Quest

Quadrotech Nova by Quest User Guide 2.0.0

User Guide

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

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

Patents

Trademarks

Legend

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

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

Quadrotech Nova by Quest User Guide
Updated February 2021

Version 2.0.0

Contents

2

User Interface

Overview of My Associations

This page lists all tenants/organizations you're associated with. Use the options to select your default organization or remove your access to an organization.
Click here to learn more about the Tenant Management System.

Overview of Users Page

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

- Changing a display name
- Updating location information
- Resetting a password
- Managing multi-factor authentication
- Inviting a guest to the tenant

Overview of Contacts Page

This page shows you a list of contacts for a certain Office 365 tenant. You can add, remove, and edit listed contacts.

Overview of Mailboxes Page

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

- Create new mailboxes
- Update information on existing mailboxes, such as adding an additional SMTP address, enabling a mailbox archive, and changing the mailbox type
- Delete mailboxes

Overview of Groups Page

On the Groups page, you can manage Office 365 groups. You can:

- Create new groups
- Remove groups
- Edit the details related to a group such as changing the owner, adding members to a group, and more.

Overview of Teams Page

On the Teams page, you can manage Office 365 Teams. You can:

- Add new teams
- Remove old, inactive teams
- Edit the details of existing teams. For example, creating new channels, updating the list of owners or members of a team, and more.

Overview of Contact Center

The Contact Center page shows a list of contacts associated with your current tenant. On this page you can:

- Search for a contact.
- View additional information about a contact.
- Edit and delete contacts.
- Add new contacts.

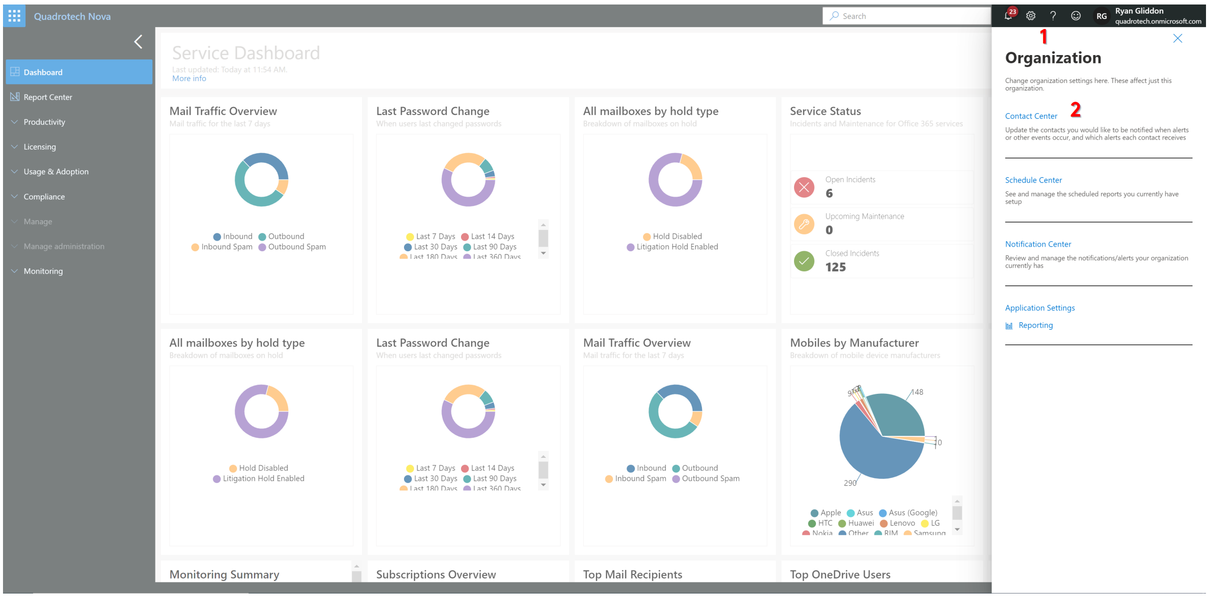
These contacts are used when scheduling reports.

Click here to learn more.

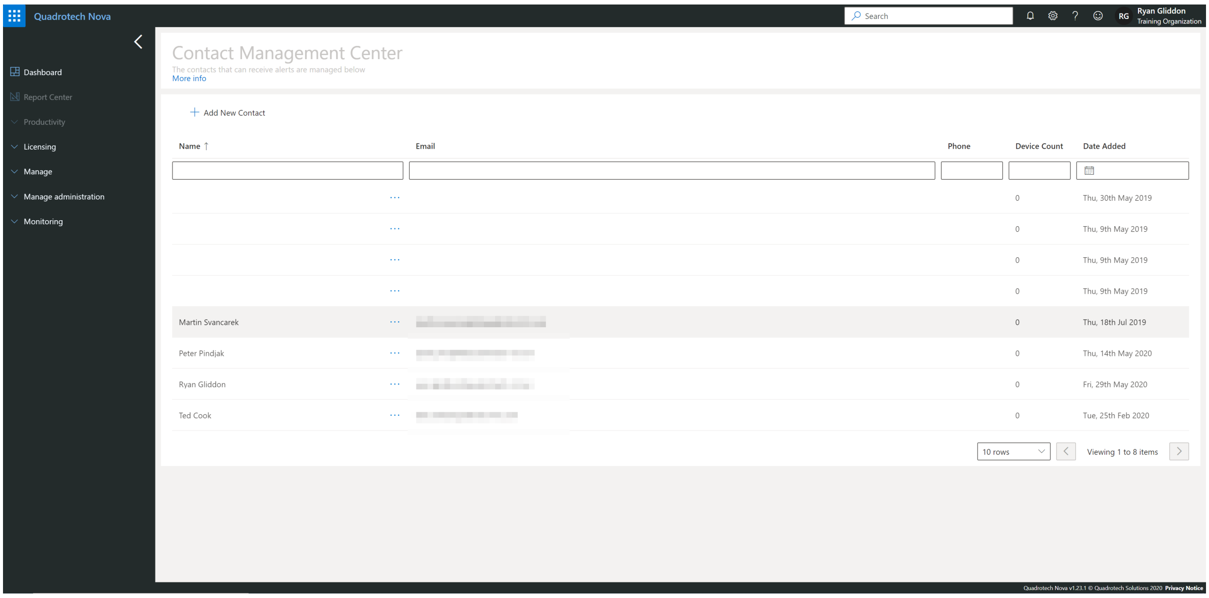
Contact Center

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

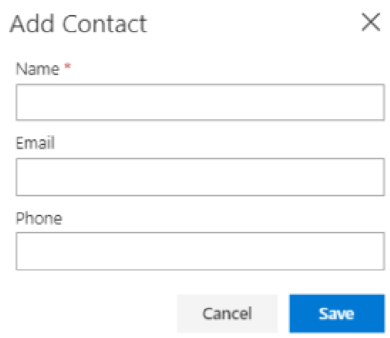
To access the Contact Center, click the Settings button (a gear) located in the top right of the Nova window, and then select Contact Center, as shown below.



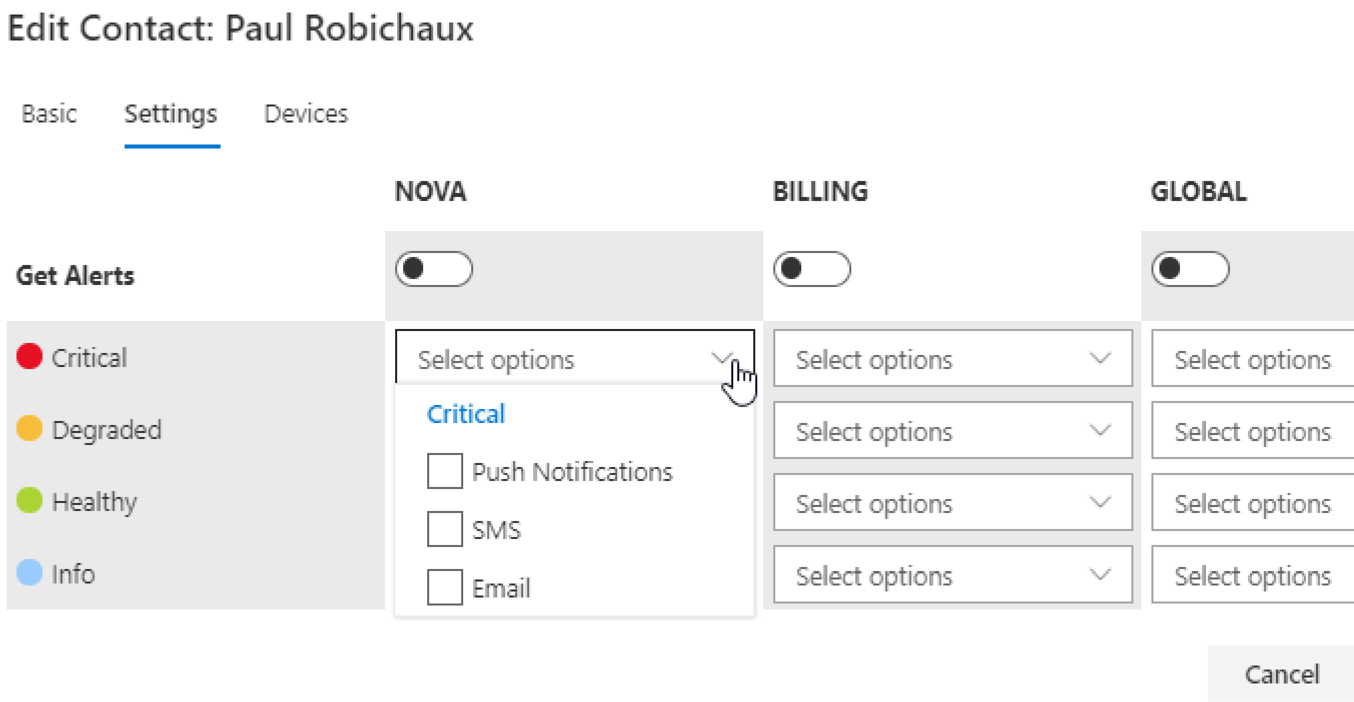
You can search for contacts and update their names. You can add new contacts manually, or they're added automatically when they're invited to log in to Nova for the first time.



