
false	false	{ "Foo" : "bar" }	true	
true	false	{ }	false	UI must send { "Foo" : "" }
true	false	{ "Foo" : "" }	true	

isMandatory	validate Not Null Or Empty	parameters value (execute request)	request is valid	Notes
true	false	{ "Foo" : null }	true	This is acceptable but "" is preferred.
true	false	{ "Foo" : "bar" }	true	
false	true	{ }	true	
false	true	{ "Foo" : "" }	false	
false	true	{ "Foo" : null }	false	
false	true	{ "Foo" : "bar" }	true	
true	true	{ }	false	Field is required
true	true	{ "Foo" : "" }	false	Field is required
true	true	{ "Foo" : null }	false	Field is required
true	true	{ "Foo" : "bar" }	true	

Boolean fields

isMandatory	parameters value (execute request)	isValid	Notes
false	{ }	true	
false	{ "Foo": false }	true	
true	{ }	false	
true	{ "Foo" : true }	true	

Example scripts

Create a user, using the Microsoft Entra ID module:

```

param(
  [Parameter(Mandatory=$true)] $displayname,
  [Parameter(Mandatory=$true)] $givenName,
  [Parameter(Mandatory=$true)] $surName,
  [Parameter(Mandatory=$true)] $supn,
  [Parameter(Mandatory=$true)] $usageLocation,
  [Parameter(Mandatory=$true)] $nickname,
  [Parameter(Mandatory=$true)] $password,
  [Parameter(Mandatory=$true)] $skuname
)
$PasswordProfile = New-Object -TypeName
Microsoft.Open.AzureAD.Model.PasswordProfile
$PasswordProfile.Password = "$password"
New-AzureADUser -DisplayName "$displayname" -GivenName "$givenName" -
SurName "$surName" -UserPrincipalName $supn -MailNickName $nickname -
PasswordProfile $PasswordProfile -AccountEnabled $true
Set-AzureADUser -ObjectId $supn -UsageLocation $usageLocation
# Create the objects we will need to add and remove licenses
$license = New-Object -TypeName
Microsoft.Open.AzureAD.Model.AssignedLicense
$licenses = New-Object -TypeName
Microsoft.Open.AzureAD.Model.AssignedLicenses
# Find the SkuID of the license we want to add e.g. Win10_VDA_E3
$license.SkuId = (Get-AzureADSubscribedSku | Where-Object -Property
SkuPartNumber -Value "$skuname" -EQ).SkuID
# Set the Office license as the license we want to add in the $licenses
object
$licenses.AddLicenses = $license
Set-AzureADUserLicense -ObjectId "$supn" -AssignedLicenses $licenses

```

Create a new Microsoft Team, with some specified channels:

```

param(
  [Parameter(Mandatory=$true)] $TeamName,
  [Parameter(Mandatory=$true)] $desc,
  [Parameter(Mandatory=$true)] $TeamVisibility,
  [Parameter(Mandatory=$true)] $channelName1,
  [Parameter(Mandatory=$true)] $channelName2,
  [Parameter(Mandatory=$true)] $channelName3
)
$group = New-Team -DisplayName "$TeamName" -Description "$desc" -visibility
$TeamVisibility
New-TeamChannel -GroupId $group.GroupId -DisplayName "$channelName1"
New-TeamChannel -GroupId $group.GroupId -DisplayName "$channelName2"
New-TeamChannel -GroupId $group.GroupId -DisplayName "$channelName3"

```

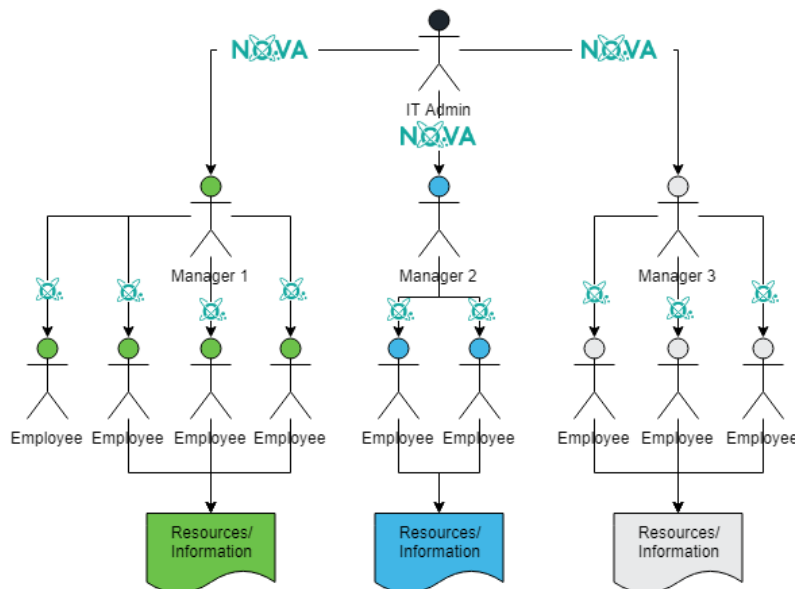
Delegated administration

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

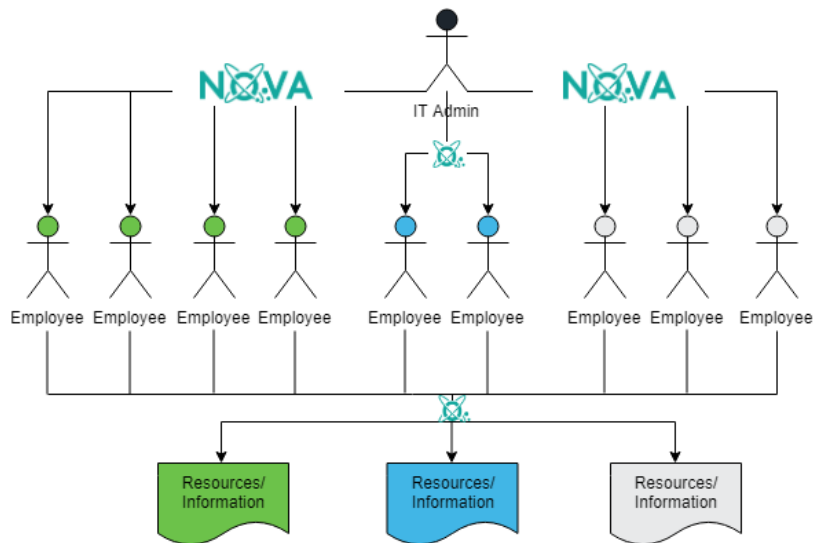


Self service

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:

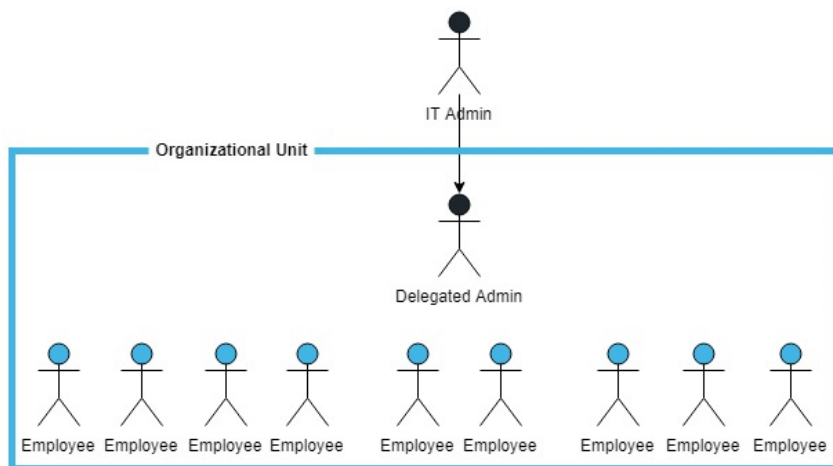
Example 2: IT Admin uses "self service" option, which gives users the ability to access Nova to manage some of their own information/resources



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



As you can see, Nova is highly customizable. In any of these examples, the administrator can specify which access rights managers/individuals/delegate administrators can assign to themselves and others.

Examples

Here are a few examples of delegated administration.

- A delegated administrator (maybe someone from the help desk) [resets a user's password](#).
- A delegated administrator can manage out of office messages.

Resetting a user password

It is easy to reset a user password with Nova, here are the steps:

1. Locate the user in the **Users** tab under **Manage**.
2. Bring up more detailed information about the user by clicking on the user.
3. Click **Authentication**.
4. Click **Reset password**.
5. Enter the new password and optionally force the user to change their password at the next login.
6. Click Save.

Nova will perform the password reset on your behalf, and a notification will be generated when the job completes.

Take a look at how to do these steps in [this quick video](#).

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.

Configure Nova DPC to use OAuth

1. Go to **Microsoft Entra ID**
2. Go to **Roles and Administration**
3. Locate the DPC application, as shown below:



Invite guest users to a tenant

1. On the create users screen, there is a new button called **Invite user**
2. When that button is clicked, a pop-up appears asking you to specify the target OU, and the email address of the person to be invited.
3. To enable a delegated administrator to easily see the type of user in a list of users, a new field was added:

Quest® Nova
Delegation & Policy Control



NOTE: When inviting guests it is expected that an underscore (_) will be used instead of the at sign (@) in domain names.

Search for external users or guests in a tenant

You can search for users in order to perform operations on them. In some Microsoft 365 tenants there might be guest accounts (also known as guest users, or external users).

In order to search for those users you can search for #EXT# in the **User principal name** field.

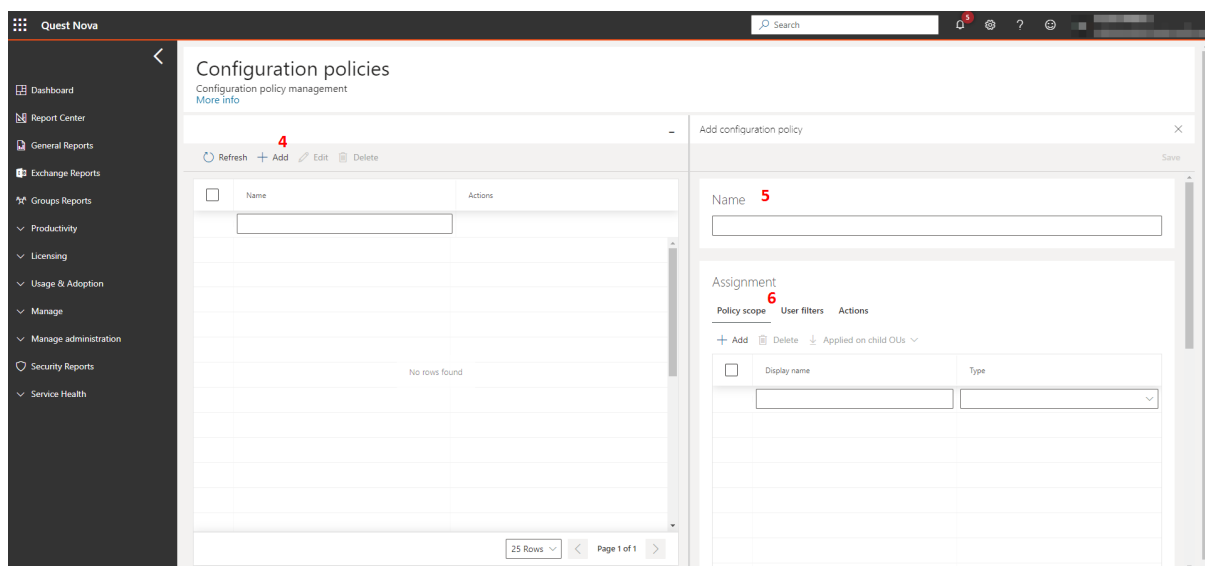
Take an action on all members of a Microsoft Entra ID security group

A configuration policy authorizes you to add actions onto groups or virtual organizational units to allow for standardization and consistency throughout your tenant. For example, you can change a users'/groups'/vOUs' Microsoft Entra ID details, add managers and so on. Look [here](#) for more information on configuration policies.

The best protocol in order to apply actions to an Microsoft Entra ID security group is to create a configuration policy scoped to the target group and not add a filter to that group. Let us go through how to do that.

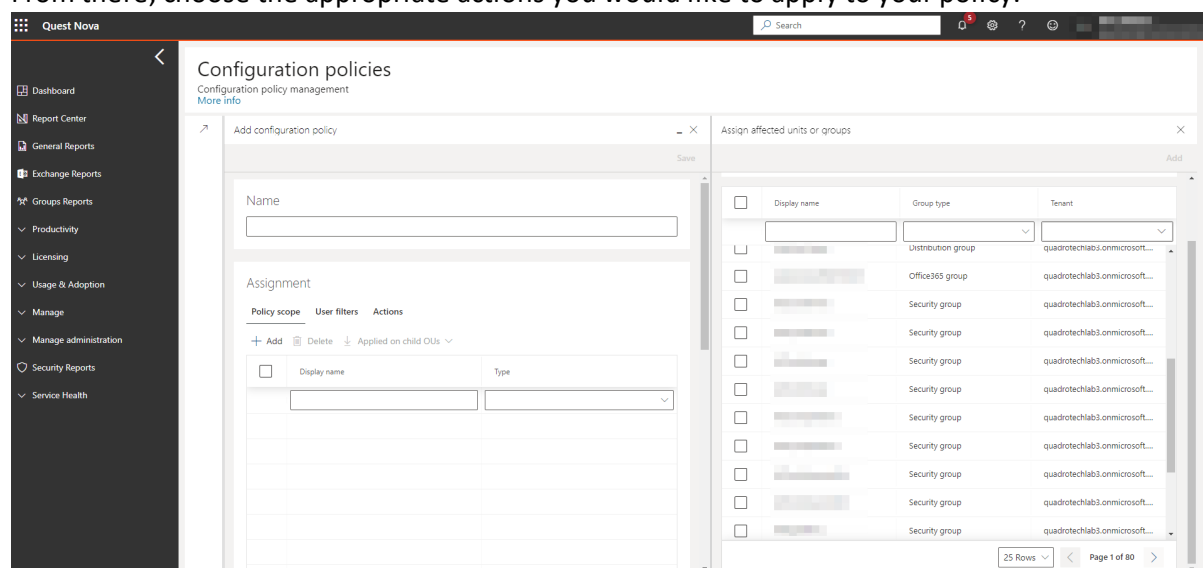
First, find the security group or groups you would like to add actions to. This can be found by going to **Nova > Manage > Groups**. Then select **Security group** from the drop down list under **Type**. Make a note of this, or add these groups to a virtual organizational unit. To do that, check out [this](#) page.

Now create the configuration policy for these groups/vOU. Go to **Manage Administration > Configuration policies**, then click **Add** then add a name to your policy. Then click **Add** on the *Policy Scope* section.



Then choose **Group** from the select type drop down list and select the security groups from your tenant. Alternatively, choose the vOU that you may have created.

From there, choose the appropriate actions you would like to apply to your policy.



Use the jobs page

Delegation & Policy Control (DPC) actions are completed via jobs. This article describes how to view, schedule, and restart jobs, and more.

Use the Jobs page to view all Nova jobs in various statuses. Apply filters to the list using fields in the top row. You can also sort the data by clicking on a column name. If the list 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.

Using the options at the top of the grid, you can manually add jobs, restart jobs, and set their priority.

Notice you can also customize the columns that display in the grid by clicking the Columns button and selecting/clearing options on the pop-up window.

Recurring jobs

Some jobs need to be performed more than once. For example, you might want the Get Mailboxes job to recur, so Nova checks regularly to see if new mailboxes have been 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.

Note: You can filter and sort the Job schedules page in the same ways you do with the Jobs page (as described above).

Adding a recurring job

Follow these steps to add a new recurring job:

1. Go to Manage Administration > Job schedules.
2. Click +Add.

3. Complete all required fields, and then click Save.

Editing or deleting a recurring job

Follow these steps to edit or delete a recurring job:

1. Go to Manage Administration > Job schedules.
2. Select the job you want to edit or delete.
3. Either:
 - Click Edit. Make desired changes, and then click Save.
 - Click Delete, and confirm the deletion.

i **NOTE:** You cannot edit or delete some recurring jobs, because they are required for Nova operations. For example, the Get Tenant Secure Score job. If you try to edit a required job, the Edit button is unavailable (grayed out).

DPC trial mode

Nova Delegation & Policy Control can be operated in two modes:

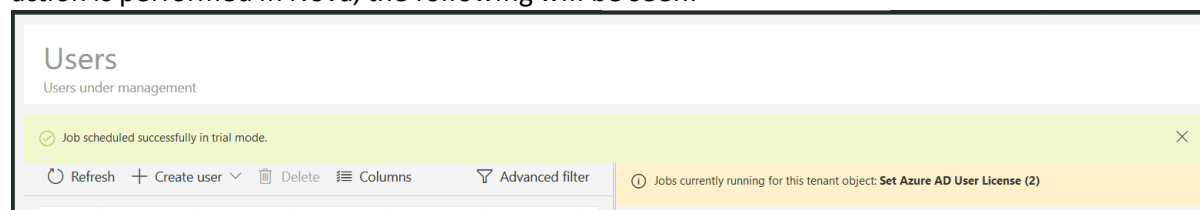
- Full subscription – this gives the users and administrators all of the actions and activities. Changes actually take place on the associated Microsoft 365 tenants.
- Trial subscription – in some cases a trial subscription may be associated with an Microsoft 365 tenant. In this mode full functionality is available, but changes **do not** take place on the tenant

What happens in 'trial mode'

When a trial subscription is added to an Microsoft 365 tenant in Nova, all of the policies, and all of the actions are still available, however the changes associated with performing an action **do not** take place on the tenant. For example, if you change a users password via Nova Delegation & Policy Control, it does not really reset the users password.

Using 'Trial Mode' can be very useful if you want to try the functionality, power, and features that Nova Delegation & Policy Control brings.

When trial mode is enabled, via a Nova Delegation & Policy Control trial subscription and an action is performed in Nova, the following will be seen:



The message says: 'Job scheduled successfully in trial mode'.

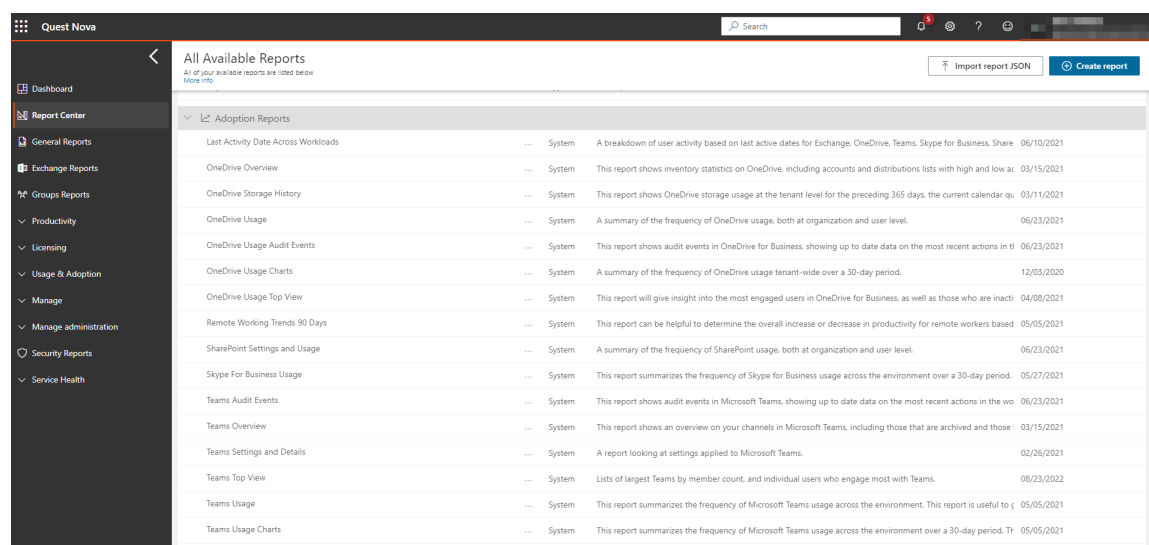
In addition, any jobs which complete, will be marked as follows:

<input type="checkbox"/>	Action	Description	Priority	Affected obj...	Tenant	Status	Completed	Last Update...
	<input type="text"/>	<input type="text"/>	▼	<input type="text"/>	▼	Comple... ▼		
<input type="checkbox"/>	Add Group...	Add a own...	3	Sales	Completed in trial	Completed i...	100 %	31. 5. 2019,...
<input type="checkbox"/>	Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
<input type="checkbox"/>	Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
<input type="checkbox"/>	Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
<input type="checkbox"/>	Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
<input type="checkbox"/>	Update Ch...		7	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...

The status will be shown as 'Completed in trial'.

Reporting

You will find Nova built-in reports right where you need them. You will find them in sub-menus related to associated operations. For example, if you want to know about things related to productivity, you can check the Mobile Device Overview report in the menu under Productivity. Or, if you want to know about usage and adoption of Microsoft Teams, you can check the Teams Usage report located under the Usage & Adoption menu option. Here is how it looks:

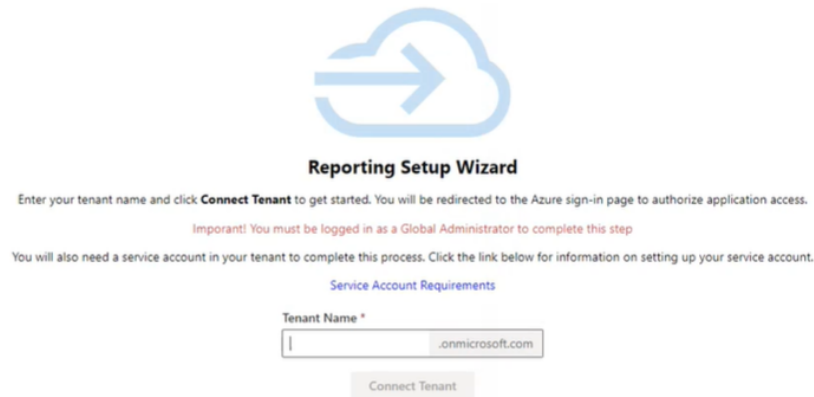


Nova reports are rich and customizable. Rather than having 10 or more mobile device reports, each showing part of the story around mobile device usage in an organization, those 10 reports are combined into one rich report with multiple sections. The condensed reports have a stunning level of detail and information, giving you a more complete picture of your organization's operations.

Reports can be also be delivered by email by scheduling them. You can also clone reports and edit the copy, upload report definition (.json) files, or use the powerful Report Center to build your own reports to suit your business needs.

Using the on-boarding wizard

Before you begin using Nova Reporting, you need to connect your tenant to the platform. This is completed through the on-boarding wizard. The steps to complete this are below.



The image shows a screenshot of the 'Reporting Setup Wizard' interface. At the top is a blue cloud icon with a right-pointing arrow. Below it, the title 'Reporting Setup Wizard' is centered. The instructions state: 'Enter your tenant name and click **Connect Tenant** to get started. You will be redirected to the Azure sign-in page to authorize application access.' A red warning message follows: 'Important! You must be logged in as a Global Administrator to complete this step'. Below that, it says: 'You will also need a service account in your tenant to complete this process. Click the link below for information on setting up your service account.' A blue link 'Service Account Requirements' is provided. The form has a label 'Tenant Name *' above a text input field. The input field contains a partial email address ending in '@onmicrosoft.com'. Below the input field is a grey button labeled 'Connect Tenant'.

Step 1: Connecting your tenant

Before proceeding, make sure to read the Microsoft [permissions](#) that you will need to accept in point 6 below.

1. Accept the invitation in your email to join the Quest Platform.
2. Check the 'Consent on behalf of your organization' box and click 'Accept'.
3. Go back to your emails, and follow the link to start using the platform.
4. Once you are within Nova, click 'My Organization'. This will direct you to the wizard.

i | NOTE: The following steps (5 and 6) must be performed by a Global Administrator.

5. Enter your tenant name and click 'Connect tenant'.
6. Click 'Accept'. Nova will then begin to connect your tenant. Click 'Next'.

Step 2: Data collection provisioning

1. Select a region for data collection depending on the needs of the environment. Once this has been provisioned, click 'next'.
2. Click 'Open Dashboard', which will navigate you to the Nova dashboard.

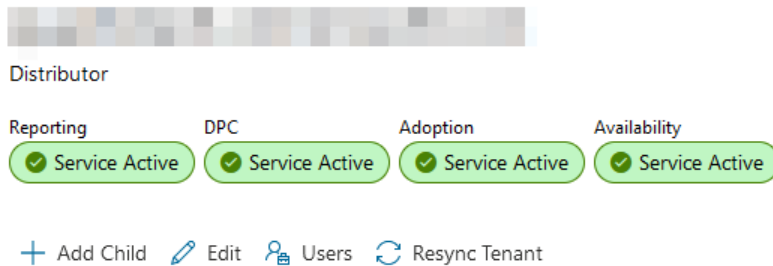
Step 3: Certificate-based authentication

You may need to use certificate-based authentication to use certain Nova services. For more on this, click [here](#).