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



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's how it looks:



Overview of My Organization

This page shows your tenant hierarchy. Use this page to add, remove, and edit tenants.

Select the tenant you want to perform an action against. Then, click either:

- **Add Child** to add a sub-tenant.
- **Edit** to update the tenant's name and settings.
- **Manage** to invite an administrator to associate with the tenant, select administrator roles, or remove an administrator's access.
- **Add Tria**: to give an organization temporary access to Nova.
- **Resync Tenant** to update the tenant details.

Click here for more information on adding customer tenants and tenant administrators.

Overview of Tenants Page

On the Tenants page, you can review the tenants that you have access to and create and manage virtual organizational units.

An important feature of Nova is the ability to set up and use virtual organizational units. If you're familiar with on-premises Active Directory, then you'll already be familiar with organizational units. The problem is that Azure Active Directory and Office 365 don't have this concept. The users are stored in a flat list, which can make working with multiple geographies and multiple departments much more difficult. So, in Nova we've re-introduced organizational units. We call them virtual organizational units. You can create a hierarchy of these just like you would in an on premises Active Directory environment.

To set up a virtual organizational unit.

Note: Any organizational units set up in Nova are not pulled into Active Directory.

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'll 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.

NOTE: If you wish to make use of the 'User Assignment Rule' feature, review this article

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's ellipses button (…) and select **Users & Groups** to see a list of users and groups that were added to the group within Nova. Note: You can see other objects as well, such as mailboxes and contacts.

To add a user or group to a virtual organizational unit:

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

To delete a virtual organizational unit containing users,and move them to another vOU

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'll move any users from the deleted vOU, and then click **OK** to apply the changes.

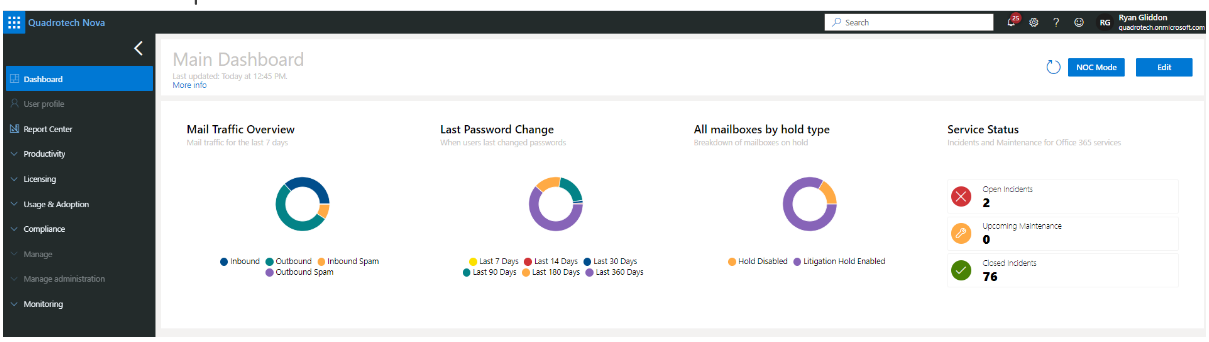
Here's a video showing the steps above:
https://youtu.be/jOsz2mE16G0

Overview of Dashboard

Nova can show a dashboard containing useful metrics related to your organization. Dashboards can be customized, they auto-refresh, and you can turn them into a visual display for a help desk, call center, or network operations center.

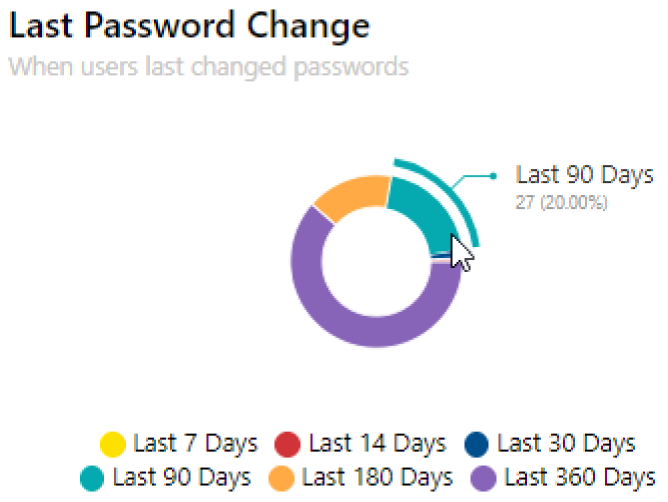
Example Dashboard

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



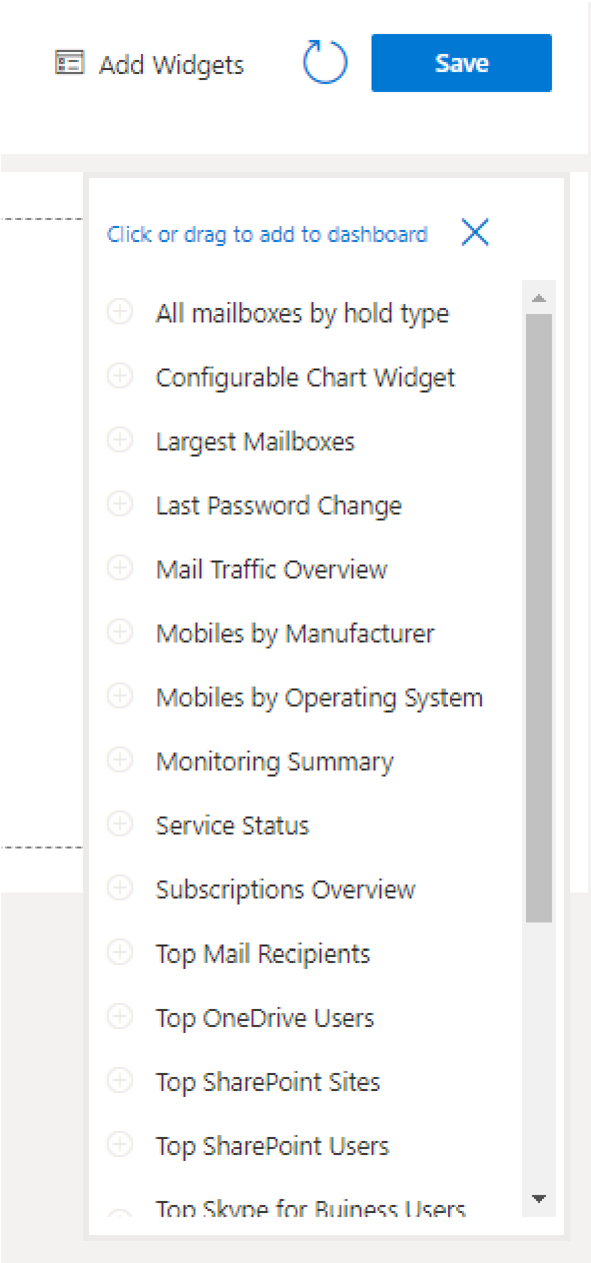
Interacting With the Data

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'll see the precise amount of users who changed their password.. Some other charts have a **More** button, which takes you to additional detail.



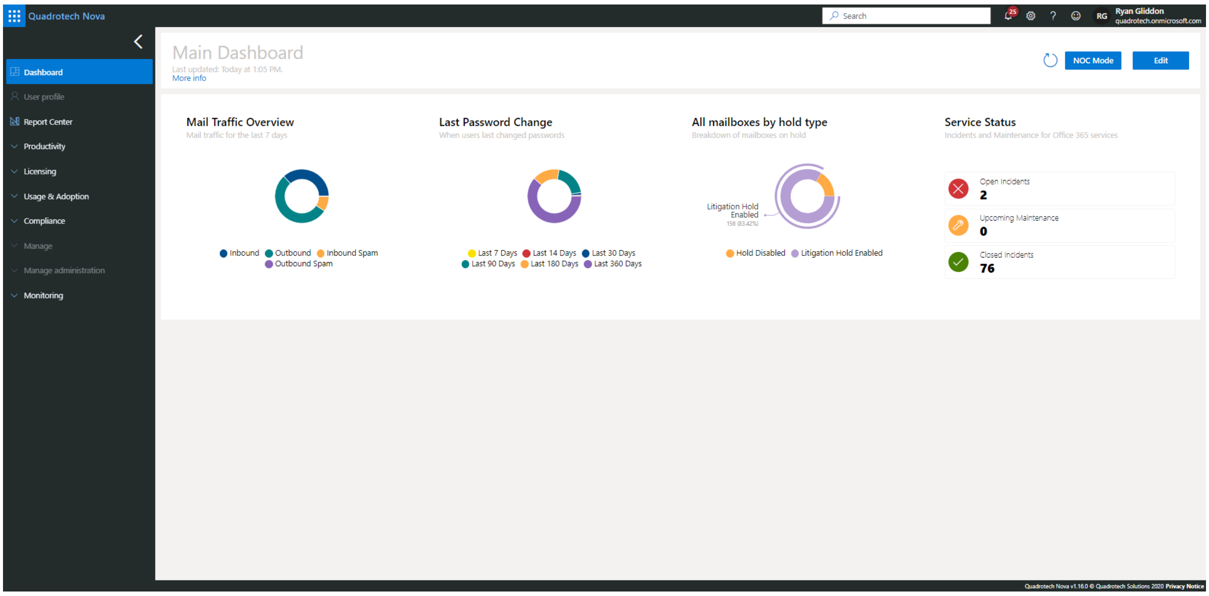
Editing a Dashboard

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 aren't needed, and add new widgets by dragging and dropping them from the list onto the page.
To do this, click on **Edit** on the Nova Dashboard, and choose the widget(s) you would like to insert into your dashboard.

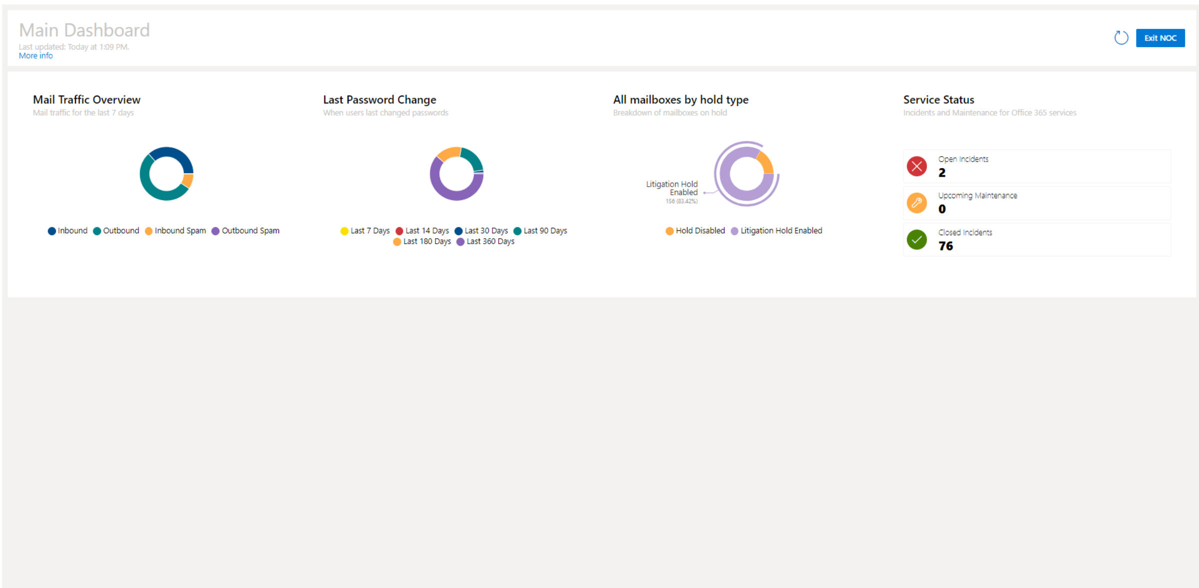

Add Widgets
Save
Click or drag to add to dashboard
All mailboxes by hold type
Configurable Chart Widget
Largest Mailboxes
Last Password Change
Mail Traffic Overview
Mobiles by Manufacturer
Mobiles by Operating System
Monitoring Summary
Service Status
Subscriptions Overview
Top Mail Recipients
Top OneDrive Users
Top SharePoint Sites
Top SharePoint Users

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's a perfect overview for call center, network operations, or help desk employees.

Move and Resize Widgets

You can move and resize widgets across your dashboard.

To move a widget, click and hold the widget you would like to move, and drag to the location you would like it to be.

To resize a widget, 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.

Video

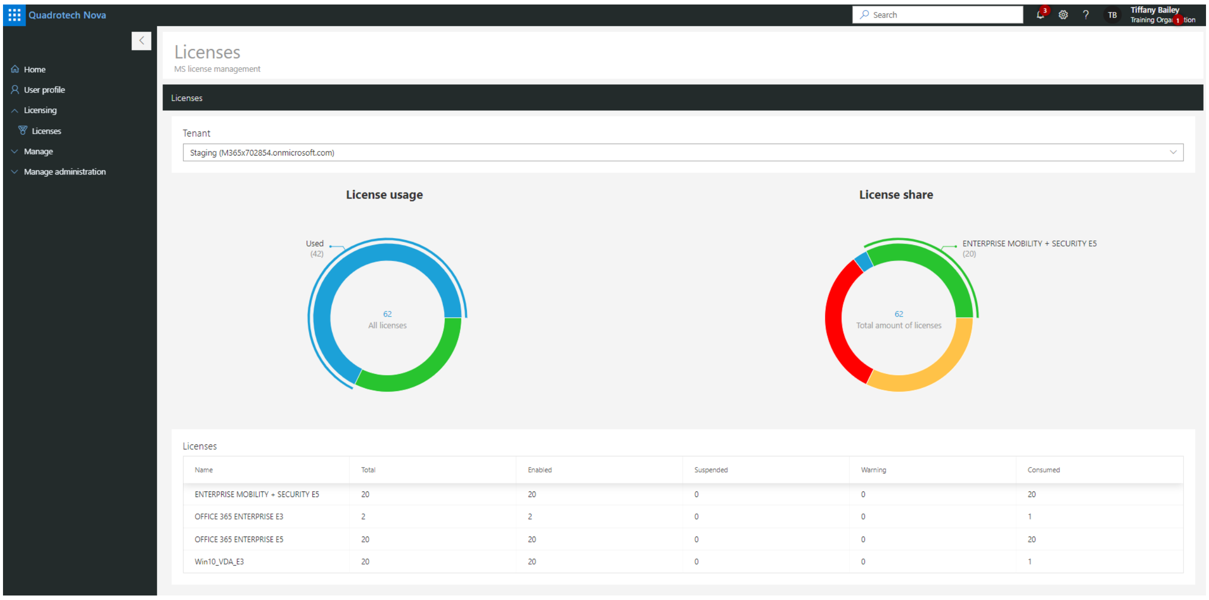
See dashboards in action in this video:

https://youtu.be/ZJ0WLxYrnqo

Overview of License Policies

Policies can be created so that Office 365 license management is delegated away from Global Administrators. For example you might want to allow regional managers handle licenses for their region.

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.