How do I know that my Reporting license has been provisioned?

Licensing for your Nova Reporting subscription should be provisioned instantaneously upon on-boarding. To check this.

1. On the top left hand side, click the menu icon, and select **TMS Client**.
2. Under **My Organization**, check that the icon under Reporting has is green with a tick, as indicated below:



How do I know the length of my subscription?

You can check the length of your Reporting subscription, including start and end dates, by doing the following:

1. On the top left hand side, click the menu icon, and select **TMS Client**.
2. Under **My Organization**, on the right hand side, click the **Subscriptions** tab.
3. Here, you will find a list of the current subscriptions for each Nova feature.

Why am I being asked to approve new admin consent?

New permissions need to be granted consent to allow SharePoint functionalities to work correctly. To grant this new admin consent (using a global administrator account):

1. On the Nova dashboard, in the banner, click **New admin consent approval required**.
2. Login using a global administrator account.
3. Read and review the permissions.
4. Click **Accept**. This will take you back to the Nova dashboard.

Microsoft permissions for Reporting

To be granted access to Nova Reporting, you need to accept Microsoft permissions during the on-boarding process of connecting your tenant.

Permission	Permission Description
Microsoft Graph	
Directory.Read.All	Read directory data
Member.Read.Hidden	Read all hidden memberships
Policy.Read.All	Read your organization's policies
Azure Rights Management Services	
Content.DelegatedReader	Read protected content on behalf of a user
Content.SuperUser	Read all protected content for this tenant
Intune	
get_data_warehouse	Get data warehouse information from Microsoft Intune
get_device_compliance	Get device state and compliance information from Microsoft Intune
Microsoft Graph	
AccessReview.Read.All	Read all access reviews
AdministrativeUnit.Read.All	Read all administrative units
AuditLog.Read.All	Read all audit log data
Calendars.Read	Read calendars in all mailboxes
ChannelMessage.Read.All	Read all channel messages
Contacts.Read	Read contacts in all mailboxes
DeviceManagementApps.Read.All	Read Microsoft Intune apps
DeviceManagementConfiguration.Read.All	Read Microsoft Intune device configuration and policies
DeviceManagementManagedDevices.Read.All	Read Microsoft Intune devices

Permission	Permission Description
DeviceManagementRBAC.Read.All	Read Microsoft Intune RBAC settings
DeviceManagementServiceConfig.Read.All	Read Microsoft Intune configuration
Directory.Read.All	Read directory data
EduAdministration.Read.All	Read Education app settings
EduAssignments.Read.All	Read all class assignments with grades
EduAssignments.ReadBasic.All	Read all class assignments without grades
EduRoster.Read.All	Read the organization's roster
Files.Read.All	Read files in all collection sites
Group.Read.All	Read all groups
IdentityProvider.Read.All	Read identity providers
IdentityRiskEvent.Read.All	Read all identity risk event information
IdentityRiskyUser.Read.All	Read all identity risky user information
IdentityUserFlow.Read.All	Read all identity user flows
InformationProtectionPolicy.Read.All	Read all published labels and label policies for an organization
Mail.Read	Read mail in all mailboxes
Mail.ReadBasic	Read basic mail in all mailboxes
MailboxSettings.Read	Read all user mailbox settings
Member.Read.Hidden	Read all hidden memberships
Notes.Read.All	Read all OneNote notebooks
OnlineMeetings.Read.All	Read online meeting details
OrgContact.Read.All	Read organizational contacts

Permission	Permission Description
People.Read.All	Read all users' relevant people lists
Place.Read.All	Read all company places
Policy.Read.All	Read your organization's policies
PrivilegedAccess.Read.AzureAD	Read privileged access to Microsoft Entra ID roles
PrivilegedAccess.Read.AzureADGroup	Read privileged access to Microsoft Entra ID groups
PrivilegedAccess.Read.AzureResources	Read privileged access to Azure resources
ProgramControl.Read.All	Read all programs
Reports.Read.All	Read all usage reports
RoleManagement.Read.Directory	Read all directory RBAC settings
SecurityActions.Read.All	Read your organization's security actions
SecurityEvents.Read.All	Read your organization's security events
ServiceHealth.Read.All	Read service health
ServiceMessage.Read.All	Read service messages
Sites.Read.All	Read items in all site collections
TeamsActivity.Read.All	Read all users' teamwork activity feed
ThreatIndicators.Read.All	Read all threat indicators
TrustFrameworkKeySet.Read.All	Read trust framework key sets
User.Read (Delegated)	Sign in and read user profile
User.Read.All	Read all users' full profiles
Microsoft 365 Exchange Online	
Calendars.Read	Read calendars in all mailboxes

Permission	Permission Description
Calendars.Read.All	Read calendars in all mailboxes
Contacts.Read	Read contacts in all mailboxes
Exchange.ManageAsApp	Manage Exchange As Application
Mail.Read	Read mail in all mailboxes
MailboxSettings.Read	Read all user mailbox settings
Place.Read.All	Read all company places
ReportingWebService.Read.All	ReportingWebService.Read.All
Tasks.Read	Read user tasks in all mailboxes
User.Read.All	Read all users' full profiles
User.ReadBasic.All	Read all users' basic profiles
Office Management APIs	
ActivityFeed.Read	Read activity data for your organization
ActivityFeed.ReadDlp	Read DLP policy events including detected sensitive data
ServiceHealth.Read	Read service health information for your organization
OneNote	
Notes.Read.All	View notes for all users
Power BI Service	
Tenant.Read.All	View all content in tenant
SharePoint	
Sites.FullControl.All	Have full control of all site collections
Sites.Read.All	Read items in all site collections

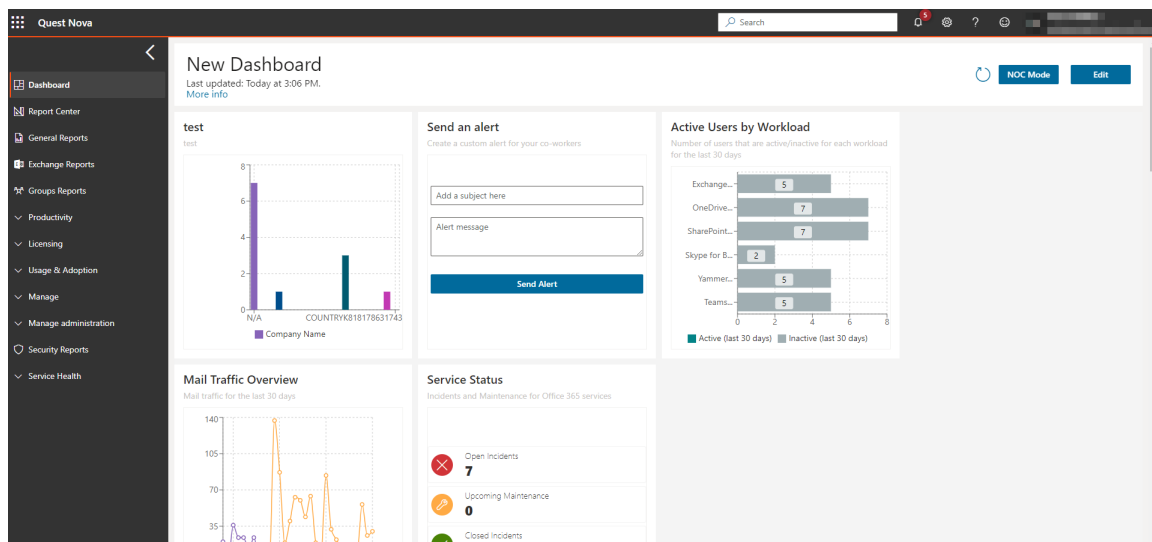
Permission	Permission Description
User.Read.All	Read user profiles

Dashboards

On the dashboard, you will see a variety of reports and widgets already pre-built into Nova, including Active Users by Workload, which shows the amount of users using and not using each Microsoft 365 workload in the previous 30 days.

Dashboards are where you can view your reports immediately; with data being updated every 24 to 48 hours, your dashboard gives you recent results on your Microsoft 365 environment straight away.

Here is an example of a dashboard that shows information about an Microsoft 365 tenant:



See dashboards in action in this video by clicking [here](#).

NOTE: The initial look of your dashboard will depend on your role within Nova.

There are several pre-existing widgets that you can add to your dashboard straight away. To do this:

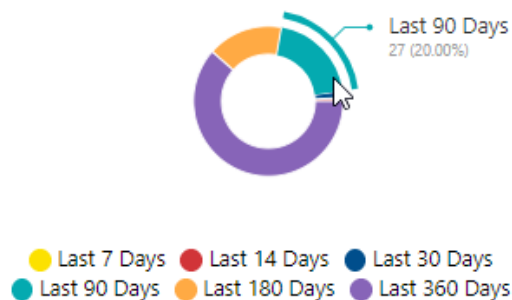
1. From the dashboard, click **Edit**, the **Add Widgets**.
2. Click on the report section you would like to add to the dashboard.
3. Click **Save**.

Interacting with the data

Many of the charts allow you to hover on segments and drill down to get more detail. For example, where we see the number of users who changed their password within a certain period of time, you can hover on that and you will see the precise amount of users who changed their password. Some other charts have a **View Data** button, which takes you to additional detail, which you can also download into a CSV file if required.

Last Password Change

When users last changed passwords



Dashboards can be edited and customized to meet your needs. You can change the title of the dashboard, move chart widgets around, remove widgets that are not needed, and add new widgets by dragging and dropping them from the list onto the page.

Change the title of a dashboard

You can change the title of a dashboard so it reflects the data within it. For example, if you have a dashboard that only reflects your environment's OneDrive data, you can change the title so the dashboard represents that. To do this:

1. From the dashboard, click **Edit** in the top right hand corner.
2. Click on the title box and input the your desired title.
3. Once done, click **Save**.

Configuring, cloning and/or removing widgets

Depending on the type of widget on the dashboard (public, private or system), you have configuration options for each widget. These are:

- **Configure widget:** this is where you can change widgets that you created using the configurable chart widget. You can not configure any pre-built widget without cloning them first.
- **Close widget:** you can clone system widgets, and then configure that cloned widget to suit your needs.
- **Remove widget:** Any widget can be removed from the dashboard.

To configure, clone or remove a widget:

1. On the dashboard, click **Edit** on the top right hand of the screen.
2. Click the **Spanner** icon on any widget, and choose your desired option.
3. Click **Save**.

Move and re-size widgets

You can move and resize widgets across your dashboard.

To move a widget:

1. On the dashboard, click **Edit** on the top right hand corner.
2. Click and hold the widget you would like to move, and drag to the location you would like it to be.
3. Click **Save**.

To resize a widget:

1. On the dashboard, click **Edit** on the top right hand corner.
2. Click and hold the arrow on the bottom right of the widget. You can resize it to your standards; the red preview box will show you how large the widget will be once its resized.
3. Click **Save**.

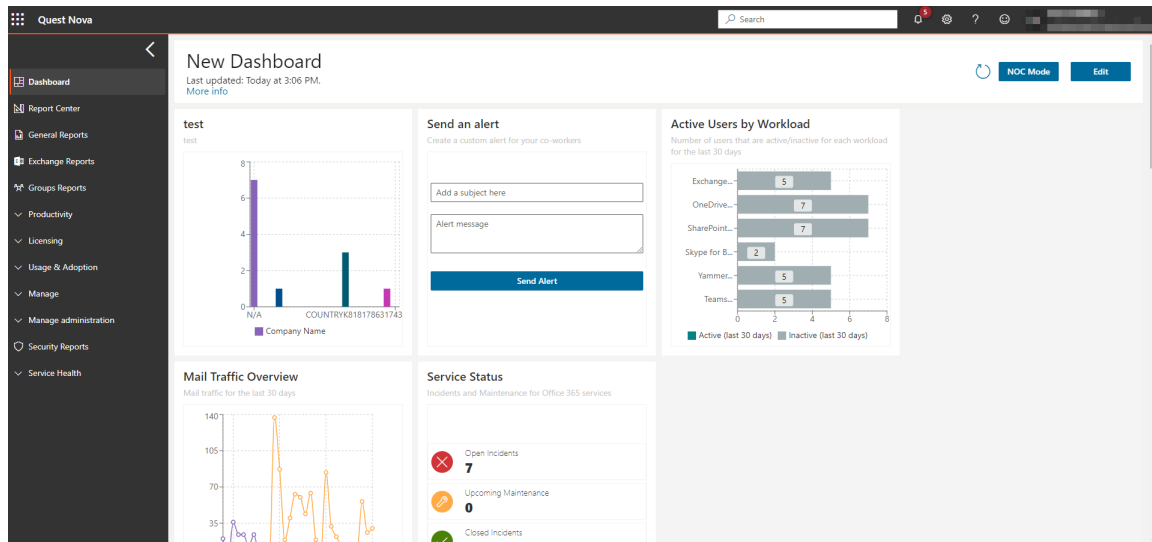
Refreshing the dashboard

On the top right hand of the dashboard, you will see a circular arrow icon. This button refreshes your dashboard and gives you real time results. Under the title, you will see when the dashboard was last updated.

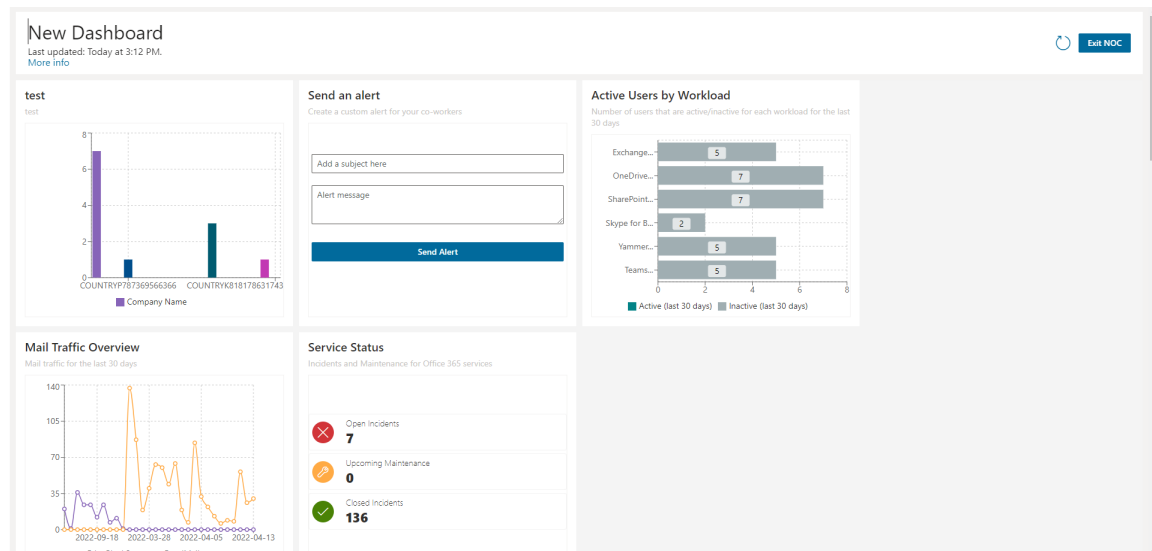


NOC mode

Network Operation Center mode (or NOC mode) clears the screen of all Nova user interface elements, leaving the chosen dashboard. The interface goes from this:



To this:



It is a perfect overview for call center, network operations, or help desk employees.

Creating a custom chart widget

Adding a custom chart widget to your dashboard follows similar steps as creating a section of a chart and pivot report, which will be covered later. This section will appear on your dashboard, which you can customize to your needs. To do that:

1. On the dashboard, click **Edit** in the top right hand of the screen.
2. Click **Add widgets**, then **Configurable Chart Widget**.
3. Enter a **Widget title** and a **Widget sub-title** if appropriate. Optionally, you can link your widget out to a report from within the Report Center.
4. Select a data source from the drop down list.

5. Select an organization and organization group, if applicable to your environment. These help to narrow down the scope of your reports.
6. Select a chart type. You can read more about chart types in the *Quest Nova Reporting Guide*.



NOTE: Only charts and pivots can be created for use in the dashboard. To create a report using any type of data presentation, use the Report Center.

7. Once you have selected your chart, choose an **Operator**. Operators are:
 - a. **Average:** This is calculated by dividing the total of all of the values by the number of values.
 - b. **Count:** The quantity of values in a data set.
 - c. **Sum:** The result of adding together the values in a data set.
 - d. **Min:** The smallest value.
 - e. **Max:** The largest value.
8. Select an **Applied to** data field. This is your Y axis. You can use the search boxes to find the exact data field you need, or filter by data type or data source.
9. Choose a **Series name** data field. This is your X axis. You can search for this the same way as the step above.
10. Optionally, choose a **category**. You can search for this the same way as step 8.
11. Add a **filter group**, if desired. Filtering allows you to narrow down the scope of your report. For example, you may only want to view users within a certain department or geographical location.
12. You can **sort** your data, if needed. Similar to step 8, you can search for a data field you would like to sort by ascending or descending order.
13. Set an **offset**. This is the starting record of your widget.
14. Set a **limit**. This is the maximum number of records returned within your widget.



NOTE: When downloading a section, this limit is ignored.

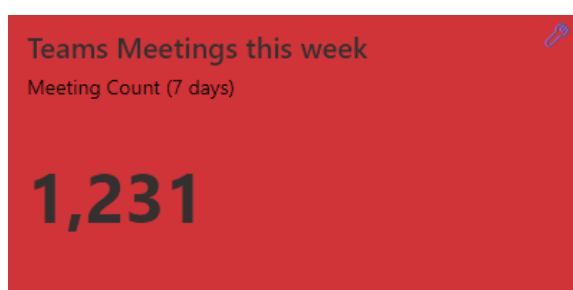
15. Select or deselect **Overflow**. This gathers data outside your limit into one section of a chart.
16. Choose your **drill down** fields.
17. Click OK, and your widget should appear in the dashboard. Click **Save** in the top right hand corner to finish the section.

Adding a card widget

If you would like to see a card presented on your dashboard, follow these steps:

1. From the dashboard, click **Edit** in the top right hand of your screen.
2. Click **Add Widgets** and select **Card Widget**.
3. Name your widget, and give it a title if necessary.
4. Create your card as you would with the steps above, and click OK.

Your card should now appear within the dashboard. If you have set analytics on your card, your card should display the color affiliated with the analytic you inserted.



i **NOTE:** You are able to move your card in the dashboard to a place of your convenience. Also, you are able to resize the widget to your standards. For more on Nova dashboards, [click here](#).

Nova Report Center

Microsoft has several different interfaces for tools used to perform Microsoft 365 management, reporting, and auditing tasks. In contrast, Nova users perform that work in a single user interface.

To achieve this, Nova gathers reporting and auditing data from Microsoft 365. Reporting data is collected about every 24 hours and auditing data is received from Microsoft when it becomes available. This data is stored in Nova for as long as the organization remains a subscriber, which is much longer than Microsoft typically stores this data in Microsoft 365.

The flexibility and power of the Nova Report Center is ideal for organizations with custom reporting needs that can not be fulfilled by the standard reports available in Nova. To create a report with the Report Center, you specify:

1. How you want the report to look. You decide what sections the report contains. Will it have charts, graphs, maps, or tables that will display the information?
2. The types of data the report will display. These are called data sources.
3. Any filters you want to apply against the data sources. For example, your data source might be a list of Microsoft Entra ID users. You might want to filter that list, so your report only shows users in North America or a certain department.

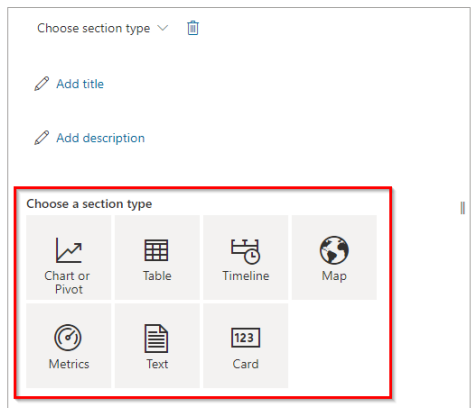
Just like other Nova reports, the reports created using Report Center can be saved, [scheduled](#), and shared. If you do not want to build an entirely new report, you could even clone an existing report and customize it to meet your new needs.

Here is more about the steps to set up a custom report:

Step 1: How will the report look?

Give a custom report structure by adding sections to control how it looks.

Here is where you select what section you will add to your report:



As sections are added to a report, you are asked to define the data source information you want to display in that section. The sections control how a custom report looks and the data sources give the report substance.

You can make sections display larger or smaller on the report, or you might drag and drop a section to another location on the report.

Step 2: What is the data source?

Reports created using Report Center are just templates, or shells. The service needs data for the shell to become a useful report. Nova gathers data from a variety of services, as described earlier in this section. Then, that data is collated, filtered, and displayed in the report.

After a data source is selected, you are asked to choose which fields related to the data source will display in the report. The report's data sources control what fields display and how they interact with other data sources on the report. Here is an example of a screen where you select the fields that display in a section:

Series name ⏏

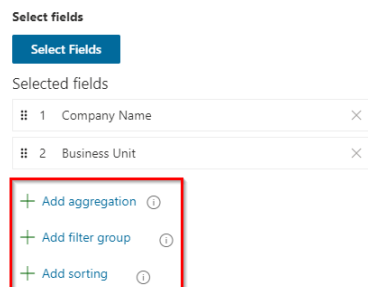
Field Name	Description	Data Type	Data Source
<input type="text" value="Field Name Filter / Search"/>	<input type="text" value="Description Filter"/>	<input type="text" value="String, Date, ..."/>	<input type="text" value="Azure AD Users, User Licen..."/>
<input type="radio"/> Account Enabled	A value indicating whether an account is enabled	Boolean	Azure AD Users
<input type="radio"/> Billing Code	The user's billing code	String	Azure AD Users
<input type="radio"/> Business Phones	The telephone numbers for the user	String	Azure AD Users
<input type="radio"/> Business Unit	The user's business unit	String	Azure AD Users

For more about data sources, go to this section.

Step 3: Do you want to filter or sort information displayed in a section?

You might add a filter to a section to show only a subset of data source information. For example, you could add a filter based on geography, so only users from a certain location display. You could add a filter that results in displaying a list of users from a specific department. Or, you could add a filter based on dates, so records older than X are filtered off the report. These are just a few examples. An organization can customize these to their specific needs.

You can also apply a sort order to a section. This is especially useful for table sections that show a list of information. For example, you can sort a list of users last name in ascending order, or you can sort that same list of users by who they report to.



These filters and sorts are saved as part of the report definition, so you will only have to configure them once.

To filter by date, check out [this](#) section.

Report Center terminology

If you are just getting started with the Nova Report Center, you may be unsure of some of the words and phrases that you encounter. Below are some common words and phrases related to Nova Report Center, along with descriptions.

It is important to differentiate what is meant between a **section** of a report and the **report** itself.

- A **Section** of a report are the individual charts, graphs and tables themselves. You can have one or multiple sections in a report.
- A **Report** is where individual data sections can be created, modified and stored.

Data sources

Data sources drive reports. They are the sets of information used to build reports. Choose a data source that is representative of the type of data you want to display. If you can not decide on a data source, you can clone one of the system reports to get started. To see more on data sources, [click here](#).

Organization

You can narrow the scope of your report to a specific organization within your tenant.

Organization Group

Select an organization group to further narrow the scope within your report.

Add Aggregation

For table reports, you can aggregate fields to get a specific count for that field. For example, let us say you want to quickly see how many Microsoft Entra ID users have been assigned to each department within your organization. You can do this by selecting **Department** as your table field, then select **Add aggregation**, then choose **Display Name** with **Count** as your operator. The amount of users within each department displays. This is useful if you need to know the number of objects within a data field.

Add Filter and Add Sorting

Filters and sorting are explained above. Note that you can use up to 5 filters within each section of your report. To learn more about filtering, click [here](#).

Offset

Set the starting record by applying an offset.

Limit

This is the highest number of results shown within the report. For example, if you have a limit of 20, then 20 entries display. Note that if you choose to download your report, the limit will be ignored and all data is shown.

Enable Paging

Useful for large data sets, paging allows you to see a select number of results per page before you need to move to the next page for more results. If this is disabled, all data displays in one table without having to page through results. If the report is downloaded, it will not be organized into pages.

Overflow

It is likely that your pie/bar chart will have a lot of data to show, resulting in a complex report that's not easy to analyze. Overflow aggregates calculations outside of your limit into one specific bar or pie wedge. For example, if you have a limit of 6 wedges or bars, any data from outside of your 6 biggest wedges or bars will be calculated and formed into one bar or wedge.

Customize and organize reports

Nova reports can be customized and organized.