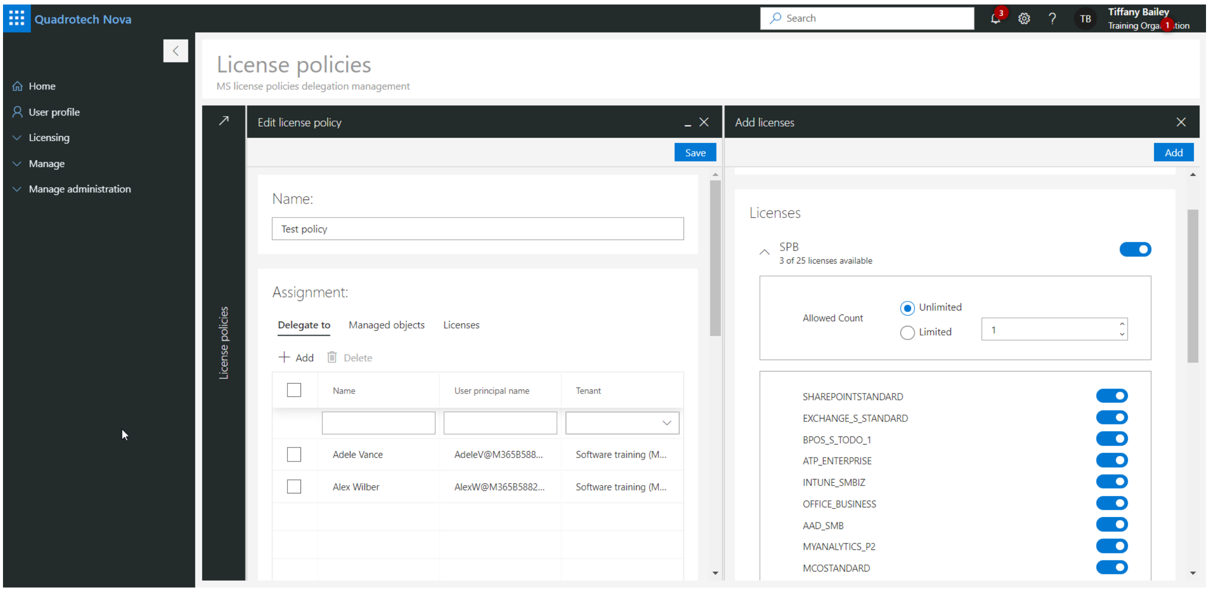
The Nova license policies and reports provide:

- The ability to apply licenses according to what has been budgeted and what's 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 Office 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 doesn't use Yammer, you can remove that workload, if desired, before assigning an E5 license to someone. You can also specify how many of a particular license delegated administrators can assign.

Here’s what it looks like when you’re setting up a license policy:



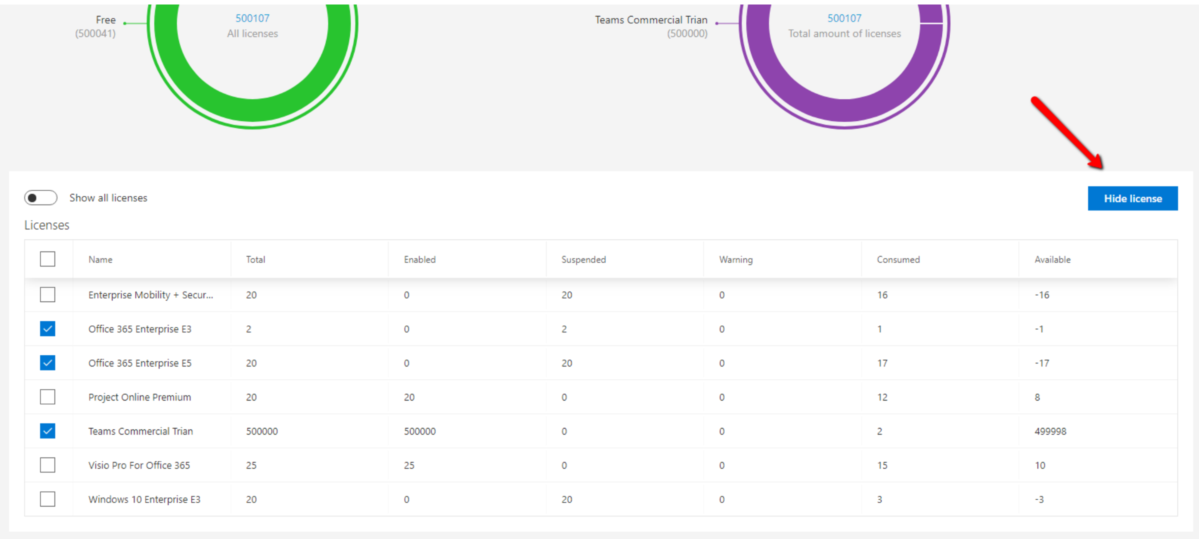
To set up a license policy:

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’ll 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’ll 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:



	Name	Total	Enabled	Suspended	Warning	Consumed	Available
☐	Enterprise Mobility + Secur...	20	0	20	0	16	-16
☑	Office 365 Enterprise E3	2	0	2	0	1	-1
☑	Office 365 Enterprise E5	20	0	20	0	17	-17
☐	Project Online Premium	20	20	0	0	12	8
☑	Teams Commercial Trian	500000	500000	0	0	2	499998
☐	Visio Pro For Office 365	25	25	0	0	15	10
☐	Windows 10 Enterprise E3	20	0	20	0	3	-3

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

Overview of On-Premises Agent

In a hybrid Office 365 environment where some resources remain on premises inside a customer organization, Nova can deploy an agent to collect metadata and perform administration. In this article we'll see how to install the agent. Once installed the agent will be automatically kept up to date by Nova.

Requirements

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

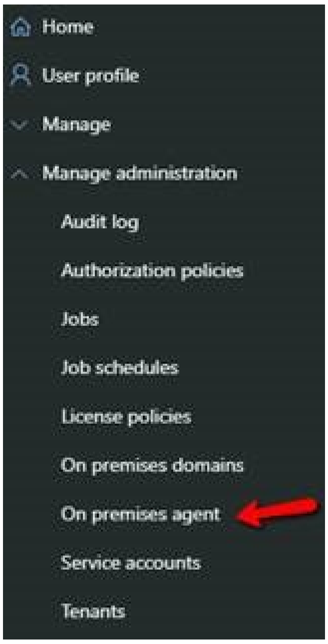
- The Active Directory module for Windows PowerShell must be installed on the machine where you'll install the on-premises agent. This can be done via PowerShell with Install-WindowsFeature -Name RSAT-AD-PowerShell
- It must have 443 access to the Nova URL for the tenant. (This is called the endpoint address)
- It must be installed on a domain joined server.
- It must have a service account that has Domain Admin rights in Active Directory 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

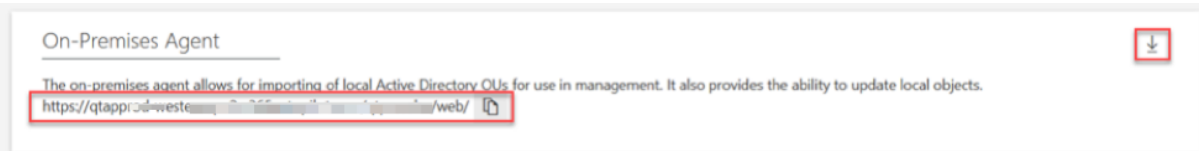
- The service account must have logon as service rights on the server.
- The agent must have a current .Net framework installed, as well as PowerShell 5.1 or above.

To obtain, and install the agent:

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



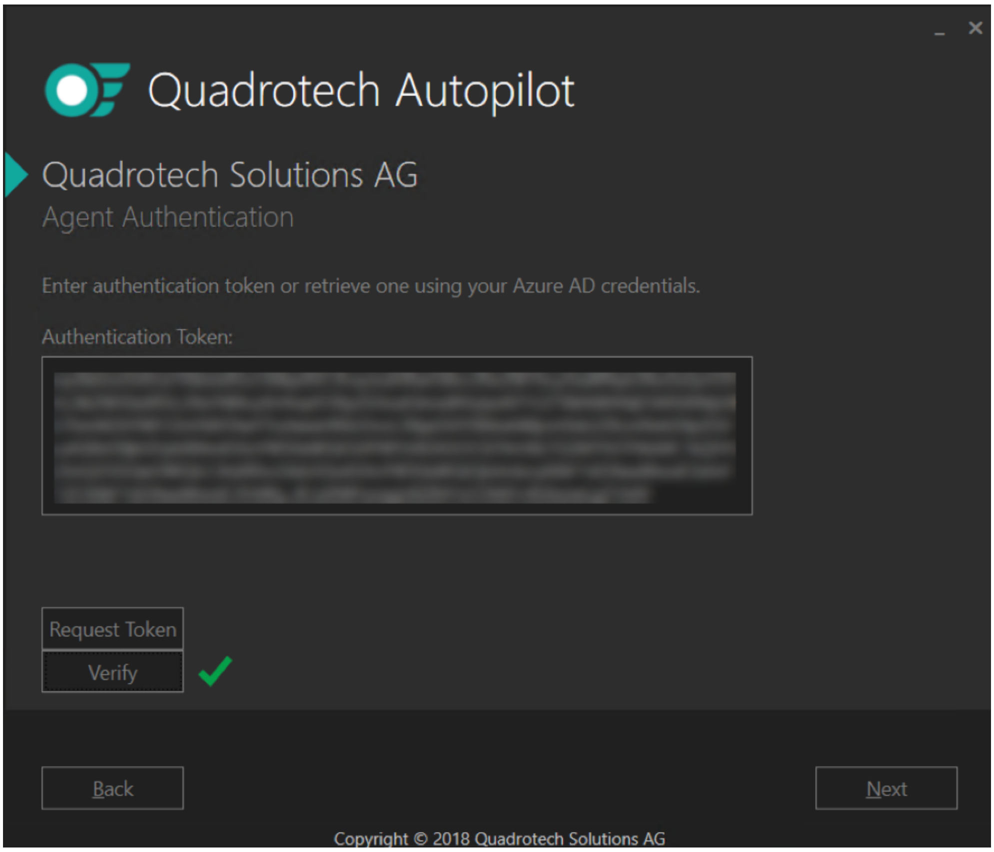
2. Ensure that the web services URL is copied and saved, it will be used during the installation:



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

Other notes

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.

Overview of On-Premises Domains

Here you can see information about the on premises domains that have been discovered by the on premises Nova agent.

Overview of User Profile

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

Overview of Adoption Accelerator

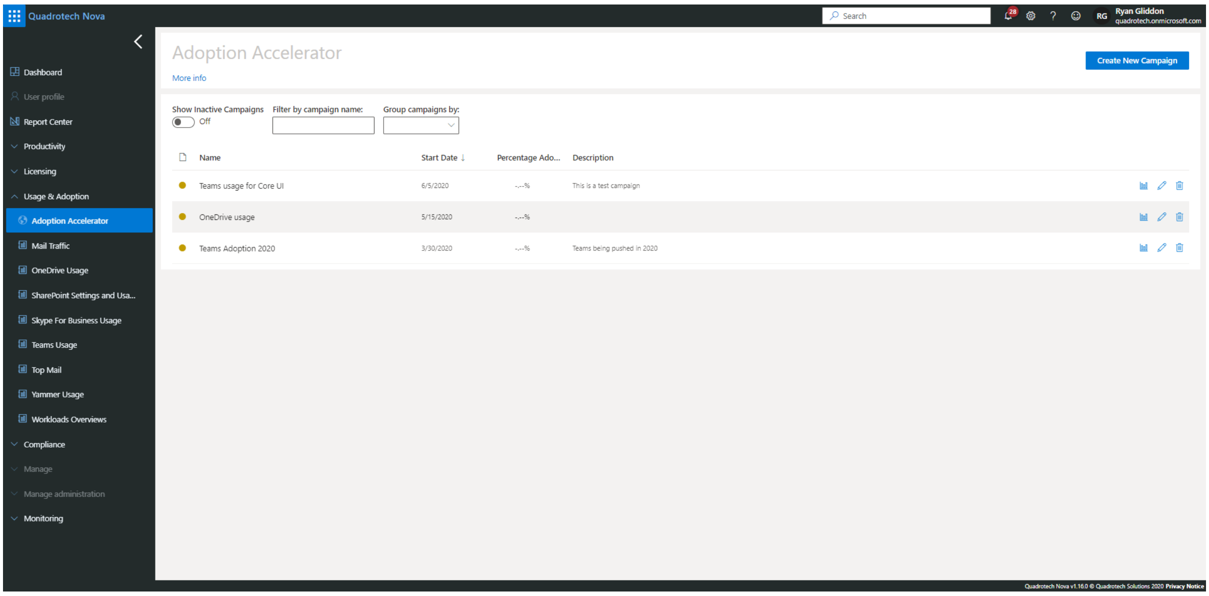
The Nova Adoption Accelerator allows you to define adoption goals and track progress against them. Every day Adoption Accelerator checks to see if users have met the goal during the last X days (the collection period). If a user has met the goals, they're considered to have successfully adopted the workload.
For more information on adoption goals, creating a campaign, and viewing, editing, and deleting existing campaigns see the Adoption Accelerator section.

Adoption Accelerator Report UI

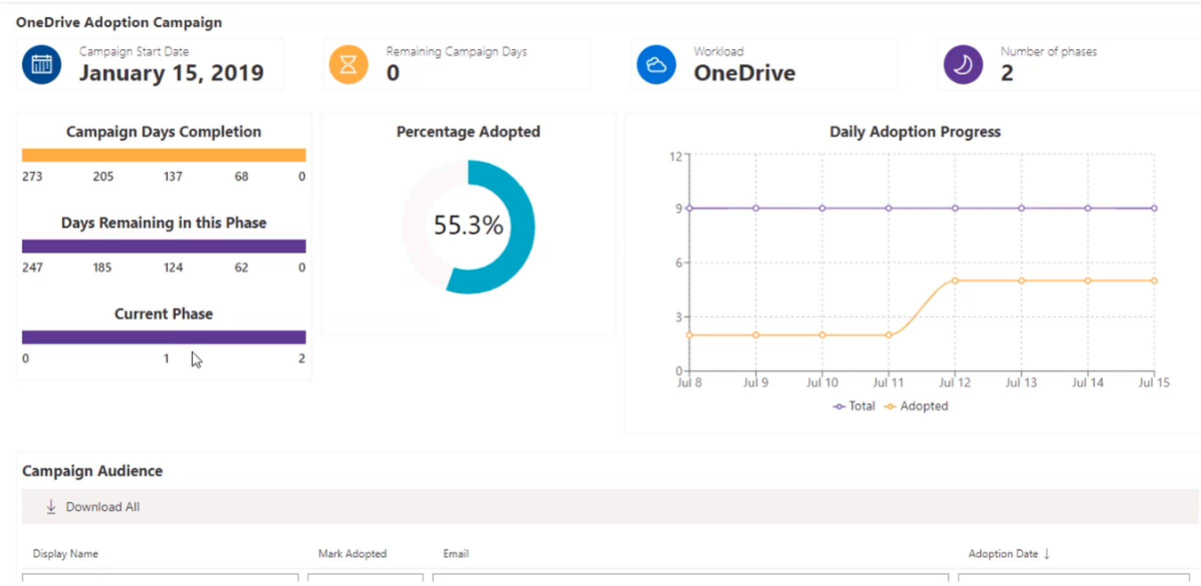
The Adoption Accelerator report user interface allows you to spend less time in searching for the Adoption Accelerator reports you need.

The User Interface now allows you to:

- toggle between hiding and showing campaigns no longer active.
- filter campaigns by their name. Search for the reports you want to see.
- group campaigns that you see in the UI. Sort campaigns by either workload (Teams, OneDrive For Business etc.) or status (ongoing or completed).



The user interface within the Adoption Accelerator reports has changed also. As you can see, data is now easier to read and digest, complete with the percentage of users who have adopted the particular workload, as well as daily tracking of the adoption campaign. Check out an example below:



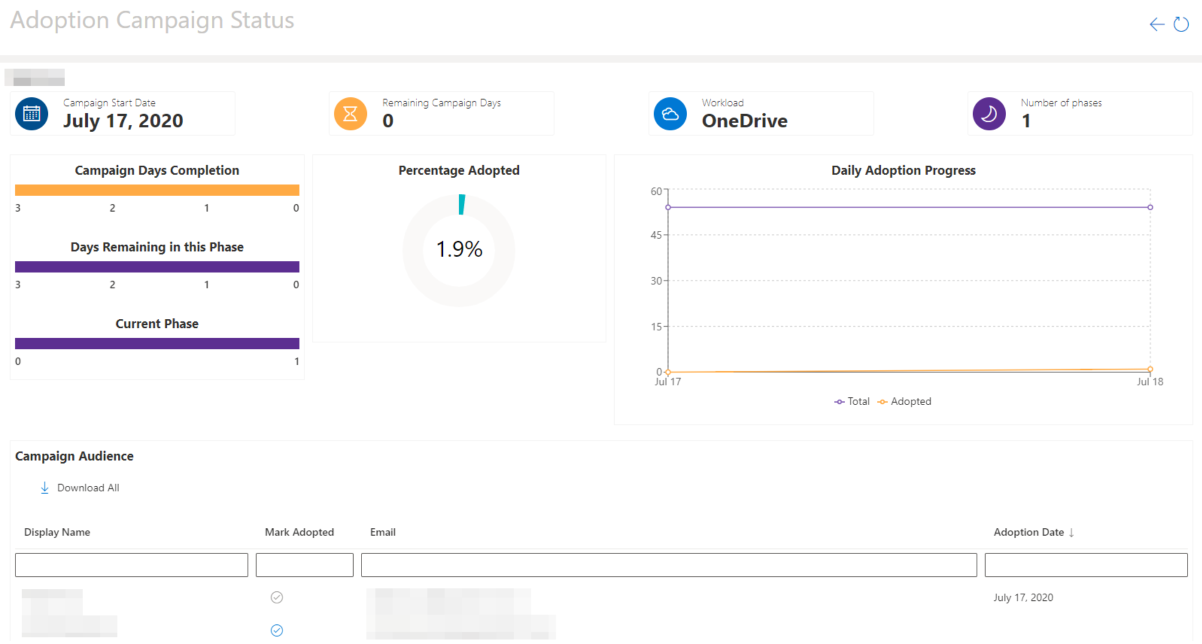
Adoption Accelerator

If people won't actually **use** a service, there's no point in having it. You won't reap any benefits. Successful implementation of Office 365 depends on user adoption. For example, when Microsoft Teams replaces Skype for Business Online, you can onboard users and get them familiar with the new platform. However, if they don't start actively using Teams for their collaboration, then the transition is going to be disruptive since you'll have to eventually force them to use the new service.