Customizing reports

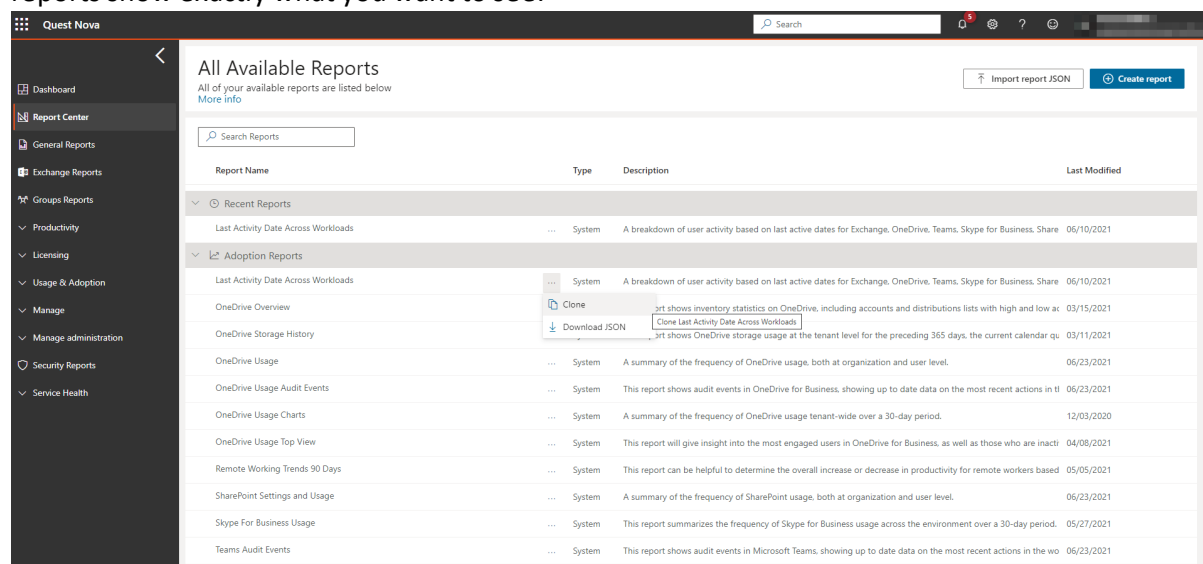
There are several ways to customize reports so they are specific to your organization. You can customize a report's sections and layout. You can customize the data source and fields used in each section. And, you can customize how information displays in each section by applying sorting and filters.

Searching reports

You can search for reports based on the title or description.

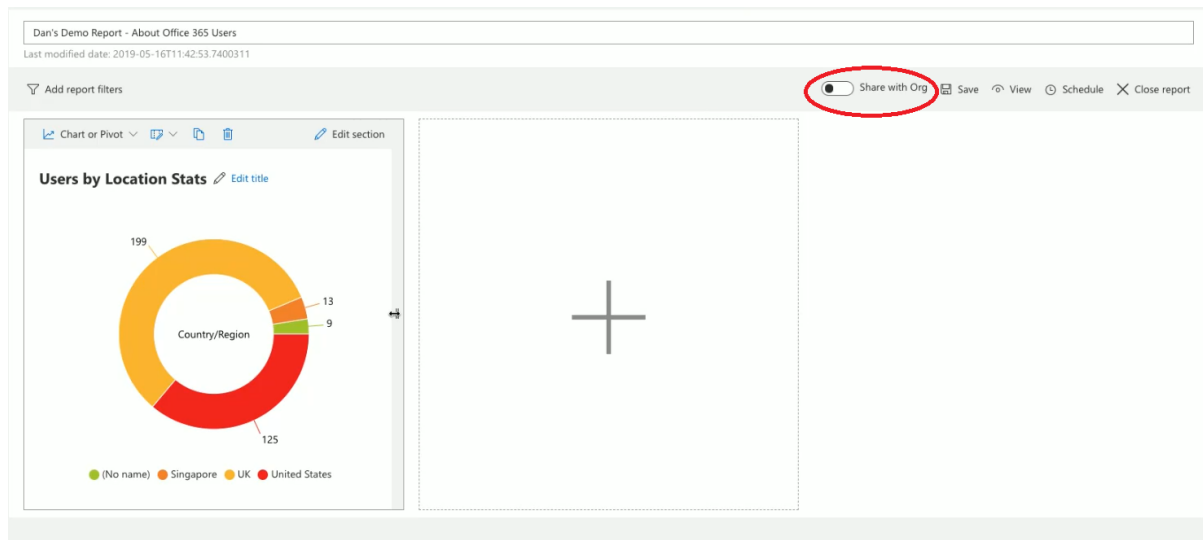
Cloning reports

You can clone any of the reports. After you give the new report a unique name, you can customize the new report by adding/removing sections, fields, and sorts/filters, so the new reports show exactly what you want to see.



Sharing reports across the organization

Organizing your organization's reports is easy, too. For example, you can share reports with the other Nova users from your organization.



Scheduling reports

You can [schedule reports](#) to be sent one time or periodically to stakeholders.

Importing and exporting report definitions

And, you can download a report definition, storing it for safe keeping. This is helpful in case the report definition gets edited by someone in your organization and you want to restore a previous version of the report. Here is how you can download a report definition:

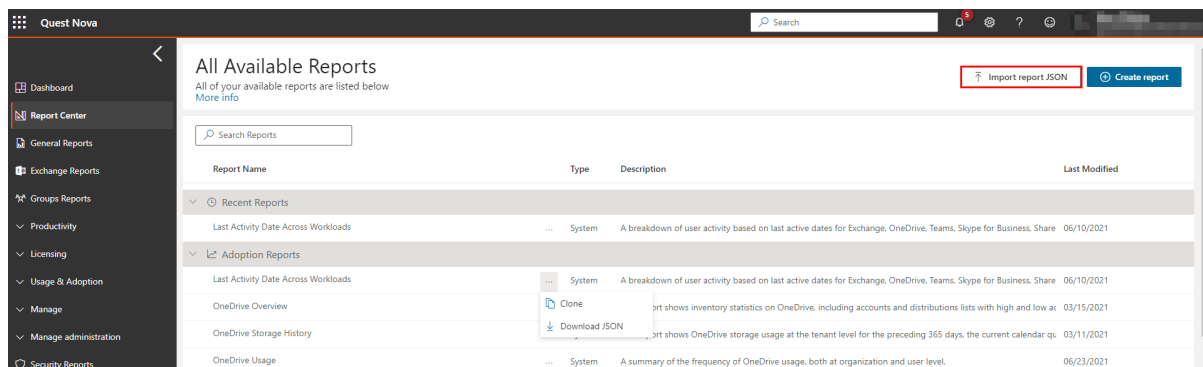
Quest Nova

All Available Reports
All of your available reports are listed below
[More info](#)

Search Reports

Report Name	Type	Description	Last Modified
Recent Reports			
Last Activity Date Across Workloads	System	A breakdown of user activity based on last active dates for Exchange, OneDrive, Teams, Skype for Business, Share	06/10/2021
Adoption Reports			
Last Activity Date Across Workloads	System	A breakdown of user activity based on last active dates for Exchange, OneDrive, Teams, Skype for Business, Share	06/10/2021
OneDrive Overview	System	Report shows inventory statistics on OneDrive, including accounts and distributions lists with high and low at	03/15/2021
OneDrive Storage History	System	Report shows OneDrive storage usage at the tenant level for the preceding 365 days, the current calendar qu	03/11/2021
OneDrive Usage	System	A summary of the frequency of OneDrive usage, both at organization and user level.	06/23/2021
OneDrive Usage Audit Events	System	This report shows audit events in OneDrive for Business, showing up to date data on the most recent actions in ti	06/23/2021
OneDrive Usage Charts	System	A summary of the frequency of OneDrive usage tenant-wide over a 30-day period.	12/03/2020
OneDrive Usage Top View	System	This report will give insight into the most engaged users in OneDrive for Business, as well as those who are inacti	04/08/2021
Remote Working Trends 90 Days	System	This report can be helpful to determine the overall increase or decrease in productivity for remote workers based	05/05/2021
SharePoint Settings and Usage	System	A summary of the frequency of SharePoint usage, both at organization and user level.	06/23/2021
Skype For Business Usage	System	This report summarizes the frequency of Skype for Business usage across the environment over a 30-day period.	05/27/2021
Teams Audit Events	System	This report shows audit events in Microsoft Teams, showing up to date data on the most recent actions in the wo	06/23/2021

And, here is how you import a report definition:



Creating a custom report

Here is an overview of the steps you will follow to create a new report.

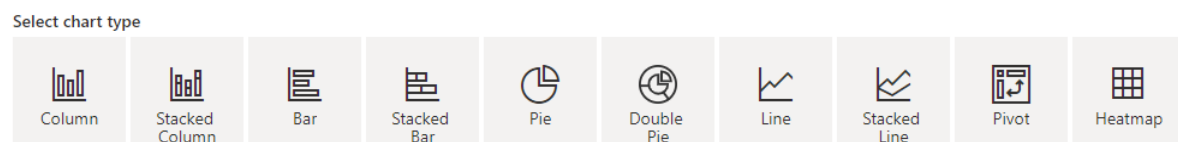
1. Select the Report Center option from the left menu bar.
2. Click **Create Report**, which is located in the top right corner of the page.
3. Enter a report name in the text field.
4. Click the + sign in the empty section to add a new section to the report.
5. Give the section a name in the Add Title field, and add a description if necessary, and select the tick icon to save the title and description.
6. Choose how you would like your data to be presented; choose between a [chart](#), [graph](#), [table](#), [timeline](#), or [map](#). Find more on data presentation types in the following sections.
7. Choose a data source, depending on the information you would like to present.
8. If necessary, choose an [organization and organization group](#).

From this point, the steps vary dependent on your choice of presentation type.

Creating a custom chart or pivot section

Charts and pivots give you a great range of graphs to view a variety of data across your tenant. Charts and pivots also give you access to view the many data sources Nova has on offer in easy to analyze diagrams.

9. Select your chart type. This includes the following types:



10. Choose your operator (average, count, sum, min, max).
11. Choose your Applied to field. This represents your Y axis.
12. Choose your Series name. This is your X axis.
13. Optionally, choose your category. This is additional information with your X axis.

14. If applicable, add sorting and [filters](#).

15. Add an offset and a limit.

- a. An Offset is the starting record for the section.
- b. The Limit is the number of records returned and visible within the report.

i | NOTE: When downloading a section, this limit is ignored.

16. Choose whether you would like the Overflow option. Setting an overflow will gather objects outside of a specific range into its only section.

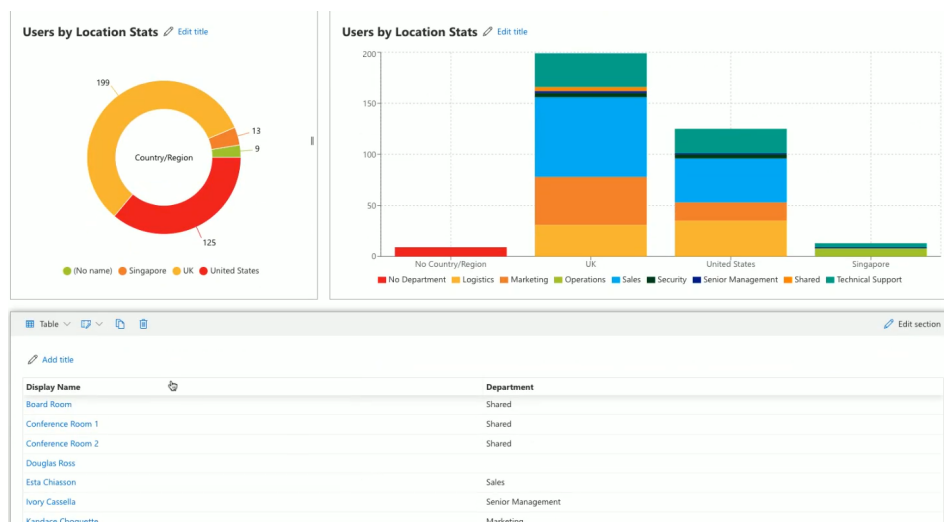
17. Optionally, choose whether to drill down data fields. These can be fields you have selected for your section, or other fields within the data source.

i | NOTE: You have the option to view the raw data in your chart.

You can now save your chart, and close the section.

Custom chart example: Microsoft Entra ID users by location

You can create an Microsoft Entra ID Users by Location report. The report shows your organization's Microsoft Entra ID users, broken down by location and department. This report could be helpful for planning helpdesk resources/staffing/coverage. The report includes a pie chart with the Microsoft Entra ID Users data source. The report's second section is a stacked bar graph with the Microsoft Entra ID Users data source. Finally, the report contains a table which shows users' display names, country/region and departments. Here is how the finished report looks:



Here are the steps to create this report:

1. Click **Create Report**.
2. Enter a report title, for example *Microsoft Entra ID Users by Location*.
3. You will add 3 sections to this report using the steps below:

Section One: Users by Location Stats

1. Add a section title, for example *Users by Location Stats*, and a description if necessary.
2. Choose the **Entra ID Users** data source under the **User Data** data source category.
3. Select the **Pie** chart type.
4. In the **Operator** field select **count**.
5. In the **Applied to** field select **Display Name**.
6. In the **Series name** field select **Country/Region**.
7. Save and close the section.

Section 2: Users by Location and Department

1. Add a section title, for example *Users by Location Stats*, and a description if necessary.
2. Choose the **Entra ID Users** data source.
3. Select the **Stacked Column** chart type.
4. In the **Operator** field select **count**.
5. In the **Applied to** field select **Country/Region**.
6. In the **Series name** field select **Country/Region**.
7. In the **Category** field select **Department**.
8. Click **Close** section.

Section 3: List of Users by Department

Find this section in the [tables](#) section of this guide.

After you are done adding sections, click Save.

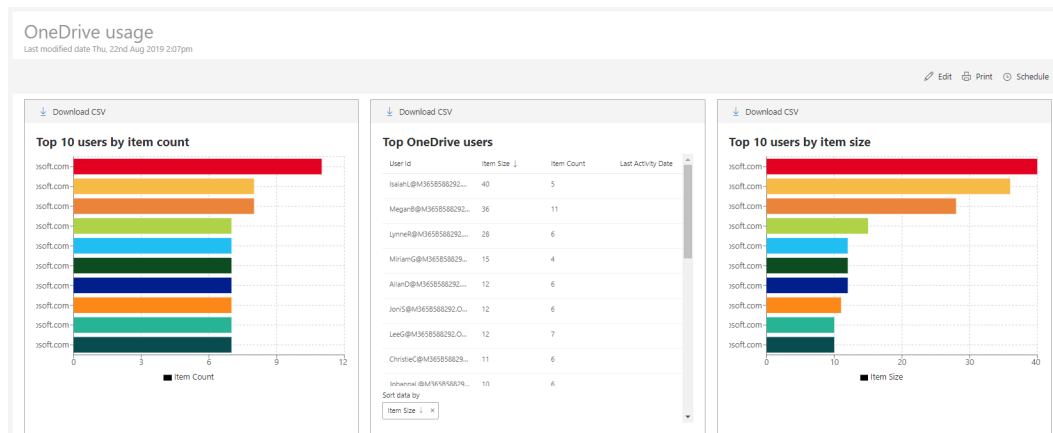
[Here is](#) a video going through these steps.

Custom chart example: OneDrive usage

You can create a OneDrive Usage report. The report shows:

- which of your users are using OneDrive for Business most (the most items and the largest items)
- vertical line bar graph with OneDrive User Data as the data source, sorted by item count (listed by user ID)
- a [table](#) that also uses OneDrive User Data as the data source. This table is sorted by item size.
- a vertical line bar graph with OneDrive User Data as the data source. This table is filtered by item size (results in this graph also listed by user ID).

Here is how the finished report looks:



Here are the steps to create this report:

1. From the dashboard, click Create Report.
2. Enter a report title, for example OneDrive Usage.
3. You will add 3 sections to this report using the steps below:

Section One: Top 10 Users by Item Count

1. Add a section title, for example Top 10 Users by Item Count.
2. Choose the **OneDrive User Statistics** data source under **OneDrive Data**.
3. Choose an organization and group, if applicable.
4. Select the **Column** chart type.
5. Under the Operator section, select **Sum**.
6. Under the **Applied to** section, click **Select field...**, and select **Item Count**.
7. Under the **Choose series name** field, click **Select field...**, and select **User Id**.
8. Click **Add sorting**, then **Select field...**, and select **Item Count**. Sort in **descending** order.
9. Under the **Offset** text field, put 0.
10. Under the **Limit** text field, put 10.
11. Un-check the 'Overflow' button.
12. Save and close the section.

Section 2: Top OneDrive Users

1. Add a section title, for example Top OneDrive Users.
2. Choose the **OneDrive User Statistics** data source.
3. Choose an organization and group, if applicable.
4. Click **Select field...**, and select **User ID**, **Item Size**, **Item Count**, and **Last Activity Date** in this order, and then close the dialog.

5. If desired, drag and drop the columns, to re-order them.
6. Click the **Add sorting** link, click **Select field...**, and then select **Item Size**.
7. If required, you can limit the amount of users in this table. Under the **Limit** text field, choose how many users you want in this table by changing the number.
8. Save and close the section.

Section 3: Top 10 Users by Item Size

1. Add a section title, for example Top 10 Users by Item Count.
2. Choose the **OneDrive User Statistics** data source under **OneDrive Data**.
3. Choose an organization and group, if applicable.
4. Select the **Column** chart type.
5. Under the Operator section, select **Sum**.
6. Under the **Applied to** section, click **Select field...**, and select **Item Size**.
7. Under the **Series name** section, click **Select field...**, and select **User ID**.
8. Click the **Add sorting** link, click **Select field...**, and select Item Size.
9. Sort in **descending** order.
10. Under the **Offset** text field, put 0.
11. Under the **Limit** text field, put 10.
12. Un-check the 'Overflow' button
13. Save and close the section.

After you are done adding sections, click Save.

Watch [this video](#) to see the above steps in action.

Custom chart example: License utilization

Here is another example of creating a report in the Nova Report Center.

Creating a report using License data sources allow you to get a scope of your license utilization within your tenant. This includes

- Assigned units – licenses applied to users
- Unassigned units – licenses not applied to users
- Idle units – licenses applied to users but are not being used i.e. disabled/deleted users

See below to view the steps on how to create a chart section on your license usage.

Click **Create Report**.

1. Enter a report title, for example License Utilization.

2. Click the plus sign to add a section to the report, and a description if desired.
3. Add a title and description for your section.
4. Choose the **Tenant License History** data source under the **License Data** data source category.
5. Click **column**.
6. Under operator, choose **Average**.
7. Under **Applied to**, choose **Percentage of Consumed Units**.
8. Under **Series name**, choose **License Name**.
9. Set your offset and limits if necessary.
10. Save, then close the section.

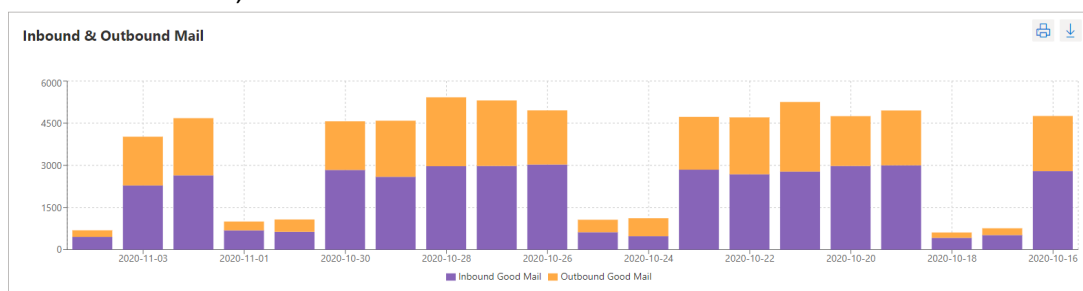
Custom chart example: Stacked inbound/outbound mail chart

Creating stacked graphs allows you to view multiple data fields in one easy to analyze chart. For example, in the chart below, we will create a stacked bar graph that shows the sum of inbound mail and outbound mail in one chart.

To begin creating your stacked chart:

1. Create a new section and give your chart a name.
2. Choose the **Office 365 Mail Traffic** data source under **Exchange Data**.
3. Choose **Stacked Column**. You can also select **Stacked Bar** or **Stacked Line** if you prefer.
4. For your operator, choose **Sum**.
5. For **Applied to**, choose **Inbound Good Mail** and **Outbound Good Mail**.
6. For **Series Name**, select **Scan Date**.
7. Add sorting, then select **Scan Date**. Choose descending from the drop down list.
8. Input your Offset and Limit. These are the amount of dates that appear in your chart.

The data should now appear within your section. Click close section, then save. This chart can download as a PDF, if desired.



Creating a custom table section

Tables are the best method to view a wide variety of data within one report. Unlike the other report types in the Report Center, tables allow you to view multiple fields with data that you select to suit your needs.

9. Select your data fields for your table. You can add as many fields as you require.
10. Add aggregation, sorting and [filtering](#) to your table.

NOTE: Aggregation brings the amount of items you have in a field together. For example, if users are involved in multiple departments, aggregating on the Department field with the Count operator will show the number of departments for that user, rather than the name of the departments.

11. Choose whether to enable paging. If paging is enabled, your table will be divided into multiple pages, depending on the amount of data collection for the section.

NOTE: Having paging enabled or disabled will not affect your download of your report; all data results will be listed within one table in your downloaded table.

12. Choose your initial page size. This is the amount of records within each page.

You can now save your chart, and close the section.

Custom table example: Spam and malware report (30 days)

You can create an Office 365 Spam and Malware report section that shows the number of spam and malware attempts over the last 30 days. The report section includes a table showing all fields related to the Office 365 Mail Traffic data source. It is sorted in descending order by scan date, and the results are filtered so only the last 30 days display. Here is how the finished report section looks:

Office 365 Spam and Malware report

Last modified date Wed, 21st Aug 2019 8:34am

Add report filters

Share with Org View Schedule Close report

Table Edit section

Spam and malware (30 days) Edit title

Table fields

Scan Date	Inbound Go...	Inbound Spa...	Inbound Spa...	Inbound Spa...	Outbound Go...	Outbound Ma...	Outbound Sp...	Outbound Sp...	Outbound Sp...
2019-08-20T00:00:00	234	2	0	18	39	0	0	0	0
2019-08-19T00:00:00	3485	78	0	602	2149	0	2	0	0
2019-08-18T00:00:00	1092	44	0	456	1842	0	1	0	0
2019-08-17T00:00:00	1222	23	0	405	568	0	0	0	0
2019-08-16T00:00:00	4599	111	0	663	2596	0	2	0	0
2019-08-15T00:00:00	3706	154	0	1083	2402	0	3	0	0
2019-08-14T00:00:00	3945	153	0	763	2572	0	1	0	2
2019-08-13T00:00:00	3553	136	0	514	1658	0	4	0	0
2019-08-12T00:00:00	3851	138	0	729	4031	0	3	0	0
2019-08-11T00:00:00	979	24	0	306	242	0	1	0	0

Click here to see how to create this report in your Nova Environment.

Here are the steps to create this report section:

1. Enter a section title, for example Office 365 Spam and Malware (30 days) and a description if necessary.
2. Choose the **Office 365 Mail Traffic** data source under the **Exchange Data** data source category.
3. Choose an organization and group, if applicable.
4. Click the Select field... link and select the following fields
 - a. Scan Date
 - b. Outbound Spam IP Block
 - c. Outbound Spam Envelope Block
 - d. Outbound Spam Content Filtered
 - e. Outbound Malware
 - f. Outbound Good Mail
 - g. Inbound Spam IP Block
 - h. Inbound Spam Envelope Block
 - i. Inbound Spam Content Filtered
 - j. Inbound Good Mail
5. Click **Add sorting**, then **Select field**, then select **Scan Date**, and make sure descending is selected.
6. Enter 31 in the **Limit** field.
7. Save and close the section.

[Here is](#) a video of these steps.

Custom table example: License utilization

However, what if we would like a table that includes the raw data, as well as data that shows assigned, unassigned and idle units? Let us see how we do that here

1. Enter a section title, for example License Utilization Table, and a description if required.
2. Choose the **Tenant Licenses** data source under the **License Data** data source category.
3. Under **choose table fields**, select, in this order:
 - a. License name
 - b. Percentage of consumed units
 - c. Assigned Units
 - d. Unassigned Units
 - e. Idle Units
4. Set your offset and limits if necessary.
5. Save, then close the section.

Check out [this video](#) on how to create this report below.

Custom table example: Assigned licenses over time


You may want to see assigned licenses for a specific license within your environment over a certain period of time. The step by step process below explains how to do that.



NOTE: Our license example is PowerBI, but use which license is relevant to your environment as you go through the steps.

See how to create this report.