Having insight about who's using Office 365 services means you can anticipate user adoption issues and plan for them. Native Office 365 tools show you how licenses are allocated, and some basic information about how they're being used, but there isn't significant detail, and there aren't tools to support user adoption initiatives.

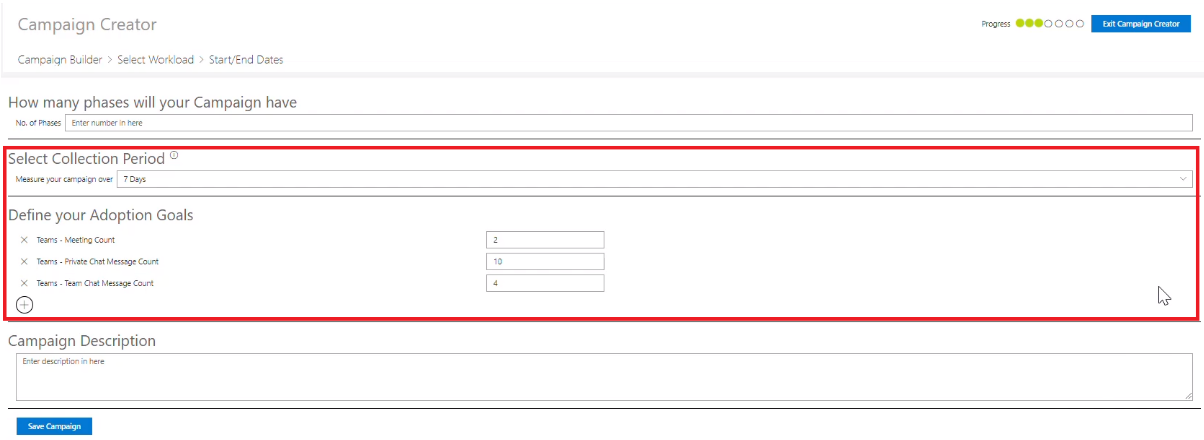
Adoption Accelerator UI

The Nova Adoption Accelerator allows you to define adoption goals and track progress against them. Here's how it looks when you check the progress of an existing adoption campaign:



Adoption Goals

When you set up a new campaign, you're prompted to set adoption goals and a collection period. These settings are used to analyze whether users are adopting the new workload. Here's how it looks:



You'll define goals for how many times you want users to perform specific actions during the collection period. So, for example, you might set a goal that you want each user to attend 2 Teams meetings during a 7-day period. Or, you might want each user to interact with a file from SharePoint 5 times within a 30-day collection period.

You might choose a shorter collection period for a workload that gets used daily, like Teams. Or, you might choose a longer collection period for a workload that gets used less often, like SharePoint. Each day the Adoption Accelerator checks if the user met adoption goals during the last X days (collection period). Any time a user meets the goals during the collection period (the previous X days), the Adoption Accelerator considers them to have adopted the workload.

Scoping Your Campaign

Before you set up a new campaign, you'll want to:

- Decide how long you'll run the campaign and what the phases will be. You'll provide dates the phases will run during the setup process.
- Determine how you'll measure whether users have adopted the workload. What are your goals? (See the *Adoption Goals* section above.)
- Create any communication materials you want to send to users during the campaign. You can add these to the Adoption Accelerator so they're sent automatically during the campaign.
- Decide which users you'll track. Will you track everyone or only certain departments? Will you use a static list of users or will you adjust your list if people leave or join the organization during the campaign?

How to Create a Campaign

Follow these steps to create a campaign:

1. Go to **Usage & Adoption** > **Adoption Accelerator.** If you are locked out of Adoption Accelerator, ensure you have the correct administration privileges. If you do and this are still locked out, contact Quadrotech support.
2. Click **Create New Campaign.**
3. Give the campaign a name and workload type, and then specify how long you want the campaign to run.
4. Identify the number of phases of the campaign. For example, you might have 3 phases broken down like this:

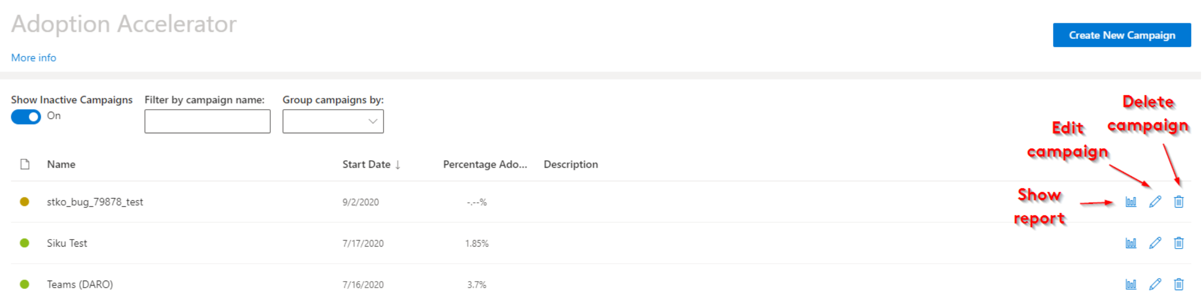
- Phase 1: Introduce the new workload.
- Phase 2: Provide more information to get users active in the workload.
- Phase 3: Provide details about corrective action to get users active in the workload.

5. Specify the time period you want to use to measure campaign progress. See the *Adoption goals* section above for more information.
6. Add goals and specify how many times you want users to perform specific actions during the collection period. See the *Adoption goals* section above for more information.
7. Enter a campaign description.
8. Define your audience type and any filters. Here's more about the Audience Type options:
   - **Dynamic:** The group of users tracked as part of the campaign changes as people join and leave the organization.
   - **Static:** A group of users is captured on the first day of the campaign and that list doesn't change throughout the campaign.
9. Define the phases by setting start date(s) and end date(s) and adding communication preferences.

Viewing, Editing, and Deleting Existing Campaigns

Follow the steps below to view, edit, or delete an existing campaign.

1. Go to Usage & Adoption > Adoption Accelerator.
2. If desired, sort/filter the list of campaigns and locate the desired campaign.
3. Either:
   - **View the campaign's statistics:** Click the graph button to view the campaign's status.
   - **Edit the campaign:** Click the pencil button, and then click through the breadcrumbs at the top of the page to edit the campaign's parameters.
   - **Delete the campaign:** Click the trash can button to remove the campaign and all associated data.



Uses Cases

Let's give an example of how you would use Adoption Accelerator.

Your organization wants to move communication platforms and believe Microsoft Teams has the best set of features that suit your users' needs. You are beginning the transition from another piece of communication software and you think it would be beneficial to get data on which users are being integrated well into Teams, and which users may need further support. Ideally, you would like the transition period (campaign date) to be around three months, and would like the campaign to happen in three phases with three adoption goals.

- **Phase One**: To ease your new users into Microsoft Teams, you may want to track the Private Chat Message Count from your users within the first couple of weeks to see who has began using Teams.
- **Phase Two:** You may be hoping to see collaboration within your departments, so defining an adoption goal around Team Chat Message Count is the best method to track this.
- **Phase Three:** By this point, you are hoping that your users are now mostly communicating with Microsoft Teams. This would be a good point to see the overall scope of your adoption campaign with Total Activities.

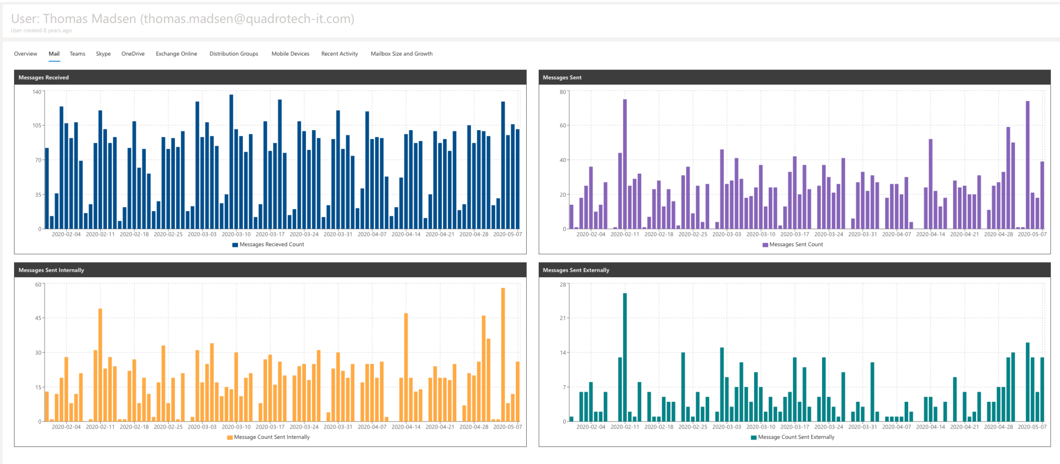
After your campaign has finished, you then have the opportunity to see who has been fully integrated into Teams and who may need further support.