1. Add a title and description for your section.
2. Choose the **Tenant License History** data source under the **License Data** data source category.
3. Select your organization and organization group, if necessary.
4. Under **Select fields**, choose:
 - The date of the statistics snapshot
 - License Name
 - Assigned Units
5. This will then show the amount of licenses you currently have assigned to **each** license you have within your environment. However, we want to see just the license assignment of **Power BI**. To do this, we need to click **Add filter group**.
6. On **Select field**, choose **License Name**.
7. On **Select operator**, choose **contains**.
8. In **Enter filter value**, enter *Power BI*.



NOTE: There are different license types with PowerBI. If you would like to search for a specific license i.e. Power BI Pro, instead of **contains** in select operator, choose **is equal to**, then enter *Power BI Pro*.
9. Enter your offset and limits.
10. Sort the date in ascending or descending order, depending on your preference.
11. Save your report.

Custom table example: List of users by department

This is a continuation of a report in the [charts and pivots section](#) of this guide. Below is a step by step guide on how to view your users by their associated department.

List of Users by Department

1. Click the plus sign to add a section to the report.
2. Click the **Table** section type to begin editing the section.
3. Add a section title, for example *Users by Department*.
4. Choose the **Entra ID Users** data source.
5. Choose an organization and group, if applicable.
6. Click the **Select fields...** link under **Choose table fields**

7. Select **Display Name**, **Country/Region** and **Department**, and close the dialog.
8. If desired, drag and drop the column names to re-order them.
9. Set your desired amount of data within your table by changing the number in the '**Limit**' text field.
10. Click Close section.

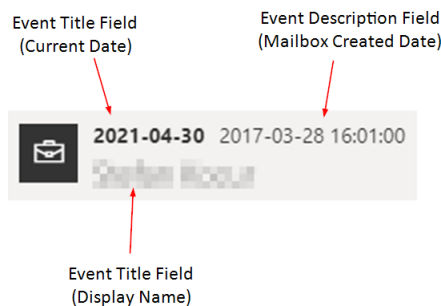
Creating a custom timeline section

Which data sources are recommended for timeline charts?

Any data source which contains time-based information can be used to create a timeline chart. The following is a list of data sources that we recommend to use for informative charts:


- Office 365 Audit Data
- Office 365 Mobiles Devices
- Detailed Message Statistics
- Microsoft Entra ID Users
- SharePoint Site Usage



Here is a diagram of the required fields for a timeline report:




9. Choose your event title, event description and event date fields. Use the diagram above to help you decide which field to select in each location.
10. Optionally, select your Event category field and any fields you would like to show in detail view.
11. Decide how you would like your timeline to look.
 - a. You can group your timeline by day, month or year.
 - b. You can view your timeline as either standard or micro.
 - i. Standard view presents a record in its entirety, but may not be suitable for large data sets.
 - ii. Micro view presents all records, but individual data sets must be hovered to be revealed.
12. Add [filters](#) if required.
13. Add an offset and/or a limit.



Individual records should now look like this:

 **2021-04-30** 2017-02-24 12:31:11



2021-04-30

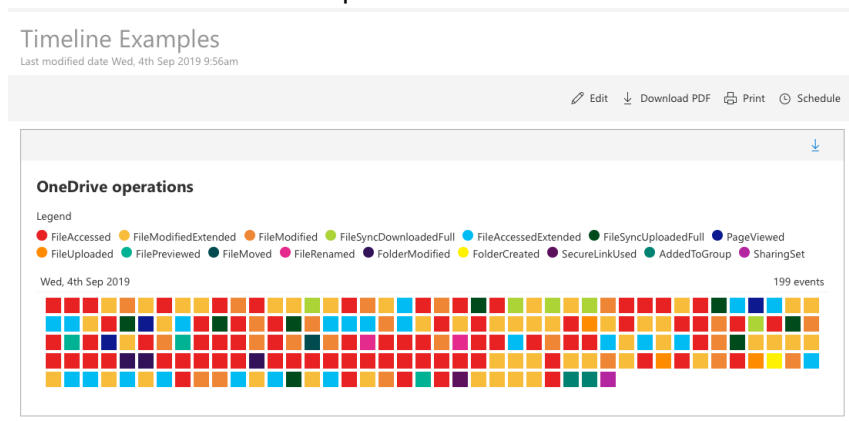
Full details

Department: Marketing

Job Title: Marketing Director

Custom timeline example: OneDrive operations

You create a section on a report that shows OneDrive operations, color-coded per operation. Here is how the finished report section looks:



Here are the steps to create this report section:

1. Enter a section title, for example *OneDrive Timeline*.
2. Choose the **Office 365 Audit Data** data source under the **Audit Data** data source category.
3. Choose an organization and group, if applicable.
4. Click the **Timeline** section type to begin editing the section.
5. Click the **Select field...** link under **Choose event title field**, and choose **Display Name**.
6. Click the **Select field...** link under **Choose event description field**, and choose **Operation**.
7. Click the **Select field...** link under **Choose event date field**, and choose **Creation Time**.
8. Click the **Select field...** link under **Choose event category field**.
9. In the **Event category field**, select **Operation**.
10. Click the **Select field...** link under **Choose fields to show in detail view**.
11. Expand the Microsoft Entra ID Users section, and choose these 6 fields: **Display Name**, **Department**, **Country/Region**, **Operation**, **Result Status**, and **Creation Time** in this order (Other fields can be added, if required).
12. Group your timeline by Day, Month or Year, depending on your preference.
13. In the drop-down list labeled **Choose view type**, select **Micro**, and enable the **Show legend** option.
14. Click **Add filter**.

15. Choose **Workload** is equal to **OneDrive**.
16. Save and close your section.

[Here is](#) a video running through these steps.

Creating a custom map section

Using the Map report allows you to see who has logged audit data within Nova. Has there been activity in a location which is unfamiliar to your organization? The map allows you to see if there is suspicious activity occurring in locations which your company is not associated with.



Each circle is representative of audit data being logged in that specific location, which can be viewed down to street level. The shade of the circle represents the amount of logs performed at that location.

To add the map report:

9. Add a title and description if necessary.
10. For the data source, choose Office 365 Audit Data.
11. Select your organization and organization group if necessary.
12. For select field, select Geo Location.
13. Save and close the section.

Creating a custom metric section

Using the metric report in the Report Center is a quick way to see:

- If you are reaching goals or targets that you want to reach. For example, emails being sent internally.
- If there are issues within your environment that may need investigation. For example, incoming spam email.

The gauge helps you see if you are reaching your target or limit, thus giving you insight into whether you are on course for a goal, or if you need to take action for your limits.



NOTE: Your data sources need to be a numerical value. If you are looking for a report with information about departments, locations, license names, etc., select another report type.

Check out this [Report Center article](#) for more information

9. Click Gauge.
10. Select your operator and Applied to data field.
11. Add a filter group, if applicable.
12. Select your minimum and maximum ranges. For example, you can set the maximum number to an acceptable limit of spam mail being received.
13. Reverse the colors of the metric if desired.

Once you have finished, click save and close the section.

Custom metric example: How many Teams meetings did we have in the last 30 days?

This metric sections is helpful if your organization hopes to have a certain number of Teams meetings within the month. To see a gauge related to the status of your target:

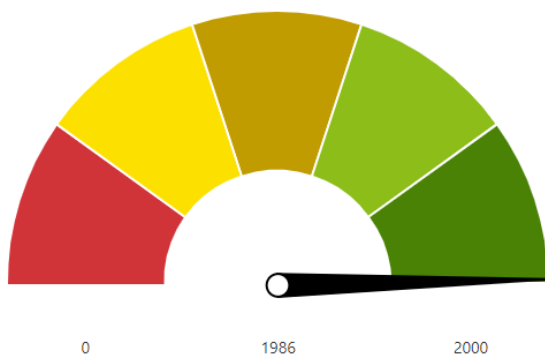
1. Add a title and a description, if necessary.
2. For your data source, click **Entra ID Users** under **Users Data**.
3. For select chart type, click **Gauge**.
4. For select operator, click **Sum**.
5. For **choose applied to**, select **Meeting count (30 days)** under the Teams User Activity Aggregate category.
6. Set your minimum and maximum numbers. Your maximum number in this example should be the number of Teams meetings you are targeting within your tenant within the previous month.

i **NOTE:** You may need to increase your maximum value to show your data.

7. Ensure the Reverse Colors checkbox is selected.
8. Close the section. Your report should now appear as a section.

How many Teams meetings have we had in the last 30 days? [Edit title](#)

We are looking to push the amount of Teams meeting our company [Edit](#)



Custom metric example: How many spam emails are we receiving?

Perhaps you are looking to get a clear metric on how many spam emails are coming in to your tenant, with a limit on what is acceptable. This metric gives a clear image on whether this limit is being reached. To create it:

1. Add a title and a description, if necessary.
2. For your data source, click **Office 365 Mail Traffic**.
3. For select chart type, click **Gauge**.
4. For select operator, click **Count**.
5. For choose applied to, select **Inbound Spam Content Filtered** under the Office 365 Mail Traffic category.
6. Set your minimum and maximum numbers. Your maximum number in this example should be the number of spam emails your administrator deems as acceptable.

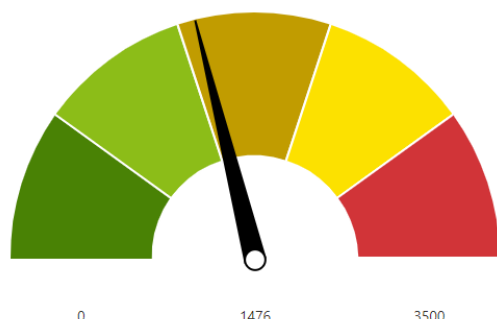
i **NOTE:** You may need to increase your maximum value to show your data.

7. Ensure the Reverse Colors checkbox is not selected.
8. Close the section. Your report should now appear as a section.

How many spam emails are we receiving?

[Edit title](#)

[Add description](#)



Creating a custom card section

Nova has a section type called 'Card'. Using this feature you can include simple sum, count, maximum, minimum or average values which might add useful additional information to your reports.

For example you could show the total count of mailboxes in an organization, or the number of users in a tenant, or the total size of all mailboxes in an organization.

In this section, we will see an example of how this can be done.

9. Select an operator and an Applied to data field.

10. Add a filter group, if applicable. For example, you may want to know how many Microsoft Entra ID users have their 'country or reigon' parameters set to the United States.
 11. Optionally, you can set analytics to 'color code' your card section. More on analytics is below.
- Click save, and close the section.



NOTES:

- The reports take a period of time to update to real time; this is usually between 24 to 48 hours. For more on this, click [here](#).
- You can add up to 6 cards in a report.

Analytics

The analytics tool is a quick way to see if a statistic in your environment is not as it should regularly be.

For example, you may want to immediately know the amount of spam mail coming into your tenant. You can select an operator relating to the value you want to input, for example you can have:

- greater than
- less than
- equal to
- is not equal to

then input a number. We can then apply the severity of the issue to the number applied. These include:

- OK
- Warning
- Critical

Analytics

Outbound Good Mail

greater than ▼

1500

OK ▼

×

Outbound Good Mail

1,714

Custom card example: Teams private message count (7 days)

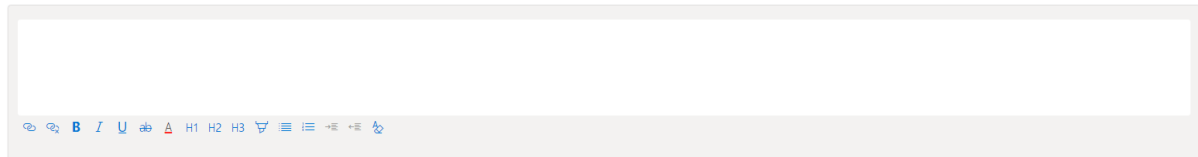
For example, you may want to keep an eye on the amount of Teams chats your users are sending if your environment has just adopted the Teams platform. You may also want to set a target for what you may deem acceptable. This can be achieved with the following steps:

1. Enter a card title, for example **Teams Chats (7 days)**.
2. For the data source, select **Teams User Activity Aggregate**.
3. Choose your organization and organization groups, if required.
4. For operator, select **Count**.
5. For **Applied to**, select **Private Chat Message Count (7 Days)**.
6. Under Analytics, select your **Operator**, **Value** and **Severity** to your needs.
7. Save and close the section.

Using text

You may need some overall context for the section(s) in your report for the report to make sense to new viewers. The text feature within the Report Center is a great method to help you expand on any additional information for either your report as a whole or for individual sections.

What is this report about? [Edit title](#)



There are a range of features you can use when creating your text section. These include but are not limited to:

- adding hyperlinks to words or phrases. Add additional links to external information.
- use headers to highlight different sections.
- use numbered lists or bullet points.

There is no character limit, so insert as much information as you need into your text section.

Filtering and sorting

Filtering your charts and tables and dates is easy to do. You are able to search within very specific time frames for a variety of data sources and data source categories.

To filter your data to within certain time frames:

1. Go to your chosen report that you have already created, or begin by [building one](#). Ensure that your report is one in which date is a valid property.
2. Go to **Add filter group**.
3. In **Select field...**, select the date property. This could take multiple forms, including Date, Activity Date, Created Date Time, Deleted Date Time, and so on. This depends on which data source you have selected.
4. Then select the parameters of your date filtering.

- With is newer than, these are dates AFTER your parameters. For example, is newer than 1 year is within the past year up to this point.
- With is older than, these are dates BEFORE your parameters. For example, is older than one year includes dates before the past year, not including the past year.

You are also able to add another filter so you can include dates within a specific time frame i.e. between 30 and 60 days. This is possible by clicking the plus button and repeating the steps above. Ensure that you have selected AND, rather than OR, if you are filtering between two dates. This can be seen in the image below.

The image shows a filter configuration interface. It features two filter rows connected by an 'And' operator. Each row consists of a field dropdown (set to 'Created Date Time'), a condition dropdown (set to 'is older than'), an 'Enter value' input field (with values 30 and 60), and a 'Select period' dropdown (both set to 'days'). Each row also includes a blue 'X' button to remove the filter and a blue '+' button to add another filter.

NOTE: A maximum of 10 filters can be added to a section of a report.

Filtering by QTD/YTD

It is possible to search within Quarter to Date (QTD) and Year to Date (YTD) metrics within the Nova Report Center for date-specific data fields.

+ Add filter group

The image shows a filter configuration interface. A filter is set for 'Activity Date' with the condition 'is during'. A dropdown menu for 'Select period' is open, showing options: QTD, YTD, previous month, previous quarter, and previous year. Below the filter, there are 'Add sorting' options with 'Offset' (0) and 'Limit' (500) fields.

The **QTD** parameter gives you data from the beginning of the current quarter, and ending at the current date.

The **YTD** parameter gives you data from the beginning of the current year, and ending at the current date.

For example, perhaps you want to see the amount of Microsoft Entra ID users created within the current year within your tenant. To do this:

- Begin by [creating a new report](#), including title and description if necessary.
- Choose your data source. For these specific filters, you will need sources that include date data fields. For our example, we are using **Microsoft Entra ID Users**.
- For **Table fields**, choose **Display Name** and **User Created**.
- Under **Add filter group**, select **is during**, then **YTD**.
- Add sorting and change your offset and limits if required.

Below is an example of what your report should look like.

User Created

is during

Select period

YTD

×

+

⊖ Add sorting

User Created

ascending

×

Offset

0

Limit

500

☒ Enable paging

Total number of results: 66

Display Name	User Created
	2020-01-06 10:55:46
	2020-01-08 10:07:01
	2020-01-08 15:15:53
	2020-01-16 10:06:02
	2020-01-27 16:30:49
	2020-01-29 09:01:54
	2020-02-05 12:33:12
	2020-02-17 09:28:22

Sorting

You can sort in ascending and descending order for any data field, even fields that you have not included in your report section. To add a searching parameter:

1. In your report section, click **Add sorting**.
2. Select the data field you would like to sort by.
3. Choose between ascending (smallest to largest, A-Z) and descending (largest to smallest, Z-A).

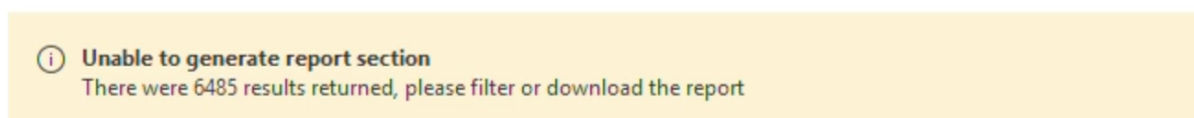
Alternatively, you can click on the heading of a table section to sort that specific field.

Filtering table data

There are three ways that table data can be filtered.

Filtering the Table

If you have a large report Nova might indicate that there are too many results to display them, like this:



Other times you might just want a subset of users, for example if you want users beginning with the letter D.

In these situations you can filter the data, by:

1. Clicking on 'Add Filter'
2. Choosing an appropriate field, like 'Display Name'.
3. Choosing an operator like 'Contains' or 'Begins with'
4. Entering the filter or search criteria.

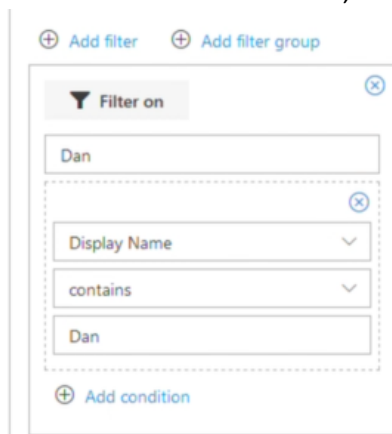
You can see how to do it in [this short video](#).

Global filtering

You can also do a global filter on a report to provide some helpful filtering to a user of the report.

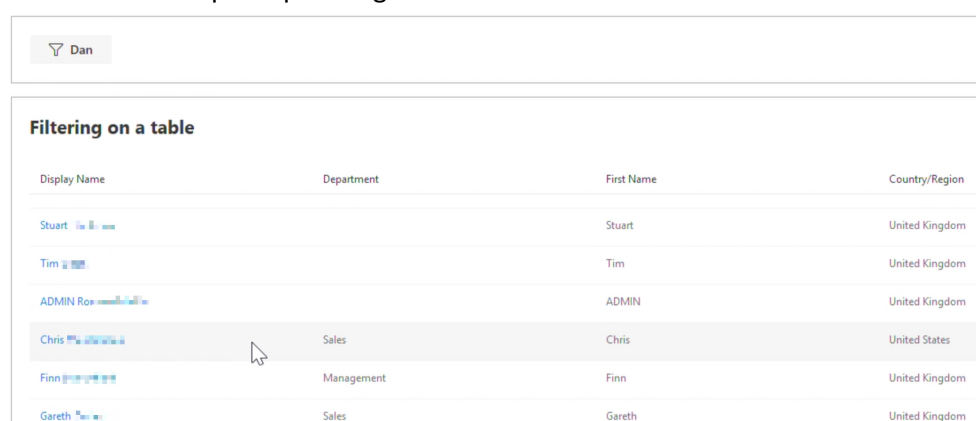
To do this you:

1. Click 'Add report filters' at the top of the report
2. Click 'Add filter'
3. Give the filter a name.
4. Click on 'Add condition'
5. Enter the filter criteria, for example 'Display Name', 'contains', 'Dan'.



Now at the top of the report you will see the filter, and it can be applied at any time, and can also be disabled at any time; giving you extra flexibility.

Here is how a simple report might be customized. Not filtered:



Display Name	Department	First Name	Country/Region
Stuart		Stuart	United Kingdom
Tim		Tim	United Kingdom
ADMIN Rox		ADMIN	United Kingdom
Chris	Sales	Chris	United States
Finn	Management	Finn	United Kingdom
Gareth	Sales	Gareth	United Kingdom

Filtered:

Dan

Filtering on a table

Display Name	Department	First Name	Country/Region
ADMIN		ADMIN	United Kingdom
Dan		Dan	United States
Dan	Marketing	Dan	United Kingdom
Dan		Dan	United Kingdom
Daniel	Development	Daniel	United Kingdom
Dan	Development	Dan	United Kingdom

Searching/Filtering after creating your report

On table data, you will also see filter/search boxes at the top of each column, so, on an existing report, you can quickly filter a working report to show just people in the Sales department for example:

User Details

Display Name ↑	Department	Country/Region
<input type="text"/>	<input type="text" value="Sales"/>	<input type="text"/>
Adam	Sales	United States
Bart	Sales	United States
Bei	Sales	United States
Chris	Sales	United States

And you can do that on any of the fields, or combine them to give you everyone in Sales in a particular country/region.

Filtering Examples

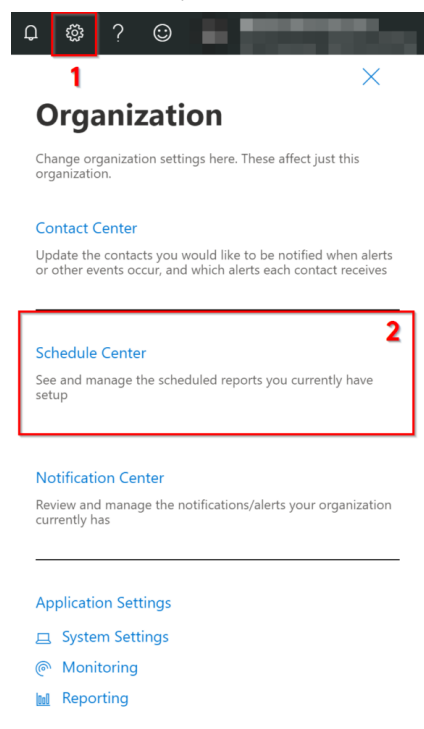
Check out some examples on how to filter your tables below:

[Date filtering](#)

Schedule Center

Use the Schedule Center to see and manage the scheduled reports you currently have set up. Schedules you set up in Nova Reporting are automatically added to the Schedule Center.

To access the Schedule Center, click the Settings button (a gear) located in the top right of the Nova window, and then select Schedule Center, as shown below.



It shows a list of previously scheduled reports, as shown below.

Schedule Center								
Current report schedules are shown below								
More info								
+ Add Report								
Report Name	Type	Last Run	Next Run	Start Time	Frequency	Creator	Recipients	
test1	...	Recurring Thu May 28 2020 2:40PM	Fri May 29 2020 2:38PM	Thu Mar 19 2020 1:38PM	Days	SP	1 recipient	
Robis scheduled report	...	Recurring Fri May 29 2020 10:30AM	Sat May 30 2020 10:28AM	Fri May 22 2020 10:28AM	Days	SP	1 recipient	
License availalbe report	...	Recurring Fri May 29 2020 10:05AM	Sat May 30 2020 10:00AM	Fri Apr 03 2020 10:00AM	Days	SP	1 recipient	
THMA - License witin in teantin	...	Recurring Fri May 29 2020 10:10AM	Sat May 30 2020 10:05AM	Fri Apr 03 2020 10:05AM	Days	SP	1 recipient	
Scheduled Department Sales US Last 7 days	...	Recurring Fri May 29 2020 8:40AM	Fri Jun 05 2020 8:35AM	Fri Apr 17 2020 8:35AM	Weeks	SP	2 recipients	
Scheduled MAOP -staging schedule PDF 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	SP	1 recipient	
Scheduled MAOP -staging schedule CSV 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	SP	1 recipient	
Scheduled Users list for active E3 users without...	...	Recurring Wed May 13 2020 11:45AM	Sat Jun 13 2020 11:42AM	Wed May 13 2020 11:42AM	Months	SP	1 recipient	
Weekly List of Licenses in tenant and individual...	...	Recurring Fri May 22 2020 1:45PM	Fri May 29 2020 1:40PM	Fri May 15 2020 1:40PM	Weeks	SP	2 recipients	
Scheduled Top Mail (clone)	...	Recurring Thu May 28 2020 2:35PM	Fri May 29 2020 2:31PM	Wed May 20 2020 2:31PM	Days	SP	1 recipient	

You will notice an ellipsis next to each scheduled report. Use the Edit button to change a report schedule, as shown here:

Schedule Center
Current report schedules are shown below
[More info](#)

[+ Add Report](#)

Report Name	Type	Last Run	Next Run	Start Time	Frequency	Creator	Recipients
test1	...	Recurring Thu May 28 2020 2:40PM	Fri May 29 2020 2:38PM	Thu Mar 19 2020 1:38PM	Days	...	1 recipient
Rob's scheduled report	...	Recurring Fri May 29 2020 10:30AM	Sat May 30 2020 10:28AM	Fri May 22 2020 10:28AM	Days	...	1 recipient
License availalbe report	...	Recurring Fri May 29 2020 10:05AM	Sat May 30 2020 10:00AM	Fri Apr 03 2020 10:00AM	Days	...	1 recipient
THMA - License witin in teantn	...	Recurring Fri May 29 2020 10:10AM	Sat May 30 2020 10:05AM	Fri Apr 03 2020 10:05AM	Days	...	1 recipient
Scheduled Department Sales US Last 7 days	...	Recurring Fri May 29 2020 8:40AM	Fri Jun 05 2020 8:35AM	Fri Apr 17 2020 8:35AM	Weeks	...	2 recipients
Scheduled MAOP -staging schedule PDF 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	...	1 recipient
Scheduled MAOP -staging schedule CSV 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	...	1 recipient
Scheduled Users list for active E3 users without...	...	Recurring Wed May 13 2020 11:45AM	Sat Jun 13 2020 11:42AM	Wed May 13 2020 11:42AM	Months	...	1 recipient
Weekly List of Licenses in tenant and individual...	...	Recurring Fri May 22 2020 1:45PM	Fri May 29 2020 1:40PM	Fri May 15 2020 1:40PM	Weeks	...	2 recipients
Scheduled Top Mail (clone)	...	Recurring Thu May 28 2020 2:35PM	Fri May 29 2020 2:31PM	Wed May 20 2020 2:31PM	Days	...	1 recipient

Schedule Center
Current report schedules are shown below
[More info](#)

[+ Add Report](#)

Report Name	Type	Last Run	Next Run	Start Time	Frequency	Creator	Recipients
test1	...	Recurring Thu May 28 2020 2:40PM	Fri May 29 2020 2:38PM	Thu Mar 19 2020 1:38PM	Days	...	1 recipient
Rob's scheduled report	...	Recurring Fri May 29 2020 10:30AM	Sat May 30 2020 10:28AM	Fri May 22 2020 10:28AM	Days	...	1 recipient
License availalbe report	...	Recurring Fri May 29 2020 10:05AM	Sat May 30 2020 10:00AM	Fri Apr 03 2020 10:00AM	Days	...	1 recipient
THMA - License witin in teantn	...	Recurring Fri May 29 2020 10:10AM	Sat May 30 2020 10:05AM	Fri Apr 03 2020 10:05AM	Days	...	1 recipient
Scheduled Department Sales US Last 7 days	...	Recurring Fri May 29 2020 8:40AM	Fri Jun 05 2020 8:35AM	Fri Apr 17 2020 8:35AM	Weeks	...	2 recipients
Scheduled MAOP -staging schedule PDF 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	...	1 recipient
Scheduled MAOP -staging schedule CSV 7:15	...	Recurring Fri May 29 2020 6:15AM	Sat May 30 2020 6:15AM	Tue Apr 28 2020 6:15AM	Days	...	1 recipient
Scheduled Users list for active E3 users without...	...	Recurring Wed May 13 2020 11:45AM	Sat Jun 13 2020 11:42AM	Wed May 13 2020 11:42AM	Months	...	1 recipient
Weekly List of Licenses in tenant and individual...	...	Recurring Fri May 22 2020 1:45PM	Fri May 29 2020 1:40PM	Fri May 15 2020 1:40PM	Weeks	...	2 recipients
Scheduled Top Mail (clone)	...	Recurring Thu May 28 2020 2:35PM	Fri May 29 2020 2:31PM	Wed May 20 2020 2:31PM	Days	...	1 recipient

This will bring you to the schedule screen, as seen in the images below.

Naming and describing the report

New Report Schedule



Schedule Name *

Scheduled Inbound & Outbound Mail

Description (optional)

Scheduling the report (time, date and frequency)

New Report Schedule



When would you like your report? *

☐ Now

☒ Later

Date

Thu May 27 2021



Time

02:15 PM



Select Report Frequency *

☐ One Off

☒ Recurring

Every

7



Days



Adding recipients for the report

New Report Schedule



Add Recipients

Search Contacts & Directory



Selecting the format for the report

New Report Schedule



Select report format *

☐ CSV

☒ PDF

Finalizing your scheduled report

New Report Schedule

✓	Name	Scheduled Inbound & Outbound Mail
✓	Description	
	Frequency	Days
	Start Date	Thu May 27 2021 2:15PM
	Format	PDF
	Recipients:	<div></div> <div></div>

Done

For example, you could schedule a subscription overview report to be sent to the CTO at the beginning of each month, so they can see how many Microsoft 365 licenses are being used and are available across the organization.

A video regarding the Schedule Center can be seen [here](#).

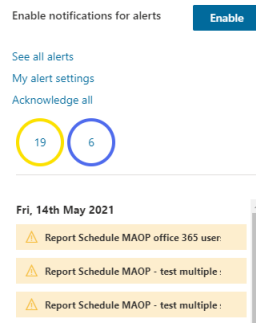
Notification Center

The notification center is where you will see Nova-based alerts and notifications across your organization. Find an overview of your notifications by clicking the bell icon in the banner.

To be notified when a new alert is registered, click **Enable**, then **Allow** based on your browsers settings.

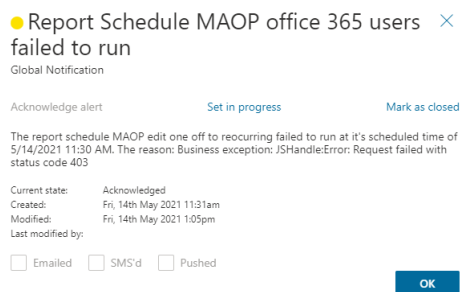
From here, you will see an overview of alerts, sorted by date and its critical status.

Alerts



Going into detail on a notification

To see an alert in more depth, click on the notification bell, then click on an alert. You will see a screen similar to the one below.



From here, you will see:

- What the alert is about
- When the alert happened
- The reason for the alert
- The alert's current state
- When the alert was created
- When the alert was last modified
- Who modified the alert
- If the email was emailed out, sent by SMS or pushed within the application, depending on how you configured the settings.

Dashboard

By clicking on the bell icon, and then click **See all alerts**, it will take you to the Notification Center dashboard.

Here, you can see all alerts that have been registered since the beginning of your subscription. From the dashboard, you can:

- Sort by Severity, Alert Name, Alert Source, Alert State and Date Added.

- Choose the columns you would like in the dashboard by clicking the plus (+) icon in the top right corner, and select/deselect as appropriate.
- Mark each alert as in an **Acknowledge**, **In Progress** or **Closed** state by either:
 - Clicking on the ellipses and selecting the appropriate alert state.
 - Clicking on the check box to the left of the alert, clicking **Manage**, then selecting the appropriate alert state.
- Click on the ellipses and select **Details** to view the details of the alert, similar to above. You can also select your alert state from here.

Alert severity

Alert severity gives you information on the status of an alert, and if attention or action is needed:

- **Informational:** These alerts describe events that have occurred within your tenant that you do not need to take action on. An example of an informational alert is notifying you that a scheduled report has been successfully sent.
- **Healthy:** A healthy notification alerts you that a critical error has successfully been resolved.
- **Degraded:** A degraded alert arises when an error occurs that needs attention. An example is when a scheduled report is unsuccessfully sent. Viewing the details shows you specifically what the error is and why it failed.
- **Critical:** A critical alert is a notification that needs immediate attention.

Alert settings

Alert settings are where you can set up notifications to be sent via email, SMS or pushed to you within Nova. You can find alert settings by clicking on the bell icon, then **My alert settings**.

If you would like to be sent notifications via email and/or SMS, enter your details within the **Personal Details** tab.

In the **Settings** tab, you can set up alerts for a range of categories (**Nova**, **Billing** and **Global**), and customize notifications depending on what you need to be notified about. For example, you can set up SMS notifications for Degraded alerts and receive push notifications and emails for Critical alerts. View the image below for an example of how you can set up notifications.

Edit Contact: [Name] [Email] [Phone]

Personal Details Settings

	NOVA	BILLING	GLOBAL
Get Alerts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Critical	SMS, Email, Push Notifications	Push Notifications	SMS, Email
Degraded	Push Notifications, Email	Email	Push Notifications
Healthy	SMS	Select options	Email
Info	SMS	SMS	Email

Cancel Save

Alert source

Alert sources are where your alerts are coming from. These sources are **DPC, Radar, Reporting, Workflow, Accounting** or **Other**.

Alert states

Alerts have four stages that can be changed by a user. Those are:

- **New:** The notification has entered the system and has not been looked into by any user.
- **Acknowledged:** The notification has been opened by a user.
- **In progress:** A user is investigating the notification.
- **Closed:** The notification has been investigated.

To change an alert level, click on a notification as described above, and click on either **Acknowledge alert, Set in progress** or **Mark as closed**.

Custom Alert Center

The Custom Alert Center notifies users when there is a change to their organization. Users can build alerts based on a custom set of conditions and filters through a wide range of data sources.

On the Custom Alert Center screen, you will see:

- **Alert Name** - the name of the alert
- **Active Status** - if the alert has been enabled or disabled
- **Date Added** - the date in which the alert was created
- **Last Trigger** - when the alert was last triggered based on the conditions
- **Creator** - the name of the user who created the alert

To build a custom alert:

1. From the Nova dashboard, click the cog icon, and select **Custom Alert Center**.
2. Click **Add Custom Alert**.
3. Click **Add Alert Name**, and enter the alert name. Click **Save a name** when completed.
4. Enter the user email in which the alert should be sent to.
5. Optionally, to add more user emails, click the plus icon and enter the user email.
6. Select the data source in which you would like to be notified about.

7. Click **Add alert condition**, and select the field, operator and value of the data source. This defines the condition of the alert. You can also add multiple conditions by following the same step.
8. Click **Save**. The chosen user(s) will now be alerted based on the defined conditions.

By clicking on the ellipses next to the alert, you can take the following actions:

- Edit - change the alert
- Disable - disable the alert
- Delete - delete the alert

Use Case: Low E3 Licenses

As an example, you may want to be alerted when the number of E3 licenses in a tenant are lower than a threshold you desire. To be notified about this:

1. From the Nova dashboard, click the cog icon, and select **Custom Alert Center**.
2. Click **Add Custom Alert**.
3. Click **Add Alert Name**, and enter the alert name. Click **Save a name** when completed.
4. Enter the user email in which the alert should be sent to.
5. Optionally, to add more user emails, click the plus icon and enter the user email.
6. Select the **Tenant Licenses** data source, under the Tenant Licenses category.
7. Click **Add alert condition**, and select License Name.
8. Select the operator as **contains**.
9. In the text field, enter **E3**.
10. Click **Add alert condition**, and ensure the clause is **And**.
11. Select **Unassigned Units**.
12. Select the operator as **less than**.
13. Enter the desired number of licenses.
14. Click **Save**. The chosen user(s) will now be alerted based on the defined conditions.

How To...

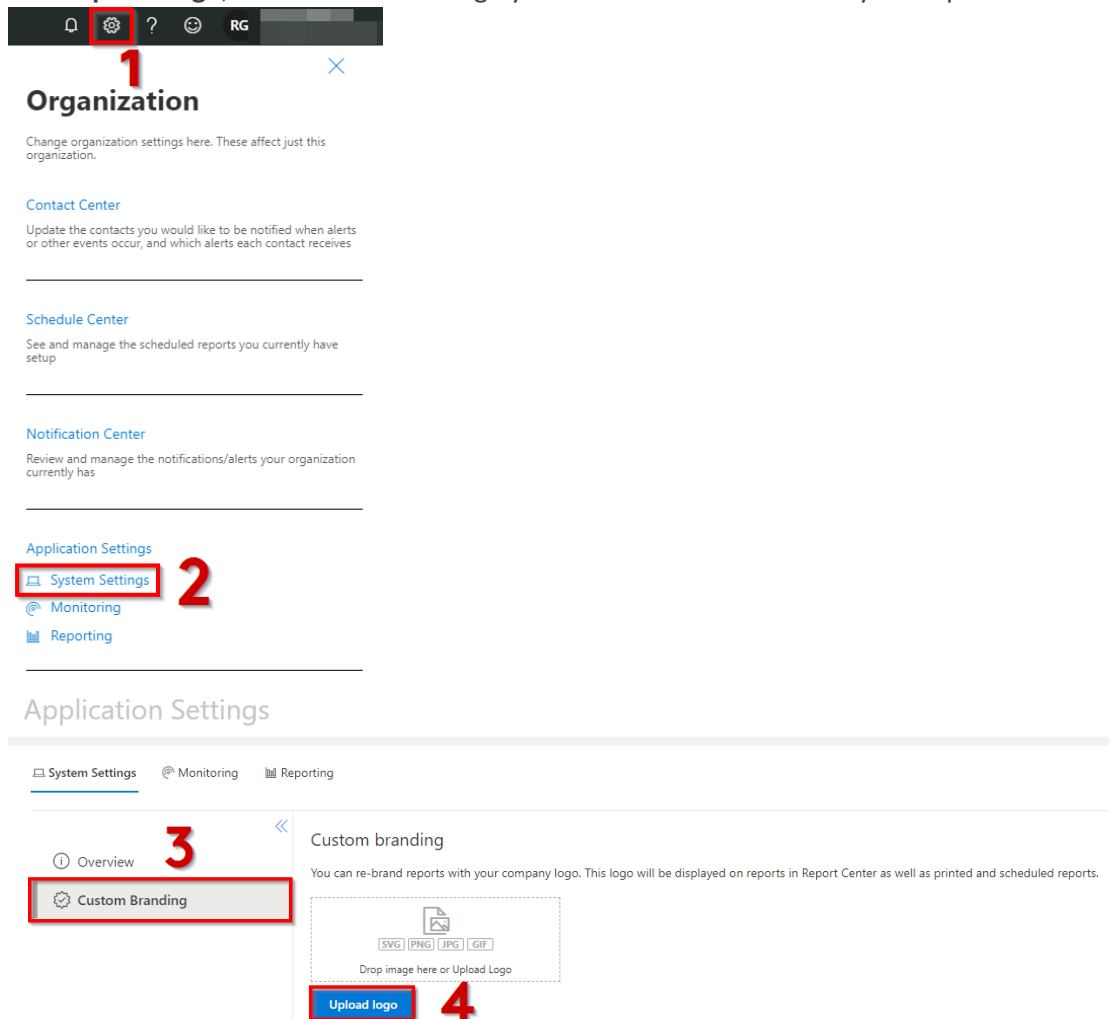
Below are some how to's on Reporting.

Add a logo to your report

You have the option to add a logo to your report. This allows you to add your own unique branding to each report, including system reports.

To do this:

1. Sign in to Nova as an administrator and click on the cog icon in the top right hand corner.
2. Click **System Settings** in the Organization sidebar.
3. In **Overview**, click **Custom Branding**.
4. Click **Upload logo**, then select the image you would like to include in your reports.



Your report should now be located in your reports in both the Nova Report Center and when downloaded as a PDF.

Combine multiple charts

Combining multiple charts allows you to see your data in one easy-to-read graph, giving you easy comparison between a variety of data sources.

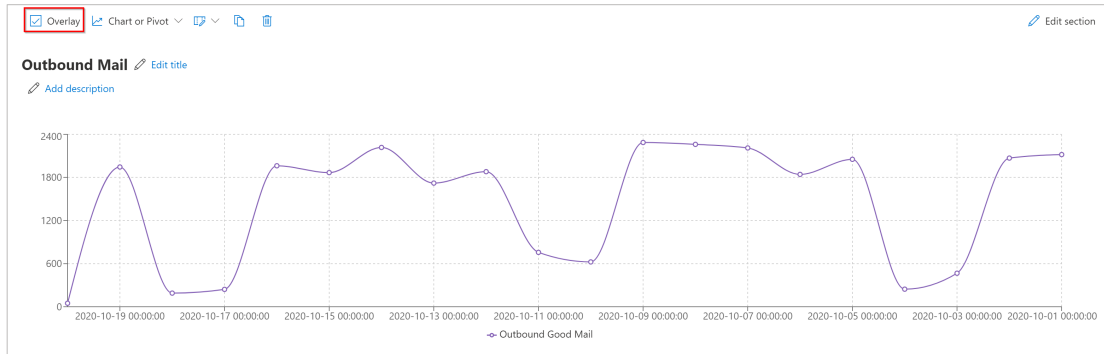
You are able to combine as many charts as you like, however there are a few caveats to keep in mind:

- The charts you would like to combine must be the same chart type e.g. bar, line, column. You are unable to combine pie charts.

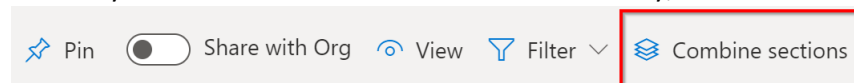
- The axis types must be the same. This is your *applied to* and *series name* categories when creating your chart.

To combine your charts:

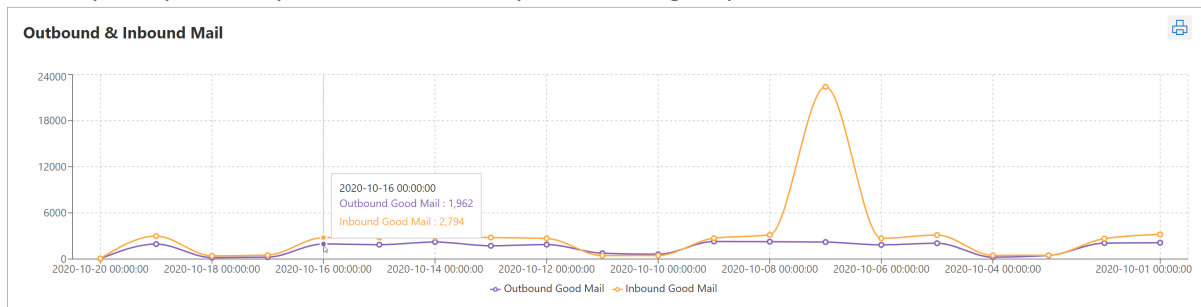
1. Create your chart. Remember that only bar, column and line graphs can be used for combining. To see how to create a chart, check out [this](#) section.
2. Click the **Overlay** checkbox to select the charts you would like to combine.



3. Once you have selected 2 or more charts to overlay, click **Combine sections**.



Your charts should now be combined into one. Your sets of data will be individually color coded for easy analysis, and you can hover over your data to get specific numbers.



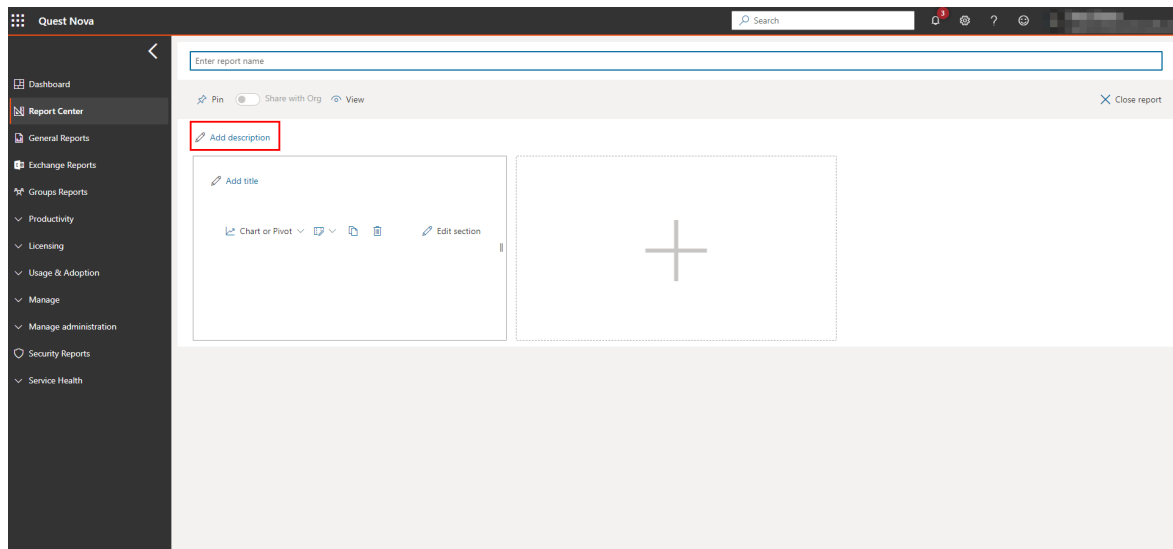
You can uncombine your charts at any time by clicking **Uncombine**. This is useful if you need to edit one chart within your combined report, as you can not do so when your charts are combined.

Describe reports and sections

Describing your reports is an excellent way to give other users context to what your report is all about. Before, it was only possible to describe your entire report, giving detail into what it was about, why it is important, how the data is relevant etc. Now, it is possible to describe both your entire report and each individual section. This is for users to better accurately describe what they are reporting on and bring further context to their data. Let us see how to do that below.

Adding a description to a report

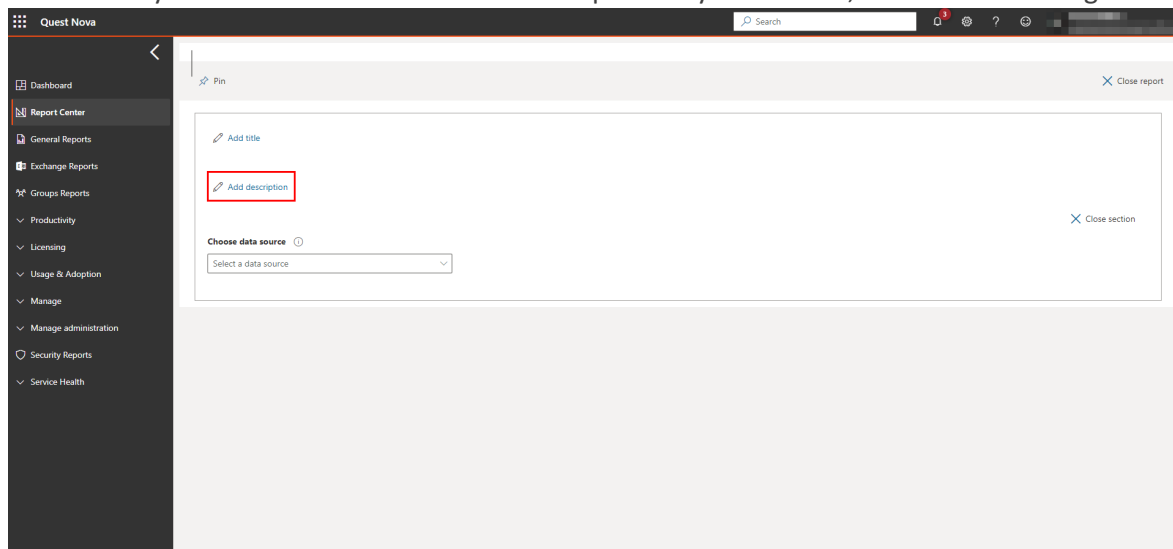
1. Open a report you have previously created, or start a new report by clicking 'Create Report' in the top right hand of the screen.
2. Then click 'add description' as highlighted below.



3. You can now add your description in the box.

Adding a description to a section

1. Open a report you have previously created, or start a new report by clicking 'Create Report' in the top right hand of the screen.
2. Then create a new section by clicking the plus icon.
3. Then click **Edit section**.
4. Now you can add both a title and a description to your section, as seen in the image below.



i | **NOTE:** If you are unsure about the title or description of your section, it is possible to create your section first then add a title and description after.

Design tools

There is a range of tools to help your description stand out, including:

- bullet points and numbered lists
- hyperlinks to other pages or reports

- highlighting

and so on. The toolbar can be found here.

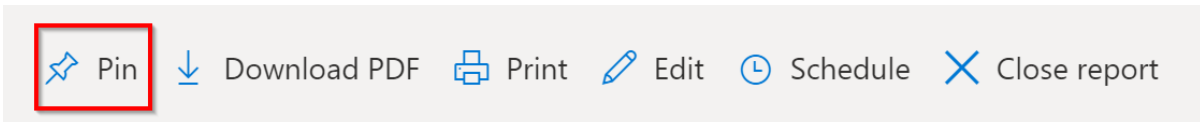


Pin reports to the navigation bar

You can pin up to 5 reports to the navigation bar, for quicker access to frequently used or viewed reports.

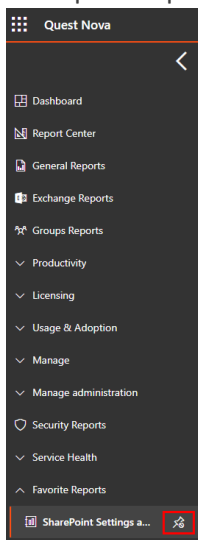
To pin reports, click on the report you want to pin.

In an unedited state, find and click on the **Pin** button.



The report then appears on the navigation bar on the left side of your screen.

To unpin a report, click the unpin button next to the report.



View extra columns in a table report section

When a table report section is added to Nova Report Center, sometimes there can be too many columns to see them all in the current browser window.

Over on the right hand side of the column headings, you can click to see those extra columns. Click the three dots (...) to bring up the list of additional columns. Values for that column will then be displayed in a pop-up window, and you can decide if you want to drag them into the list of columns which are visible.