Video Overview

Here's a video showing Adoption Accelerator in action:
https://youtu.be/vZvwpBhsUio

Mail Statistics in Noval User Profile

The User Interface gives an administrator better a understanding of mail usage for a specific user.



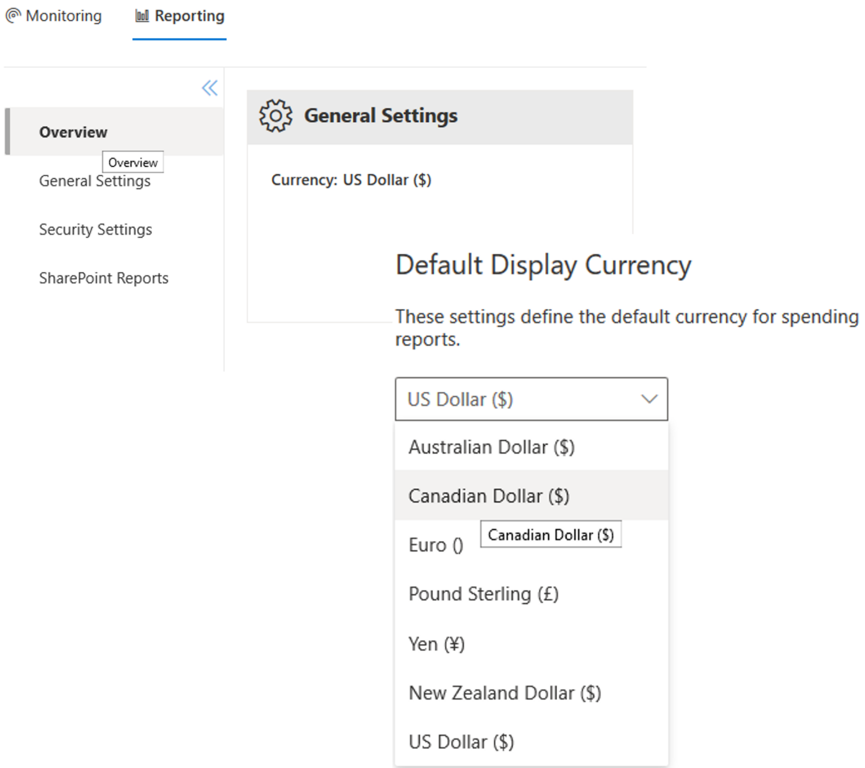
Set a Currency Symbol for your Reports

Users have the ability to set currency for your reports if required, instead of a generic number. This gives your report better context and understanding. Currencies currently supported are:

- US Dollar ($)
- Australian Dollar ($)
- Canadian Dollar ($)
- Euro (€)
- Pound Sterling (£)
- Yen (¥)
- New Zealand Dollar ($)

More currencies will be added soon.

To do this,
1. go to the **settings cog** on the top right hand side of Nova.
2. click **Reporting**.
3. go to **overview**
4. On **General Settings,** find **Default Display Currency** and find your currency from the drop down list.

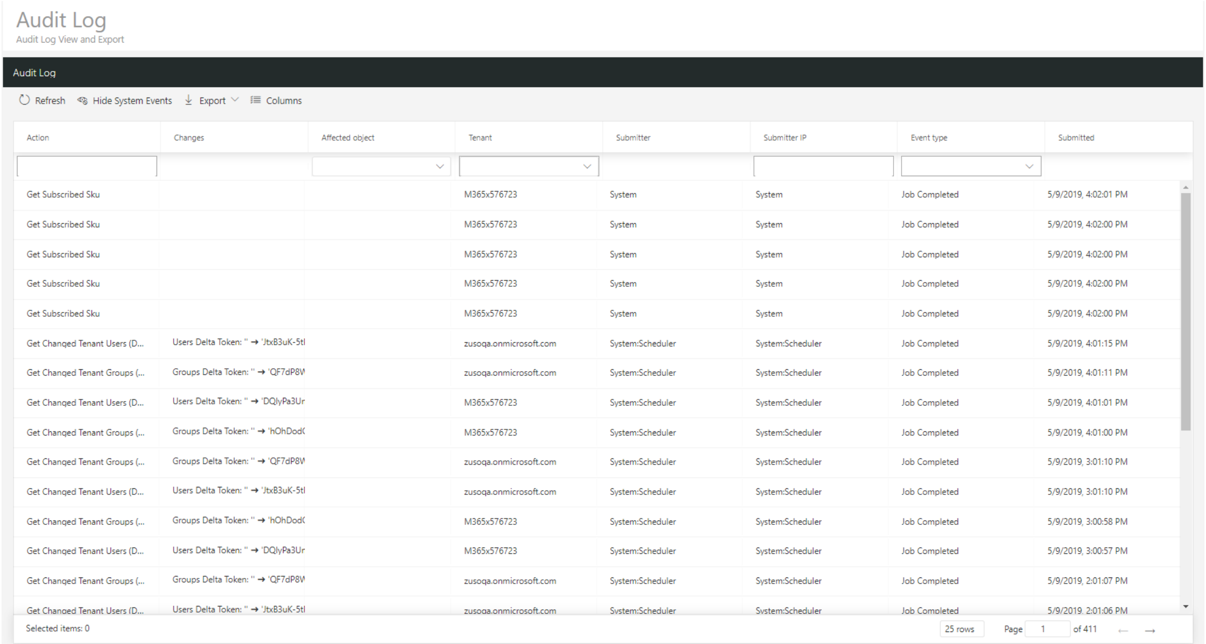


Manage Administration Audit Log

The audit log shows who performed what actions against which object. The audit log can be filtered and sorted. Additionally, you can customize which columns display.
Here’s more information about the audit log:
Using the Audit Log

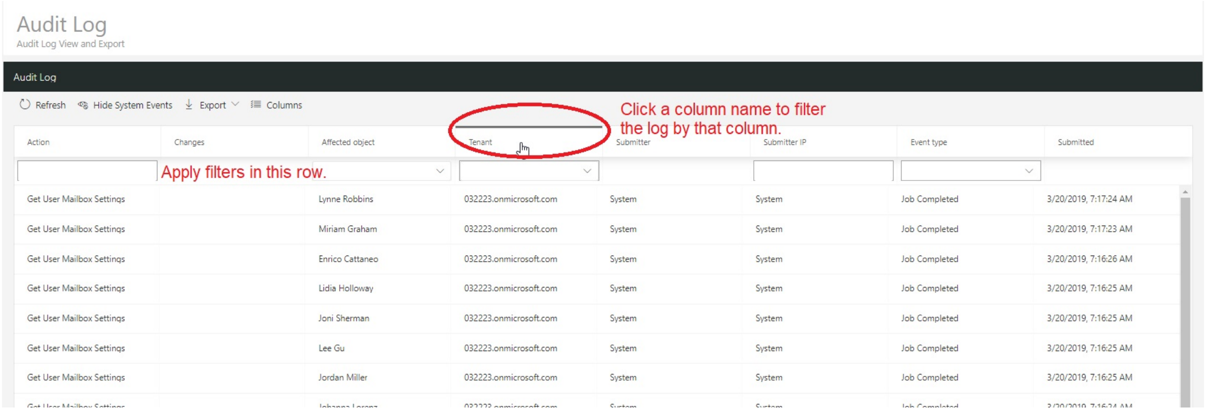
Using the Audit Log

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



Filtering and Sorting the Audit Log

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



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

Audit Log Contents

Here's 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

Video Overview

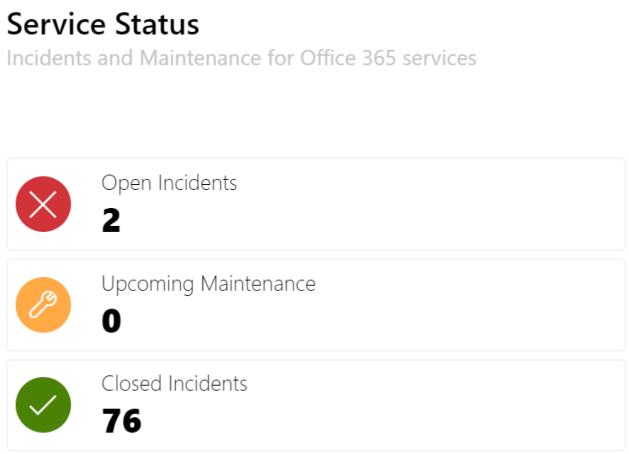
Here's a video showing the audit log:
https://youtu.be/t3uvL5L_GAY

Add a Service Status Widget in the Nova Dashboard

Users can view maintenance and incident reports straight from the Nova dashboard. This allows users to get a quick look at the outlook of their Office 365 services.

To add the Service Status Widget do the following:

1. Go to your Nova Dashboard, and click **Edit**.
2. Click **Add widgets**.
3. Find the Service Status widget. This will then appear in your Nova dashboard.
4. Click **Save**.