Display Name ▾	Job Title ▾	User Type ▾	Type of Recipi... ▾	State/Province ▾	Last Exchange... ▾	Primary Email... ▾	Primary Dom... ▾	+	...
Pure IP TEST		Member	User						Postal Code Office
CallQueue Supp...		Member	User						
CallQueue Supp...		Member	User						
CallQueue Supp...		Member	User						
CallQueue Supp...		Member	User						
CallQueue Switc...		Member	User						

For more information on tabular data in Nova, click [here](#).

Tenant Management System

The Nova Tenant Management System (TMS) allows service providers to support multiple customers from a common interface. Using the Nova TMS, the service provider adds new customer tenants, and then delegates access to those tenants and the Nova platform.

[Click here](#) for a video overview of the TMS user interface.

This section explains how to manage customer tenants and add tenant administrators.

My Associations

Here, you can select your default tenant or remove your access to a tenant. This is where you can view all of the tenants that your QTID is associated with. To access this, click your tenant name at the top right hand side of the toolbar, then select **My Associations**.

My Invitations

Here, you can invite someone to associate with the organization and delegate management rights to them. Use this page to view the status of invitations you send. To access this, click your tenant name at the top right hand side of the toolbar, then select **My Invitations**.

Adding a Customer Tenant

Use the Nova Tenant Management System to add customer tenants. If you are managing a lot of tenants, or if some of your customers have multiple tenants, you might need to organize the tenants into organization groups. Here is how to add a new tenant to the TMS:

1. On the My Organization page, click Add Child.
2. Enter the organization name. We like to format this with the logical name, followed by the Microsoft 365 tenant name in parenthesis. It looks like this: Organization Name (tenant)
3. Select an organization type.
4. Select the 2 check boxes, if desired, which allows the parent organization to view the child organization's data and manage the child organization's settings.
5. Click Create.

[Click here](#) to watch a video showing how to add and manage customer tenants.

Adding a Tenant Administrator

You will want to invite someone from the organization to act as the tenant administrator. Follow the steps below to invite a tenant administrator.

1. On the My Organization page, expand the organization hierarchy until you can select the tenant to which you will add a tenant administrator.
2. Click Manage.
3. Enter their email address and select the role(s) you want to assign to them.

They'll receive an email invitation to access the application. When they follow the link in the email and accept the invitation, they'll authorize Nova to access their tenant's data and they'll allow the setup process to be completed.

i | **NOTE:** If the invited user does not receive an email, check the contents of any junk mail folder.

[Click here](#) to watch a video showing this process.

Additional Notes About Tenants

Here are some additional notes about the Tenant Management System:

- The individual who adds a tenant to TMS is automatically the tenant's default association and system administrator until a different default association and administrator is assigned.
- If you want to change your default tenant, go to My Associations and click the circle icon for the tenant you want to set as your default organization.
- If you want to remove your association/access to a tenant, go to My Associations, and click the **Remove association** button next to that tenant.
- If you are managing several tenants, you might want to organize them into groups using the Organization Groups page.

Configuring certificate-based authentication

Due to the deprecation of basic authentication, it may be necessary to use certificate-based authentication to access some Quest Nova services. Click [here](#) to learn more.

If your organization uses one or more of the following services:

- Exchange ActiveSync
- POP
- IMAP
- Remote PowerShell
- Exchange Web Services
- Offline Address Book
- Or Outlook for Windows and Mac,

You will need to assign the Microsoft Entra ID role to the Nova Read application. To use certificate-based authentication in Exchange Online, you will need to assign the Global Reader role to the Nova Read-Only Access application. For general instructions about assigning roles in Microsoft Entra ID, click [here](#).

There are two methods of assigning the Global Reader role:

Automatic

The tenant administrator can assign the Global Reader role within Nova by doing the following:

1. Go to TMS and select the desired organization.
2. Select the **Data Collection** tab.
3. Next to **Global Reader**, click **Setup automatically**.

The screenshot shows the 'Data Collection' tab selected in the top navigation bar. Below the navigation bar, there are three rows of configuration items:

- Global reader role:** Status is 'Not granted' (indicated by a red minus icon). To the right are two buttons: 'Verify' (with a refresh icon) and 'Setup automatically' (with a checkmark icon). A link 'Setup manually' is also present.
- Data Collection:** Status is 'Provisioned' (indicated by a green checkmark icon).
- Data Collection enablement:** Status is 'Enabled' (indicated by a blue toggle switch).

4. Login and grant consent.
5. The Global Reader role status should now have changed to **Granted**. If the status has not changed, click **Verify** to refresh the status.

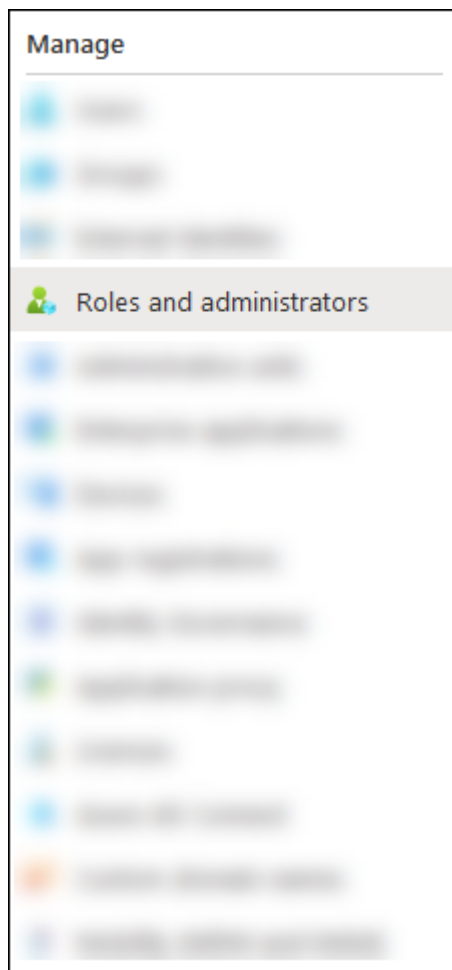
The screenshot shows the 'Data Collection' tab selected in the top navigation bar. Below the navigation bar, there are three rows of configuration items:

- Global reader role:** Status is 'Granted' (indicated by a green checkmark icon). To the right is a 'Verify' button (with a refresh icon).
- Data Collection:** Status is 'Provisioned' (indicated by a green checkmark icon).
- Data Collection enablement:** Status is 'Enabled' (indicated by a blue toggle switch).

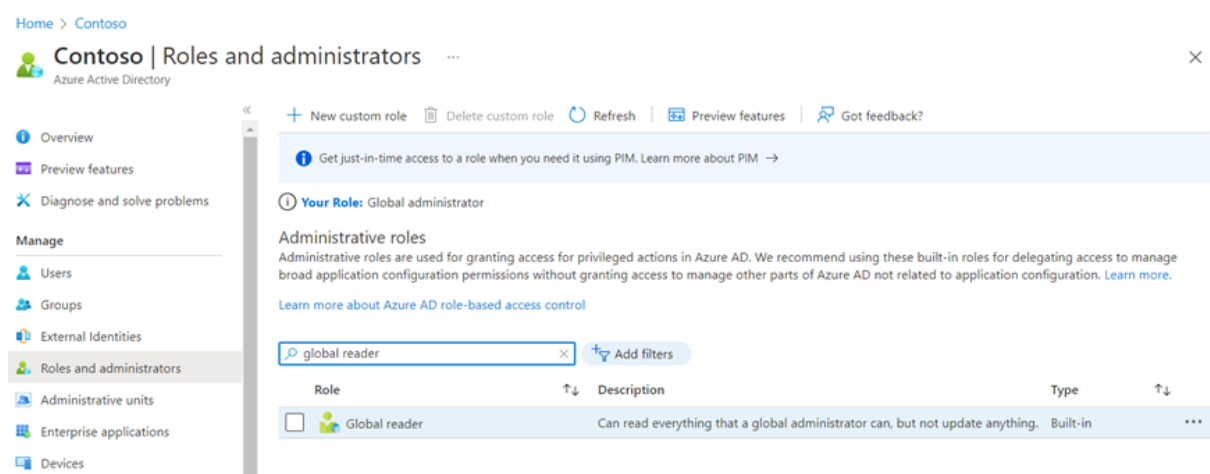
Manual

If you prefer to assign the Global Reader role manually, follow the steps below:

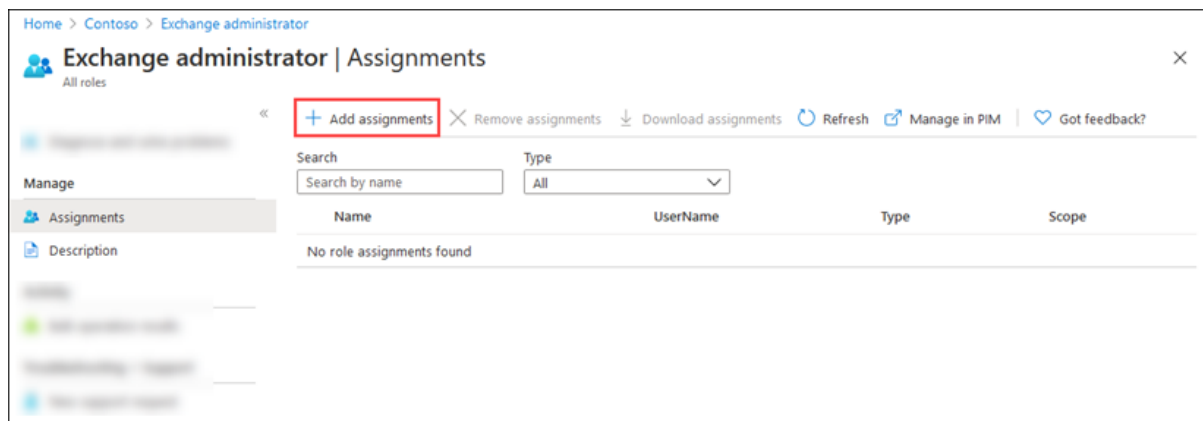
1. Open the Microsoft Entra [portal](#), and click Microsoft Entra ID.
2. On the **Overview** page, under Manage, select **Roles and administrators**.



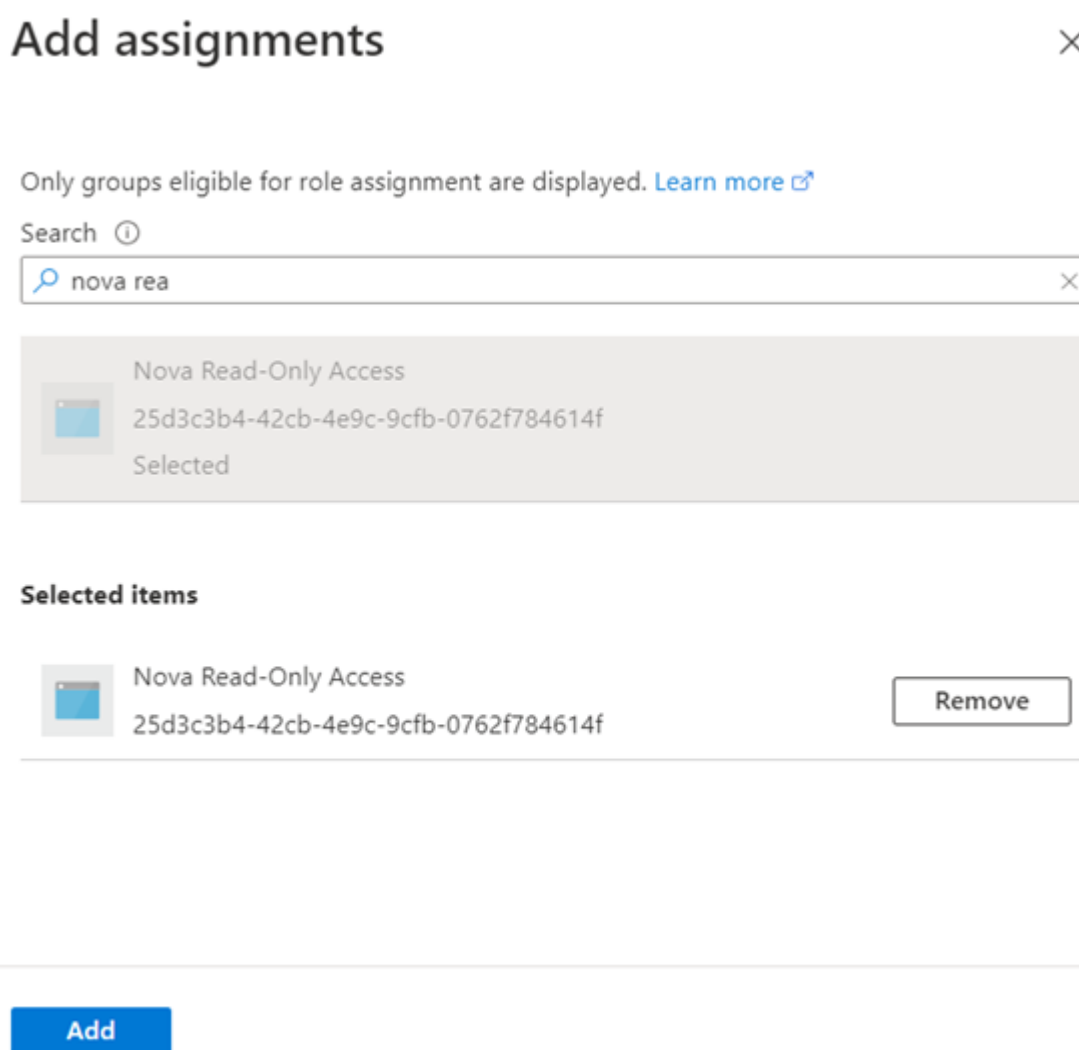
3. On the **Roles and administrators** page, find and select **Global reader** by clicking on the name of the role (not the check box) in the results.



4. On the **Assignments** page, click **Add assignments**.



5. In the **Add assignments** flyout, find and select the **Nova Read-Only Access** app. Note that if you are a SoftwareONE user, this app will be named **SoftwareONE Cloud Insider – Read Only**.



When you are finished, click **Add**.

6. Go back to the **Assignments** page and verify that the **Nova Read-Only Access** (or **SoftwareONE Cloud Insider – Read Only** for SoftwareONE users) app has been assigned to the role.

Home > Contoso > Global reader

Global reader | Assignments

All roles

« + Add assignments X Remove assignments Download assignments Refresh Manage in PIM Got feedback?

Diagnose and solve problems

Manage

- Assignments
- Description

Activity

- Bulk operation results
- Troubleshooting + Support
- New support request

You can also assign built-in roles to groups now. [Learn More](#)

Search Search by name Type All

Name	UserName	Type	Scope
<input type="checkbox"/> Nova Read-Only Access	25d3c3b4-42cb-4e9c-9cfb-0762f78461...	ServicePrincipal	Directory

SharePoint API permissions

You need to grant consent to new API permissions to avoid losing access to some SharePoint data. Consent of the API permissions will depend on the Azure application you are using. Click [here](#) to learn more on certificate based authentication.

All users using the Azure application 'Nova Read-Only Access' must grant consent to the following API permissions:

- Sites.FullControl.All
- User.ReadWrite.All

Users using the Azure application 'SoftwareONE Cloud Insider - Read Only' must grant consent to the above two API permissions, as well as the following permission:

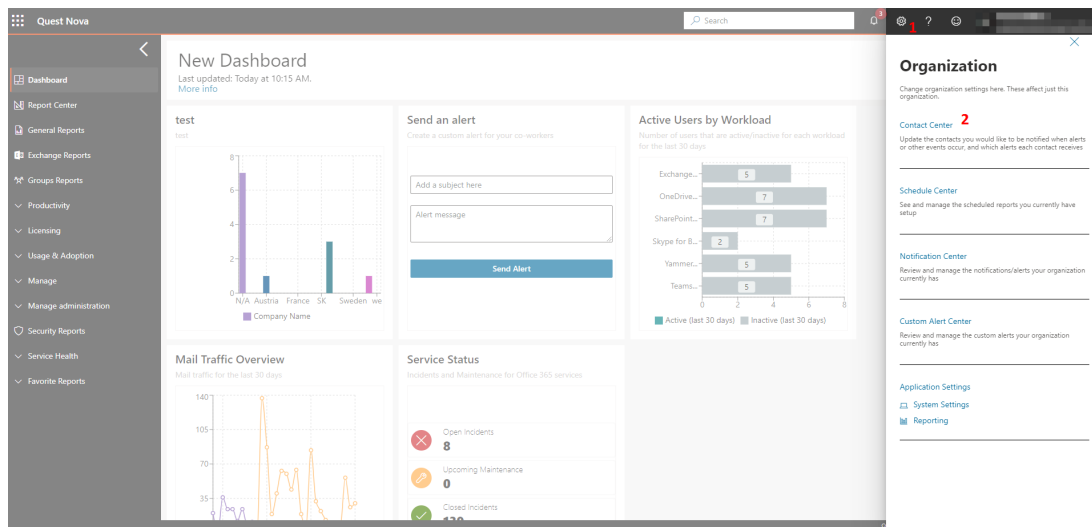
- User.Read.All

Nova administration

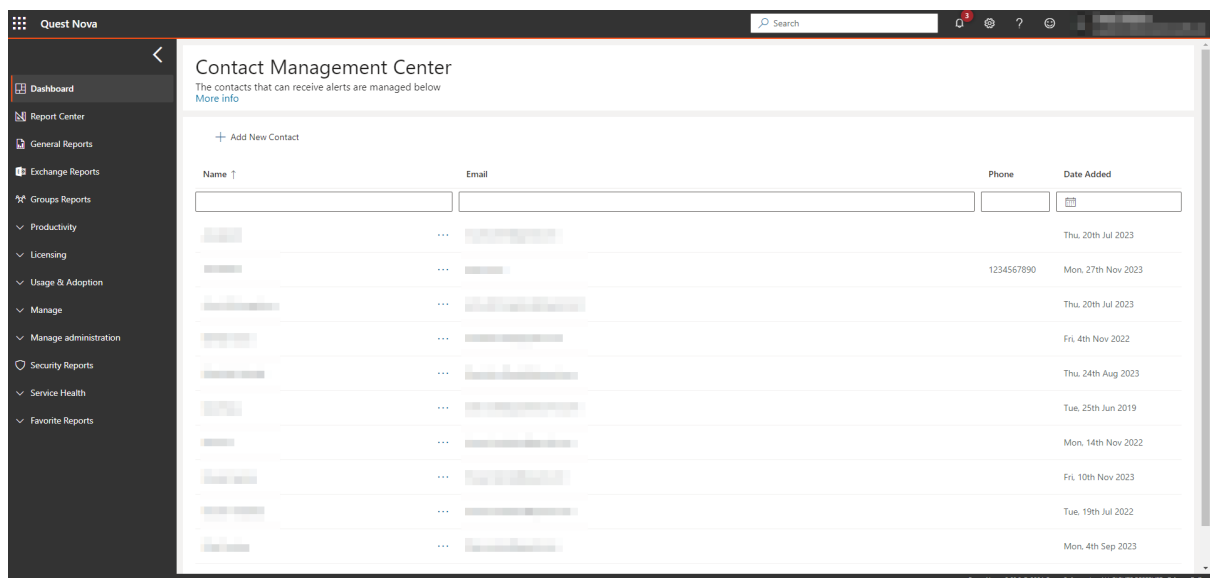
Contact Center

Use the Contact Center to manage the list of individuals who you want to be notified when alerts or other events occur.

To access the Contact Center, click the Settings button (a gear) located in the top right of the Nova window, and then select Contact Center, as shown below.



You can search for contacts and update their names. You can add new contacts manually, or they are added automatically when they are invited to log in to Nova for the first time.



This list of individuals in the Contact Center is also used when you are scheduling reports. So, if you are sending a scheduled report to someone who is not already listed in your contacts, open the Contact Center and add them manually before scheduling the report.

Add Contact ✕

① Either telephone number or email address must be supplied

Name *

Email

Phone

Cancel Save

From the Contact Center, you can specify which alerts you want each contact to receive by clicking **More** button, and then selecting the **Settings** tab. Here is how it looks:

Edit Contact: ██████████

Personal Details Settings

	NOVA	BILLING	GLOBAL
Get Alerts	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
● Critical	Select options ▼ Critical <input type="checkbox"/> Push Notifications <input type="checkbox"/> SMS <input type="checkbox"/> Email	Select options ▼	Select options ▼
● Degraded		Select options ▼	Select options ▼
● Healthy		Select options ▼	Select options ▼
● Info		Select options ▼	Select options ▼

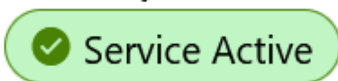
Cancel Save

Cross-tenant reporting

i | **NOTE:** These steps can only be completed by a System or Account Administrator.

Optionally, you may need to report across one or multiple tenants in order to get a wider scope of Microsoft 365 data in your organization. To do this:

1. Add your organization to Nova. This is done through your on-boarding process with Quest Support.
2. Setup reporting using the on-boarding wizard. To do this, click **Setup Reporting**, which will take you to the Reporting on-boarding wizard. For more on this, click [here](#) (recommended to open in a new tab). You will know if you have been provisioned if your reporting status has 'Service Active', as shown in the image below:

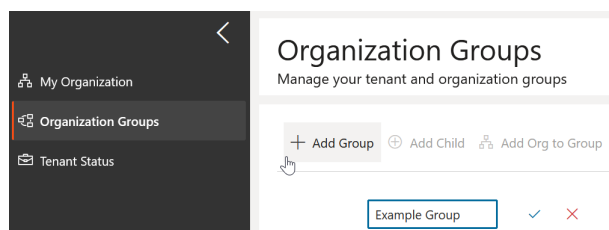


3. Add any child tenants you would like into the organization. For multi-tenant reporting to function, these need to be under the same parent tenant. Click [here](#) for steps on how to add child tenants.

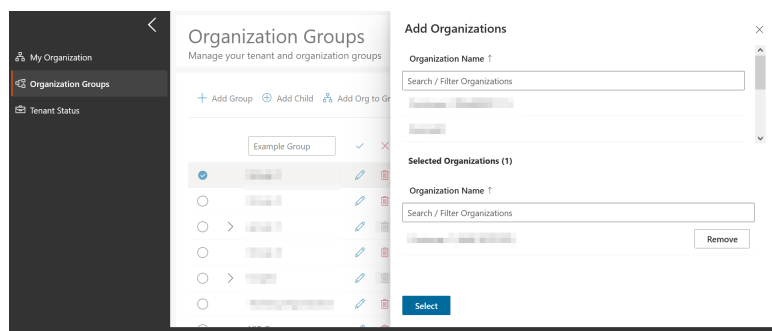
i | **NOTE:** These child tenants also need to have reporting provisioned. This can be done using the same instructions highlighted in step 2.

3. Once you have created your child tenants, and have had reporting provisioned, you can create your Organization Group. To do this:

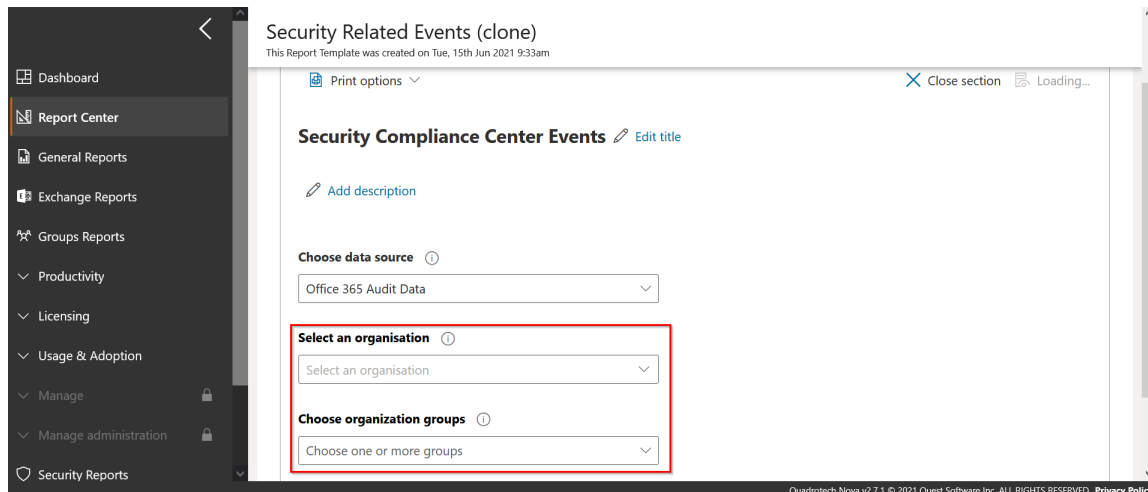
- a. On the left hand navigation pane, click **Organization Groups**.
- b. Click **Add Group**, and give it a distinctive name. Then click the tick icon.



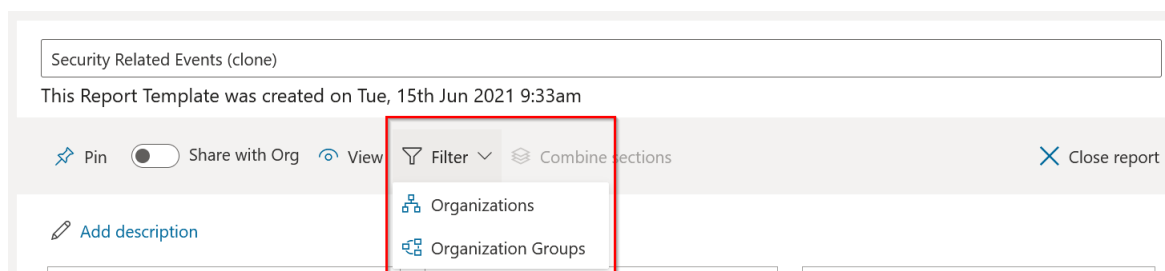
- c. Click on your Org Group, then click **Add Org to Group**, and add the tenants you would like to be in the group, and then **Select**.



- d. If applicable, you can add child groups, and add organizations to them using the same steps as above.
4. Once this is completed, you should now be able to filter reports by your chosen organization and organization groups. Filter by organization and/or organization groups using the boxes below when [creating or editing a section](#):



You can also filter an report, narrowing the scope of all sections within it. You can do this by clicking on any report, and selecting **Filter** from the drop down menu. If you are in Edit mode, you can select an organization and/or organization group to filter by, and save it to keep the filter assigned to that report. In View mode, you can temporarily add filters to your group.



Deprovision data collection

Users can stop the collection of data for a tenant by doing the following:

1. In TMS, click the 'Data Collection' tab.
2. Next to 'Data Collection Enabled', click 'Deprovision'.

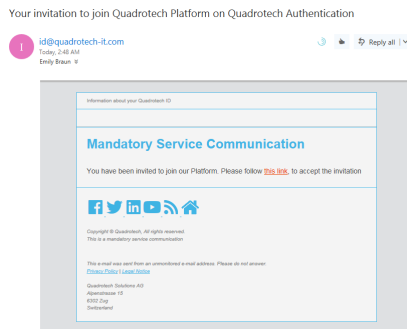


NOTE: This can only be completed by a user with either a 'System Administrator' or 'Quest TMS Admin' role.

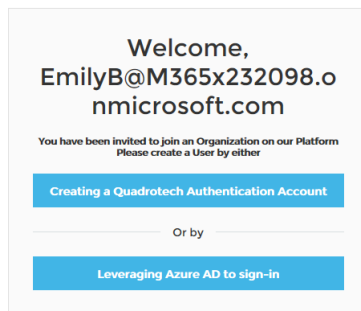
Invitation to access Nova

This section describes what a user sees when they are invited to access Nova.

First, the user receives an email invitation that looks similar to this:



When they click the link in the email, they are prompted to create a user account:



Here is more about the options to create a user account:

- **Creating a Quest Authentication Account:** Create credentials that are unique to their Nova/Quest account.
- **Leveraging Microsoft Entra ID to sign in:** Use Microsoft Entra ID credentials to access Nova.

Finally, the user might be asked to enter/confirm their name:

User Account Settings

User Info Security Configure Login Methods

Edit User

First Name:
Emily

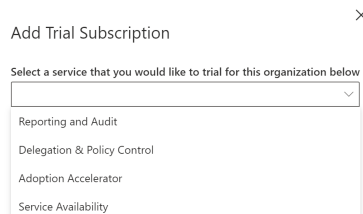
Last Name:
Brown

Email Address:
EmilyB@M365x232098.onmicrosoft.com

License types

There are several types of license that can be added to give access to features and services within the product. The Nova System Administrator for your tenant can see the licenses which are assigned, as well as the roles relating to individual users.

This is an example of a screenshot of what the Nova System Administrator might see:



Types of license

The available licenses are as follows:

Delegation and Policy Control

This gives access to the [Delegation & Policy Control](#) areas of Nova. It allows administrators to create and manage policies, as well as delegated administrators to perform actions according to those policies, such as changing an end-user password, adding an out-of-office message and so on

Reporting and Audit

This gives access to the reporting areas of Nova including pre-built reports and the Report Center.

On-premises agent

Requirements

The following are the requirements for the Nova on-premises agent:

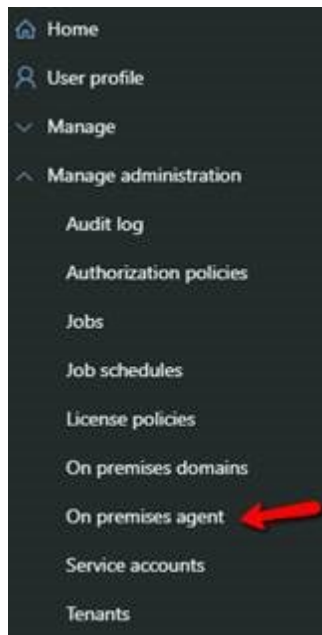
- The Microsoft Graph module for Windows PowerShell must be installed on the machine where you will install the on-premises agent. This can be done via PowerShell with *Install-WindowsFeature -Name RSAT-AD-PowerShell*
- It must have 443 access to the Nova URL for the tenant. (This is called the endpoint address)
- It must be installed on a domain joined server. The server will need to have outbound ports 443 and 44388 open to the Autopilot application IP.
- It must have a service account that has Domain Admin rights in Microsoft Entra ID for each domain in the forest that the agent will manage. This is used for proxied administration.
- Service Account must be member of following groups in domain:

CN=Administrators,CN=Builtin
CN=Domain Admins,CN=Users
CN=Enterprise Admins,CN=Users

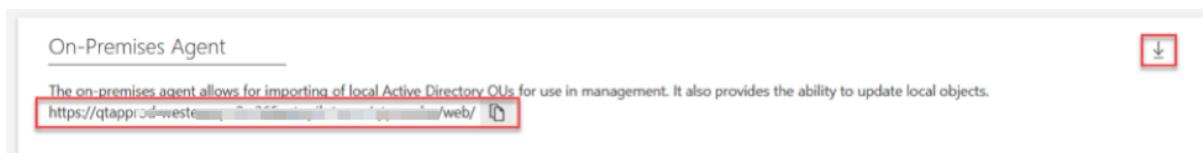
- The service account must have logon as service rights on the server.
- The agent must have a current .Net framework installed, as well as PowerShell 5.1 or above.

To obtain and install the agent:

1. Go to the **On premises agent** page.

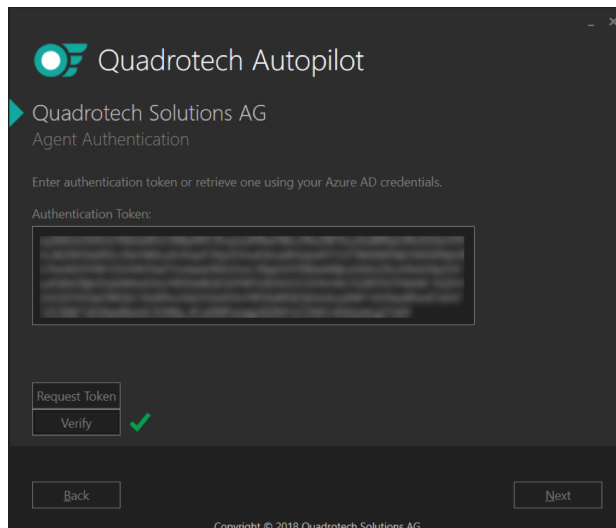


2. Ensure that the web services URL is copied and saved, it will be used during the installation:



3. Download the agent
4. Run the installation, and follow the prompts.

i **NOTE:** During the installation you will request a token on the following screen:

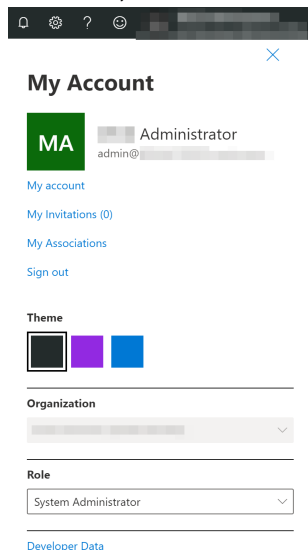


When prompted for an account to connect with, use the same Global Admin account which was used for the Service Account.

Persona menu

The Persona menu allows a user to see information about their Nova settings, their account, language and chosen color scheme. It also shows the current role and organization, and allows a user to switch to other roles and other organizations.

To access the Persona menu a user clicks on their name at the top right of the Nova user interface, and the menu will appear:



If a new role or organization is selected the user interface will switch, and jump to that chosen role and organization. For more on roles, click [here](#).

Nova remembers which tenant and role a user was last using, so the next time that user logs into Nova it takes the user back to the same place. This happens across browsers, and across sessions.

Sometimes when you log in to Nova, you may not see quite what you expect. For example, you may see users listed on the Users page that you do not immediately recognize.

If this happens, you will want to check your Persona Menu. It could be that the last time you logged in, you switched your role, or switched your organization, or switched your role *and* organization. Nova remembers those changes between sessions.

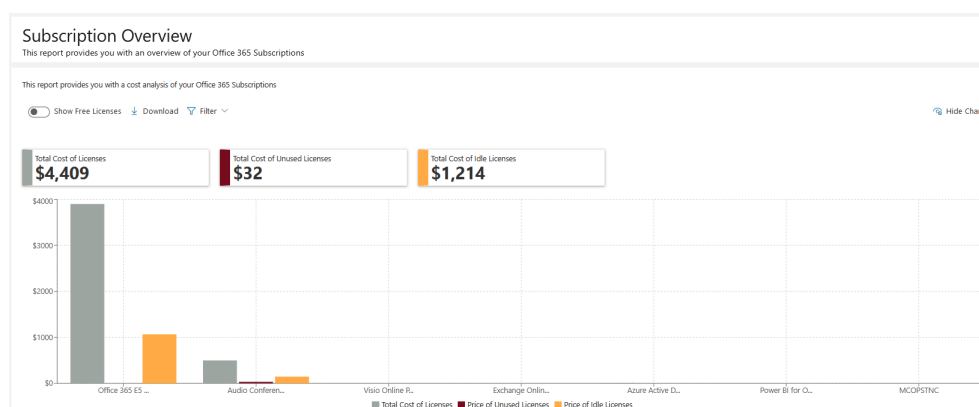
Subscription overview

The subscriptions overview page allows you to get an overview of licenses which are consumed in an organization, and gives you the ability to configure price information so you can determine the cost of licensing to your organization. This includes licenses which are assigned, unassigned and are idle.

For more clarification on what total, assigned and unassigned units are:

- **Total:** Currently enabled licenses + suspended licenses
- **Assigned licenses:** Licenses consumed by users
- **Unassigned licenses:** Total number of licenses - assigned licenses

The dashboard provides an overview of licenses that are being used in the tenant. This includes a total cost of all licenses being used, including total costs of unused and idle licenses. You can download this chart in a .csv format, or filter the chart by organization and/or organization group.



The table provides information on each license, including the percentage of licenses used, how many licenses there are and how many have been assigned, unassigned or are remaining idle.

The price associated with each license can be changed by clicking on it and entering the number.

Organization	License Sku Name	Percent Used	Total Licenses	Assigned Licens...	Unassigned Licenses	Idle Licenses	Price / Unit / Month ↓
<input type="text" value="Filter Organizations"/>	<input type="text" value="Filter License Sku Name"/>	<input type="text" value="Filter Percent Used"/>	<input type="text" value="Filter Total Li..."/>	<input type="text" value="Filter Assign..."/>	<input type="text" value="Filter Unassigned..."/>	<input type="text" value="Filter Idle Lic..."/>	<input type="text" value="Filter Price"/>
quadrotech.onmicrosoft.com	Office 365 E5 Without Audio Conferencing	<div><div>100%</div></div>	150	150	0	41	\$26
quadrotech.onmicrosoft.com	Azure Active Directory Premium P2	<div><div>100%</div></div>	1	1	0	0	\$9
quadrotech.onmicrosoft.com	Audio Conferencing	<div><div>93.6%</div></div>	125	117	8	37	\$4
quadrotech.onmicrosoft.com	Visio Online Plan 2	<div><div>0%</div></div>	11	0	11	11	\$0
quadrotech.onmicrosoft.com	Exchange Online (Plan 1)	<div><div>100%</div></div>	10	10	0	0	\$0
quadrotech.onmicrosoft.com	Power BI for Office 365 Standard	<div><div>1.5%</div></div>	200	3	197	198	\$0
quadrotech.onmicrosoft.com	MCOPSTNC	<div><div>0%</div></div>	10000000	31	9999969	9999980	\$0

User detail

Finding statistics on workload usage in easy to analyze graphs and charts is simple with Nova. In one screen, you can find data relating to a user's:

- Email usage
- Teams usage
- OneDrive for Business usage
- SharePoint usage
- Exchange Online usage
- Audit activity
- Mobile Device usage

and more.

To find this, search for the user in Nova's search bar, and click on the user you want to see statistics of.

User overview

The user overview section gives you general information on that user, including:

- Name
- Job Title
- Department
- Manager
- Office
- Location

The screen also contains information on licenses that have been assigned to that user, including if that license has been successfully applied to that user or if it is pending.

User created 6 months ago

Overview Mail Teams Skype OneDrive SharePoint Exchange Online Distribution Groups Mobile Devices Audit Activity Mailbox Size and Growth

User

Display Name	
User Login Name	
First Name	
Last Name	
Job Title	
Department	
Reports To (Display Name)	
Office	
Full address	
User Created	
Strong Password Required	✓
Password Never Expires	✓

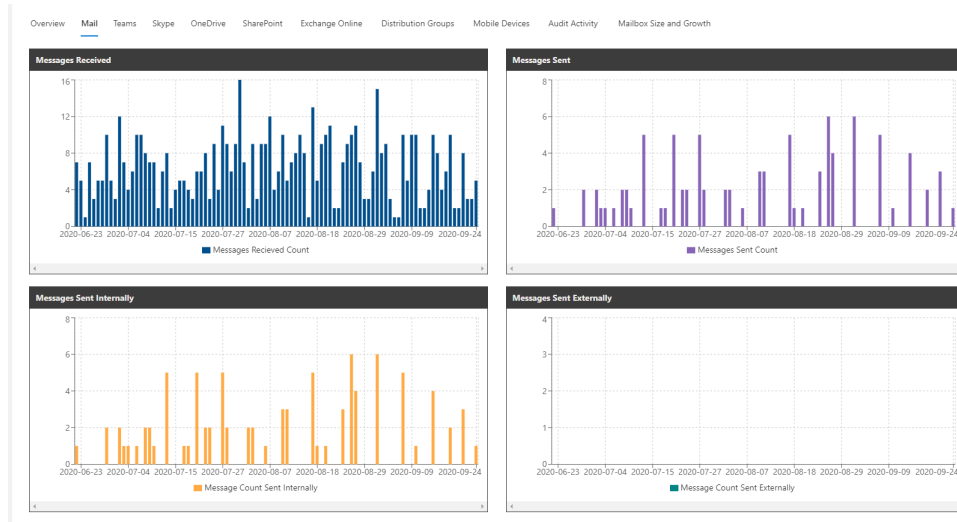
User Licenses

- > OFFICE 365 ENTERPRISE E5 WITHOUT PSTN CONFERENCING
- > ENTERPRISE MOBILITY + SECURITY E3

Mail

The mail tab gives you detail on the user's email activity over the past 3 months. This includes:

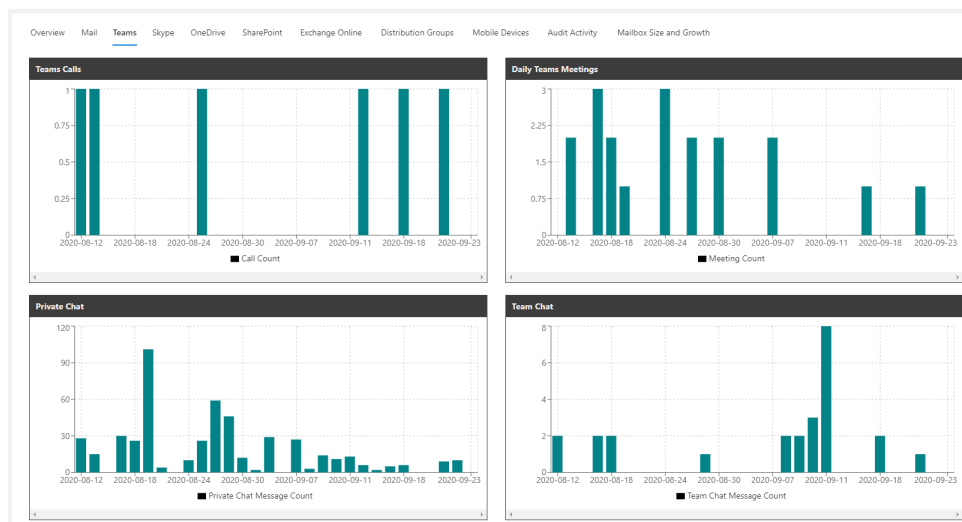
- Messages received
- Messages sent
- Messages sent internally
- Messages sent externally



Teams

The Teams tab gives you detail on the user's Teams activity over the past month. This includes:

- Teams Calls
- Daily Teams Meetings
- Private Chat
- Team Chat

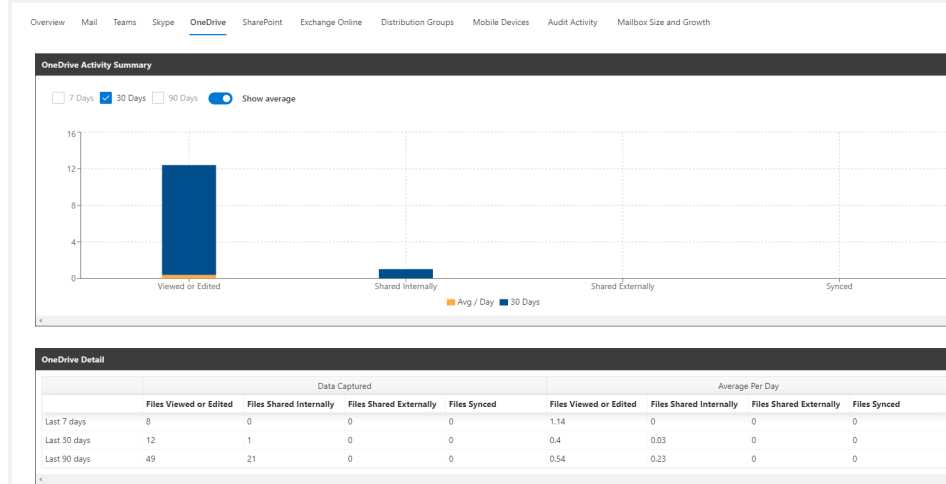


OneDrive

The OneDrive tab gives you comprehensive information on a user's OneDrive usage. See statistics within 7, 30 or 90 day parameters. Select 30 days, then show average to get a daily average total on activities such as:

- Files viewed or edited
- Files shared internally
- Files shared externally
- Files synced

Use the table to get exact data straight away, including average statistics on activity per day.

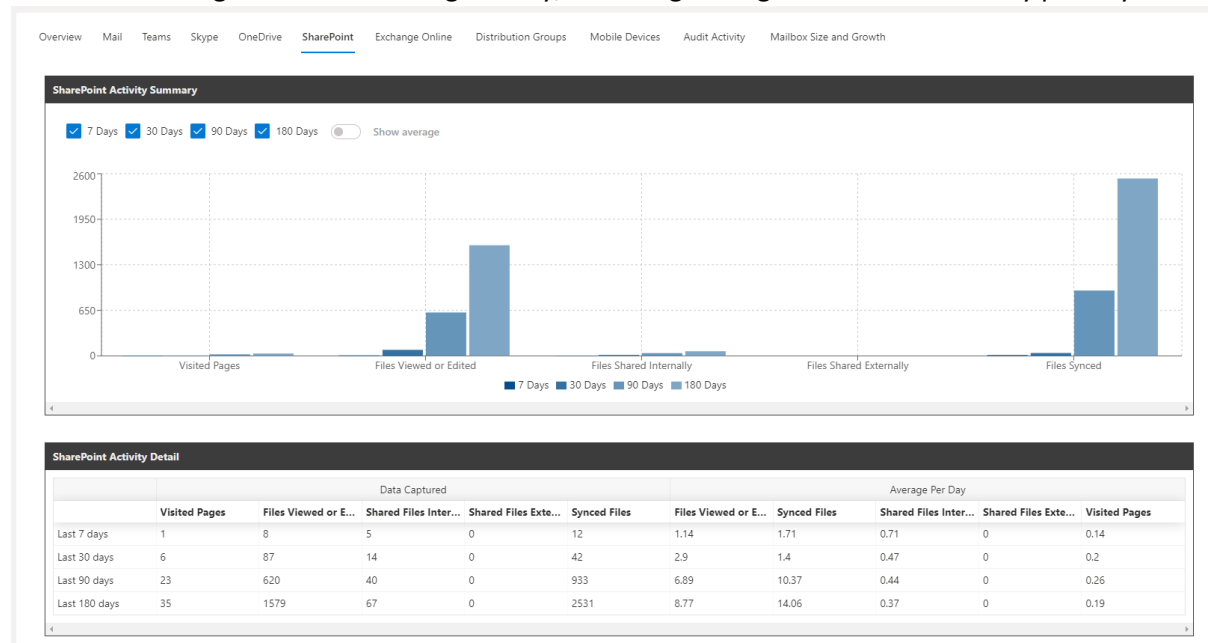


SharePoint

The SharePoint tab gives you comprehensive information on a user's SharePoint usage. See statistics within 7, 30, 90 or 180 day parameters. Select 30 days, then show average to get a daily average total on activities such as:

- Files visited
- Files viewed or edited
- Files shared internally
- Files shared externally
- Files synced

Use the table to get exact data straight away, including average statistics on activity per day.



Exchange Online

The Exchange Online tab gives you information on details such as:

- access to specific mailboxes
- last Exchange activity
- when the mailbox was created
- Exchange item count
- enablement of services such as
 - OWA (Outlook Web Access)
 - Active Sync
 - POP (Post Office Protocol)
 - IMAP
 - MAPI (Messaging Application Programme Interface)
 - EWS (Exchange Web Services)

Overview Mail Teams Skype OneDrive **Exchange Online** Distribution Groups Mobile Devices Audit Activity Mailbox Size and Growth

Mailbox Permissions

This user has access to the following mailboxes

Mailbox Owner	Access Type	Is Inherited	Is Deny
	FullAccess	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Exchange Details

Primary SMTP Address	
Last Exchange Activity	2020-09-23
Mailbox Created	2020-01-29 09:06:53
Forwarding Address	
Item Count	3125
Active Sync Enabled	<input checked="" type="checkbox"/>
OWA Enabled	<input checked="" type="checkbox"/>
POP Enabled	<input checked="" type="checkbox"/>
Imap Enabled	<input checked="" type="checkbox"/>
Mapi Enabled	<input checked="" type="checkbox"/>
Ews Enabled	<input checked="" type="checkbox"/>
OWA Mailbox Policy	OwaMailboxPolicy-Default
Active Sync Mailbox Policy	Default

Mobile Devices

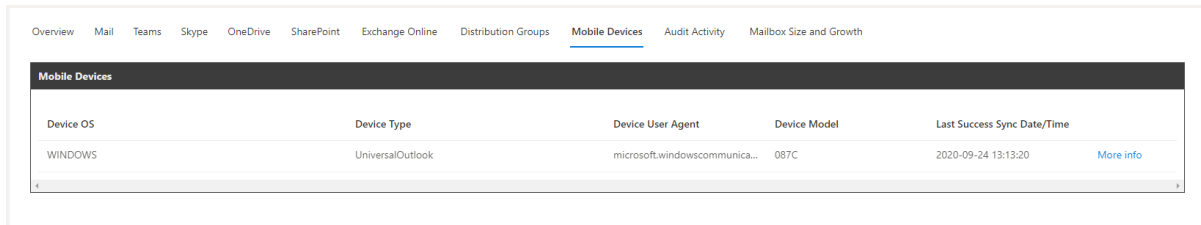
The Mobile Device tab gives you information on mobile devices affiliated with a user. Overview details include:

- Device OS
- Device Type
- User Agent
- Device Model
- Last date/sync time

Clicking **More Info** gives you much more information about a device, including:

- Device ID
- Device Manufacturer
- Device OS Version
- First date/time sync

and more.



Mobile Devices				
Device OS	Device Type	Device User Agent	Device Model	Last Success Sync Date/Time
WINDOWS	UniversalOutlook	microsoft.windowscommunica...	087C	2020-09-24 13:13:20 More info

Audit Activity

The Audit Activity Tab gives you a detailed look at your users activity across all workloads, including:

- Operation
- Creation Time
- Record Type
- Target Object
- If the action was successful

Audit Activity						
Workload	Operation	Creation Time	Record Type	Target Object	Result	Client IP
Exchange	MoveToDeletedItems	2020-09-25 09:41:46	Exchange Multiple Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:41:40	50		Succeeded	
Exchange	MailItemsAccessed	2020-09-25 09:41:14	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:41:14	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...
Exchange	MoveToDeletedItems	2020-09-25 09:41:03	Exchange Multiple Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...
SharePoint	ListViewed	2020-09-25 09:40:30	SP List Event	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	FilePreviewed	2020-09-25 09:40:28	SP File Or Folder Operation	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	FilePreviewed	2020-09-25 09:40:28	SP File Or Folder Operation	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	AddedToGroup	2020-09-25 09:40:27	SP Sharing Event	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	SharingSet	2020-09-25 09:40:27	SP Sharing Event	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	AddedToGroup	2020-09-25 09:40:27	SP Sharing Event	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	FileAccessed	2020-09-25 09:40:27	SP File Or Folder Operation	https://quadrotech.sharep...	Not logged	86.182.37.168
SharePoint	CompanyLinkUsed	2020-09-25 09:40:27	SP Sharing Event	https://quadrotech.sharep...	Not logged	86.182.37.168
Exchange	FolderBind	2020-09-25 09:37:50	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:37:47	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c:5960ae001:35c2:8410:8bf...

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:

Refresh

Hide system events

Export

Columns

Action	Changes	Affected obj...	Tenant	Submitter	Submitter IP	Event type	Submitted
<div></div> <div>Get tenant ...</div>		<div></div>	<div></div> <div>quadrotec...</div>	<div>system.Sch...</div>	<div></div>	<div></div> <div>Job Compl...</div>	<div>23/06/202...</div>
Get Chang...	Groups Del...		quadrotec...	System:Sch...		Job Compl...	23/06/202...
Get Intune ...			quadrotec...	System:Sch...		Job Compl...	23/06/202...
Get Chang...	Users Delta...		quadrotec...	System:Sch...		Job Compl...	23/06/202...

25 Rows

Page 1 of 2044

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.

Action	Changes	Affected object	Tenant	Submitter	Submitter IP	E...	Submitted
		Apply filters here					
Get user dire...		Bill Jennings	quadrotech-...	System	System	J...	23/06/2021, ...
Get Cloud U...		Bill Jennings	quadrotech-...	System	System	J...	23/06/2021, ...
Get Change...	Mailboxes W...		quadrotech-...	System:Sche...		J...	23/06/2021, ...
Get Change...	Distribution		quadrotech...	System:Sche...		J...	23/06/2021

25 Rows Page 1 of 2044

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
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.

Virtual Business Boundaries

Virtual Business Boundaries (VBBs) gives system administrators more control over the data that the users within their tenant can see, modify and create reports from. VBBs are not static or confined; they support environments with many different logical overlaps and complexities, such as covering several geographic locations and/or departments. VBBs are designed to fit the intricate needs of the administrator, no matter the size of the environment, over the data in which is most relevant to them and their users.

This includes three concepts, which can be used individually or in combination:

1. **Data Anonymization** - Administrators have the ability to filter certain data and data sources from its' users within the boundary, including data that the administrator can anonymize. For example, you can anonymize names, departments and emails from the user.
 - a. **Use case:** You want to set up Nova for a particular customer, and you want help desk staff to see data from a particular data source, but you do not want personal identifiable information (PII) to be revealed, such as names and email addresses. Putting these help desk staff into a VBB and anonymizing this data allows this to happen. You can then create another VBB for global administrators with no anonymization, so that these administrators can see the PII.
2. **Data Source Restriction** - Prevent users from viewing data from certain data sources and specific fields within those sources when viewing and creating reports.
 - a. **Use case:** You may have a large complex environment that has many different teams, for example a Teams administration team, a Microsoft Entra ID team and an email administration team, and you only want users to find these particular scopes of data. Here, you can assign a VBB to these individual users in these teams, and add the relevant data sources to these VBBs. Now the users in these VBBs can only see these particular data sources.
3. **Data Scope Restriction** - Filter the returned data, allowing users in a boundary to see a subset of the data based on a use case. For example, you can filter by country so those users can only see data about users based in a specific country, or filter by department so users in the boundary only see information about users who are in a certain department.
 - a. **Use case:** You have an environment which spans many different countries and departments, but you wish to return reports that only specifies data from the United States for a team in that location. Adding users from the United States, and applying a United States data scope filter to a VBB allows those users to only see data from that location.



NOTES:

- For Virtual Business Boundaries to take effect in reports, an Microsoft Entra ID field must be included in the report. This field does NOT have to be the same field that is assigned to the boundary.
- Virtual Business Boundaries can only be created and accessed by a [System Administrator](#).

- You can only input individual users when creating boundaries. Adding groups of users is not currently supported.

VBBs give system administrators the ability to isolate data for their users. For example:

- Giving Level One support in Germany the ability to only see German users.
- Allowing a Business Unit manager to only see data for its users from within their Business Unit.
- Allowing business users to only see data for specific workloads (SharePoint Online, Teams, Exchange etc).
- Personal Identifiable Information can only be visible for those within certain geographies and/or departments, whilst being restricted to those outside of them.

To access Virtual Business Boundaries:

1. Log in to Nova with a user that has the System Administrator role.
2. Open the menu in the top left corner of the navigation menu, and select **TMS Client**.
3. Click **Virtual Boundaries** from the left navigation menu.

Creating a boundary

Follow the steps below to create your own boundary:

1. Select the organization you would like to apply the boundary to.
2. Click **Add Boundary**.
3. Create a boundary name, and add a description if required.
4. Check the **Anonymize sensitive information for selected users** box if you would like to have sensitive information, such as names and email addresses, hidden for your selected users. See **Data Anonymization** on [this](#) page to find out more about this.
5. Enter the name of the user to add to the boundary, and click on the name from the drop down list.
6. Once all of your chosen users have been added, select **Add Users**.
7. Revise your selected users. You can remove a user by hovering over the chosen user, checking the circular box, and clicking **Remove Users**. Once you are done reviewing your users, click **Next**.
8. Select the data source(s) you would like users in the boundary to see by checking the box. See **Data Source Restriction** on [this](#) page to find out more about this.
9. All data fields are checked by default. Uncheck the data fields you would not like to your users to see, and click **Next**.

10. Scope Restrictions is where you can narrow the data of the boundary. See **Data Scope Restriction** on [this](#) page to find out more about this. For example, if you would like to narrow the scope of the boundary to apply only to users in the Sales department in the United States:
 - a. Click **Add Filter Group**.
 - b. Click **Select field...**, then choose **Country or region**.
 - c. For **Select operator**, click **is equal to**.
 - d. In the **Enter filter value** box, enter **United States**.
 - e. Click the plus icon, and ensure the operator states **And**.
 - f. Click **Select field...**, then choose **Department**.
 - g. For **Select operator**, choose **is equal to**.
 - h. In the **Enter filter value** box, enter **Sales**.
 - i. Click **Next**.
11. Review the settings you have created. Once you are satisfied, click **Create Boundary**. This will then appear in the list of created boundaries.

i | **NOTE:** Virtual Business Boundaries will not take effect immediately, and may take up to 30 minutes to operate as normal upon creation.

Permissions for each user

By clicking on **Check Permissions**, and entering the name of a user, you can check the list of permissions assigned to that user, the boundary they have been assigned to, and if data is anonymized for that user. You can download the list of permissions for that user into a .csv file by clicking **Download CSV**.

Downloading boundaries to .csv

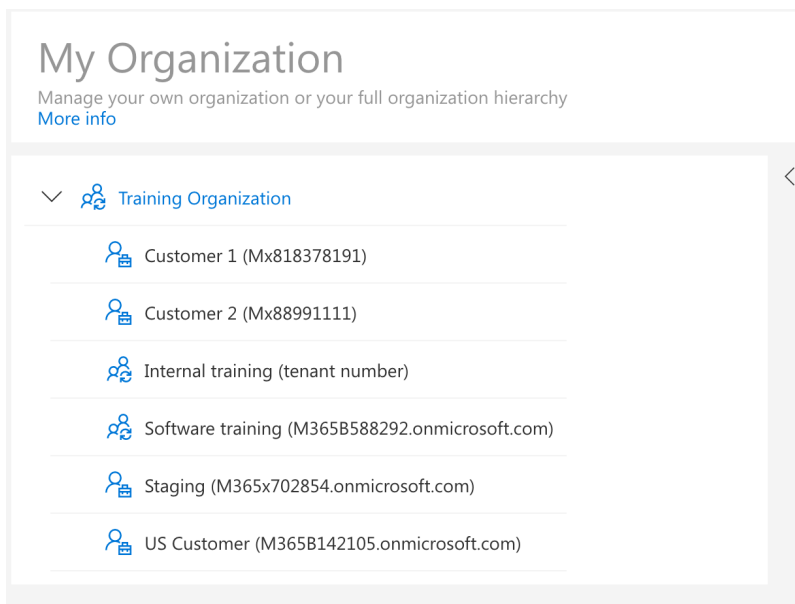
You can download a list of created boundaries, including their created and modified dates, to a .csv file by clicking **Download CSV**.

How to add new users

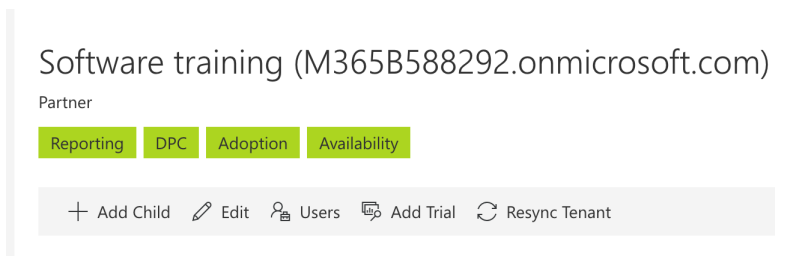
New users can be added to tenants that you have access so that they can have access to Nova features and services. This is performed in TMS (the Tenant Management System).

These are the steps that you should take:

1. Login to [TMS](#) using an account with the System Administrator role.
2. Locate the tenant/container where you want to add a new user and click on it.



3. Then click on 'Users'.



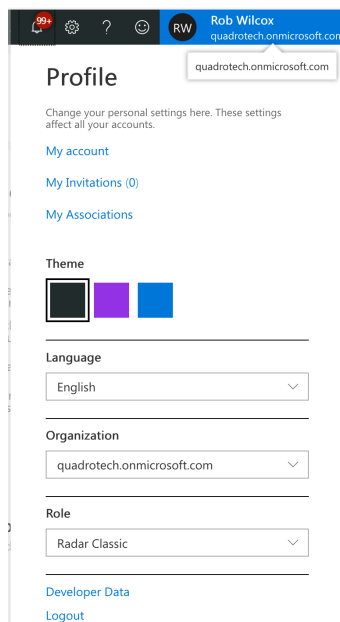
4. You will be shown a list of users who are already associated/invited/active in your chosen tenant. On the 'invitations' tab, you can invite a new user. Enter their email address, choose appropriate roles, and click on 'Invite'.
5. Upon addition of the user, the user then needs to accept the invitation using one of the links below (dependent on which platform the user is operating with):

For the Quest platform: <https://account.nova.quest.com/invites>

You can see invited users on the invitations tab.

Once the user has accepted the invitation, the user will appear on the list of users. They are then associated (or linked) to that container/tenant and have a particular role with associated capabilities within that tenant.

If a user has access to multiple container/tenants then they should use the Persona menu to switch to different tenants:

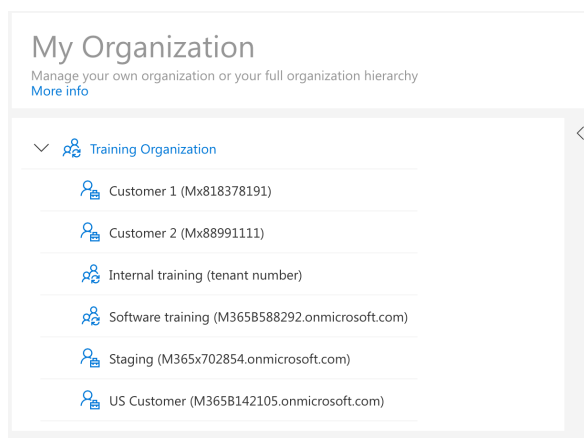


To learn more about the Persona menu, see this [section](#).

Nova remembers which tenant and role a user was last using, so the next time that user logs into Nova it takes the user back to the same place. This happens across browsers, and across sessions.

What is an association?

In the above description we have mentioned 'association' several times, this is essentially a link between your user account, and a tenant, via a particular role. In some organizations there is a one-to-one link, in other organizations a single user might have access to multiple Office 365 tenants. It is also possible for the same user to have different access levels in different organizations. In other words they would have different roles. Let us say we have multiple tenants in an organization, as shown below:



An account, can have different roles in different tenants in this structure.

Software training (M365B588292.onmicrosoft.com) User Associations

[Associations \(25\)](#) [Invitations \(1\)](#)

Name	Email	Date Associated	Roles
Thor		15th June 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C
		9th July 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C
Greg	greg	24th July 2019	System Administrator, Account Administrator, Autopilot Classic
Tomas	tomas	24th September 2019	System Administrator, Radar Classic
Jan	jan	10th July 2019	Auth Policy Admin, Organizational Unit Admin, License Admin, System #
Martin	martin	18th July 2019	System Administrator, Account Administrator, Autopilot Classic
Rob Wilcox	rob.wilcox@quadrotech-it.com	28th May 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C

Staging (M365x702854.onmicrosoft.com) User Associations

[Associations \(4\)](#) [Invitations \(0\)](#)

Name	Email	Date Associated	Roles
Greg	greg	31st July 2019	System Administrator, Account Administrator, Autopilot Classic
Martin	martin	6th August 2019	System Administrator, Account Administrator, Autopilot Classic
Rob Wilcox	rob.wilcox@quadrotech-it.com	31st July 2019	System Administrator
		31st July 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C

And in fact might not have access to certain tenants in the structure.

Removing a user

To see how to from your tenant, see this [section](#).

Adding additional service accounts

Microsoft 365 implements a series of throttling policies on Microsoft 365 tenants that can inhibit the collection of reporting data for Nova customers.

In order to improve the reliability and speed of the data collection process, we recommend that Microsoft 365 tenants with more than 10,000 users take advantage of our Multiple Service account feature.

By adding multiple Nova service accounts, you will help ensure that reporting data is updated in a timely manner without impacting your Microsoft 365 tenant. These service accounts do not require a Microsoft 365 which means that taking advantage of this feature does not add any cost to your Microsoft 365 subscription.

Getting started

Before we begin, you must create some additional accounts within your Microsoft 365 environment with the correct permissions.

For simplicity, we recommend that these service accounts are named as follows:

NovaDPC@<domain>.onmicrosoft.com

NovaDPC1@<domain>.onmicrosoft.com

NovaDPC2@<domain>.onmicrosoft.com

etc

To create the service accounts for DPC, please follow the steps outlined at [this section](#).

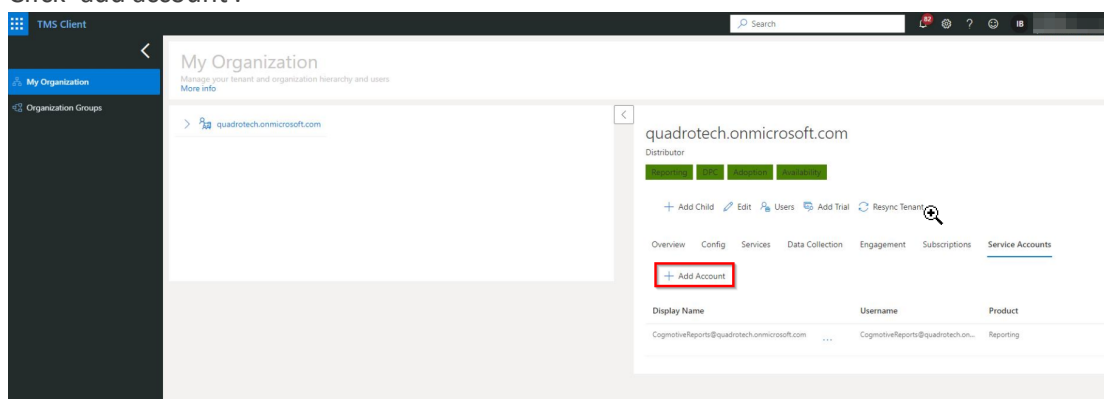
NOTE: If you are using the SharePoint Online Reports module, you will also need to give this account the correct permissions to the SharePoint Online Site Collections you are reporting on – you can find the steps to do so at this section.

Alternatively, you can create a Security Group in Microsoft 365 with these correct permissions and add the Nova Service accounts into this security group.

Adding these accounts to Nova

To add an additional service account,

1. Log in to your tenant as an administrator at <https://account.quadro.tech>
2. Go to the My Organization tab
3. Select your tenant
4. Click 'add account'.



An expansive section on service accounts can be found [here](#).

Remove a user from your tenant

From time to time it might be necessary to remove a user from your tenant. We also call this removing the user association. It is easy to do by following these steps:

1. Login to [TMS](#) using an account with the System Administrator role.
2. Locate the tenant/container which you want to manage and select it.
3. Then click **Users**.

You will be shown a list of users who are already associated / invited / active in your chosen tenant.

Software training (M365B588292.onmicrosoft.com) User Associations

Associations (25)				Invitations (1)	
Name	Email	Date Associated	Roles		
Thomas	thomas@quadrotech.onmicrosoft.com	15th June 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C		
Paul	paul@quadrotech.onmicrosoft.com	9th July 2019	System Administrator, Radar Classic, Account Administrator, Autopilot C		
Greg	greg@quadrotech.onmicrosoft.com	24th July 2019	System Administrator, Account Administrator, Autopilot Classic		
Thomas	thomas@quadrotech.onmicrosoft.com	24th September 2019	System Administrator, Radar Classic		

Click on the icon to the right of the user and their roles, and it will remove their association with this tenant.



NOTE: There is no confirmation dialog and the user will be removed immediately.

Creating a group and Team prefix

Administrators can define a prefix that is applied to the name of newly created groups and teams. The prefix can be set separately for each organizational unit in the enterprise.

Creating a new group prefix

Follow these steps to enable this functionality for newly created groups and groups associated with teams:

1. Go to **Manage Administration > Tenants**.
2. Find the desired root tenant or meta Organizational Unit (OU).
3. Click the ellipsis (...) and select Edit.
4. Enter a prefix that will be applied to all newly created groups.

Creating a new Team prefix

Follow these steps to enable this functionality for new teams.

1. Go to **Manage > Teams**.
2. Find the desired Teams OU.
3. Click the ellipsis (...) and select Edit.
4. Enter a prefix that will be applied to all groups associated with newly created teams.

Identify when jobs are not running

As a Nova administrator, it is important to quickly identify when jobs within your tenant are not running and troubleshoot these issues.

Jobs are color-coded accordingly:

- Jobs that have not been running for 0-3 days are not color-coded.
- Jobs that have not been running for 3-6 days are YELLOW.
- Jobs that have not been running for 6+ days are RED.

Here is how it looks:

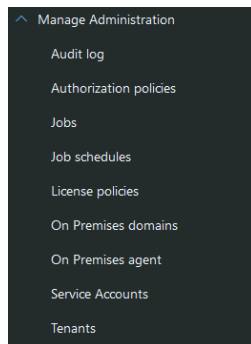
Tenant Domain	Mailbox Count	User Count	Data As Of	Next Scan
M365x304230.onmicrosoft.com	27	0	24-Jul-2020 00:00:00	3-Sep-2020 09:47:08
M365x973834.onmicrosoft.com	27	0	9-Jul-2020 00:00:00	2-Sep-2020 11:51:12
M365x984996.onmicrosoft.com	27	33	17-Jul-2020 00:00:00	27-Jul-2020 10:00:00
M365x404194.onmicrosoft.com	27	33	2-Aug-2020 00:00:00	5-Aug-2020 13:06:00
M365x950714.onmicrosoft.com	27	0	30-Aug-2020 00:00:00	2-Sep-2020 11:51:41
M365x417809.onmicrosoft.com	27	33	1-Aug-2020 00:00:00	5-Aug-2020 10:14:53
M365x343423.onmicrosoft.com	27	0	18-Aug-2020 00:00:00	2-Sep-2020 19:05:12

What are the roles within Nova?

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.

Radar Classic

This gives access to reporting data, and the Report Center.

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).

Why do some Nova roles have 'Classic' suffixes?

Two parts of Nova have existed in different systems and different formats before Nova. Nova has users which are now using Nova that used to use those systems, so these roles are named as shown on this page so that those customers understand what functionality, broadly speaking, they'll be getting with those roles. These two are:

- **Radar Classic:** This gives users the same functionality as they would have had in our Radar product.
- **Autopilot Classic:** This gives users the same functionality as they would have had in our Autopilot product.

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.

Settings

Service accounts for Nova

Overview

Nova is a modular solution. There are two types of service accounts that have different requirements for the process to run smoothly, and it is recommended that each module has a separate service account.

Details

To easily spot that an account is used by Nova, the service account should be named the same way.

We recommend that you should use the name of product followed by module **NovaDPC**.

NovaDPC

This is for a service account for the **Management (DPC – Delegation & Policy Control)** module to manage tenant data.

Details with requirements for this service account are detailed in [this section](#).

Note

The service account names featured here are just recommendations. If a customer has a different naming policy, they should follow that policy instead.

Examples

NovaReporting@myTenant.myTopDomain

NovaDPC@myTenant.myTopDomain

Application settings menu

As a System Administrator, by clicking on the gears (settings) icon, and clicking **Application Settings**, this will give you a variety of system and reporting settings to configure different modules for Nova.

System Settings

Custom Branding

You can re-brand reports with your company logo if you desire. This logo will be displayed on reports in the Report Center, as well as printed and scheduled reports. To find out more, click [here](#).

Reporting

General Settings

In General Settings, you can change the default currency for reports where currency is applicable.

Security Settings

Here, you have two options:

- **Anonymize Data** - Applicable to [Virtual Business Boundaries](#), this setting allows you to anonymize personal details for each user.
- **Collect Phone Numbers** - this setting gives Nova permission to store phone numbers to be available for reports.

SharePoint Settings

This allows you to add and remove site collections for SharePoint. To see more on this, click [here](#).

Data Update

Data update allows you to update specific attributes on user accounts using defined rules. For more on this, see below.

Rule sets

Rule sets help segment your user/group data by five different properties; business units, billing codes, and three custom fields defined by the user. Each rule set can contain multiple rules to set the values for the segmented data.

Rule sets have the ability to run on a schedule that tailors to your needs. This ensures your users and groups are updated regularly with the appropriate metadata, keeping your segments up to date. You can also enable or disable a rule set, as well as an individual rule within a rule set.

Below is an example of how to segment your users by business unit based upon their primary domain:

1. Go to **Application Settings > Reporting > Data Update**
2. Click **Add Rule Set**
3. Enter the Rule Set name and description, and choose whether to instantly enable or disable the rule set. Then click **Next**.

4. Click **Add Rule**, and enter the name of the rule.
5. Select **User Objects**, then **Add Filter Group**.
6. Click **Select Field**, then in the **Field Name Filter/Search** box, enter **Primary Domain**, and select the field.
7. Enter the domain which you would like to apply the rule to.
8. On the drop down menu, select **is equal to** for the operator. Optionally, add extra filters to narrow the scope of your rule, for example departments and/or regions. Then click **Next**.
9. Click **Add Field**, then from the drop down menu, select **Business Unit**, and create the name of the business unit to apply the rule to, for example **BU1**.
10. If you have added additional filters, such as a region or department, we would recommend you add those following the value. For example, if you have applied a Sales filter, using the same example above, enter **BU1_Sales**. Then click **Next**.
11. Review the summary and ensure the details are correct. If you would like to run the rule now, click **Run Now**. Then click **Save**. This is now added to the rules section in the rule set. Click **Next**.
12. Enter when you would like the rule set to run. You can run it immediately, or schedule it for a specific time.
13. Choose whether to run the rule set only once, or in recurrence. Then click **Next**.
14. Revise the summary for your rule set, then click **Finish**.

Copyright

Copyright

© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

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

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.

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

Quest® Nova
Updated October 2024

About

We are more than just a name. We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical Support Resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>. The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos

- Engage in community discussion
- Chat with support engineers online
- View services to assist you with your product