Voice Workloads Key Metrics Overview in Nova

Transponder beacons and workloads monitor a number of key metrics for both Skype for Business and for Teams. There are many results in the test results dialog for the voice workloads (Skype and Teams) which are for informational purposes only, but may be valuable to help troubleshooting issues between the beacon and the remote endpoint.
This article will describe key metrics for voice workloads. Strategic placement of customer beacons and workloads is valuable to help determine how your infrastructure impacts VOIP call quality for your users.

Round Trip Latency

- Measures the time taken to send a data packet from the beacon server to the remote endpoint (Remote IP). Round trip time is affected by the physical distance between 2 endpoints and the transmission speed and any overhead on the routes in-between.
- The latency impacts the call quality between 2 people.
- Too much latency causes breaks and gaps in voice conversations.
- When you are on the phone and people end up talking at the same time, the likely cause is too much latency.

Packet Reorder Ratio

- Packet reordering is important because excessive reordering of packets will also affect call quality.
- When packets arrive in a different order than they were send it can be seen as packet loss or network congestion.
- This metric is also used to calculate the Mean Opinion Score.
- Packet reordering can impact packet send rate which will increase round trip time.
- Calls can be distorted and cut out at times.

Packet Loss Rate

- Microsoft recommends to keep packet loss less than 1% during a 15 second call.
- If packet loss is less than 3%, acceptable call quality can be maintained. Thus the default threshold for a healthy scan is packet loss < 3%.
- Packet loss rate is used in the Mean Opinion Score calculation.
- Excessive packet loss during a call will result in degraded voice quality and call attendees may sound like a robot.

Mean Opinion Score

MOS is a prediction of end-user audio quality experience. Multiple factors are considered in calculating the MOS (Mean Opinion Score). The score ranges from 1-5. The highest score is usually around 4.4 because of the audio codec in use.
A MOS < 3 will result in poor call quality
A MOS < 2 will result in critical reduction in call quality.

Degradation Average

- This metric shows the impact of jitter and packet loss. This value should always be less than 1 for acceptable user experience.
- If you see degradation here, you will encounter audio distortion. This is the result of network congestion or insufficient bandwidth, which impacts packet loss and jitter.

Average Jitter

- Audio packets are sent at regular intervals. Sometimes they are not received with the same intervals (usually because of network latency).
- The buffer waits for all packets before reconstructing them in the correct order.
- Jitter is the size of the buffer that is needed to store packets before reconstructing them.
- Jitter value is calculated over a 15s period.
- Low jitter means that the connection to the call is healthy.
- Medium / High jitter is a sign of network congestion.
- Jitter is also used in the Mean Opinion Score calculation.

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's 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 **NovaReporting** or **NovaDPC.**

NovaReporting

This is for a service account to fetch data for the **Reporting** module. It needs to read data from the O365 tenant only.
Details on how to assign appropriate roles is detailed in this section.

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

3

Delegation & Policy Control (DPC)

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

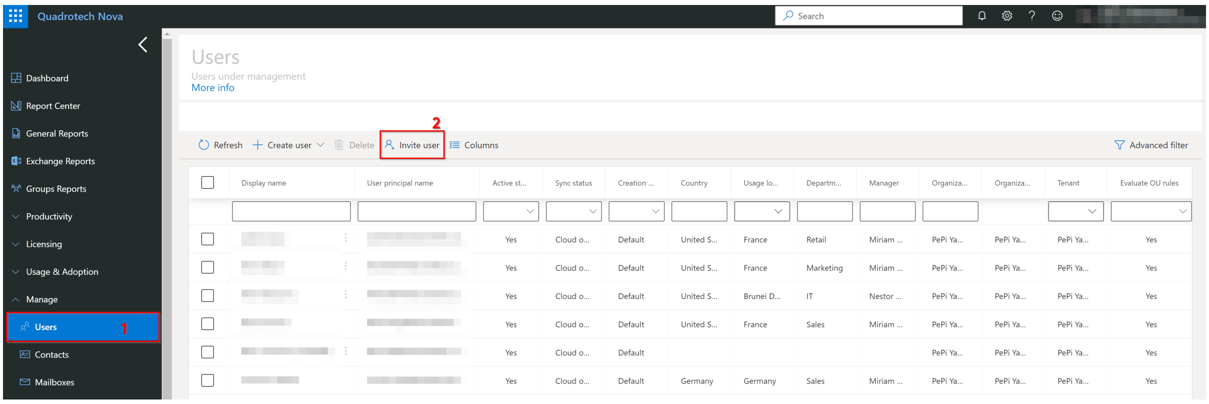
See the following topics to take a look into what DPC can do to manage users within your environment:

- Authorization Policies
- Delegating Administrative Rights Using Nova
- Policy Properties
- Authorization Policy Properties
- License Policies
- Service Accounts for DPC
- Configuration Policies
- Perform Custom Tasks with Powershell
- User Assignment Rule
- Device Compliance Policies
- Policy Examples
- Virtual Organizational Units

Inviting Guest Users to a Tenant

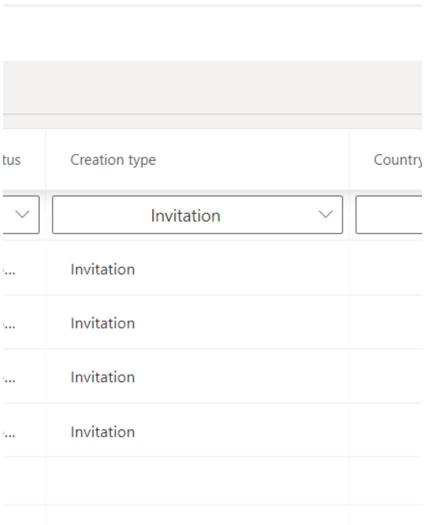
Using Nova Delegation and Policy Control a delegated administrator can be given the ability to invite guest users into a tenant. Here is how that's done.

On the create users screen, there is a new button called 'Invite user':



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:

To enable a delegated administrator to easily see the type of user in a list of users, a new field was added:



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

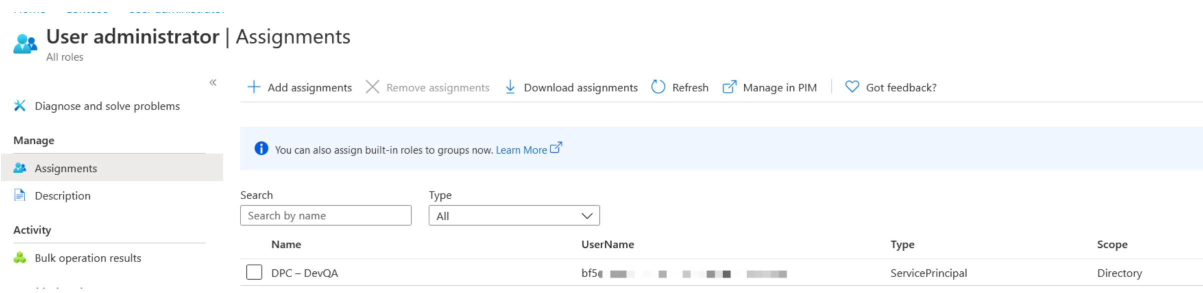
How to Configure Nova DPC to use OAuth

Some organization might want to use oAuth for authorization of actions performed by Nova Delegation and Policy Control, rather than service accounts. To do this, follow these steps:

Go to Azure Active Directory

Go to Roles and Administration

Locate the DPC application, as shown below:

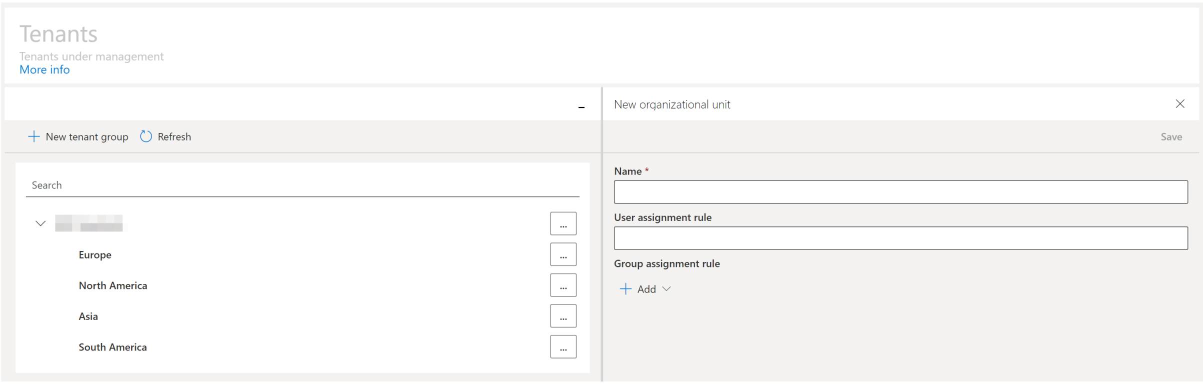


Grant **Exchange Administrator** and **User Administrator** roles for the application.

After this Nova DPC will use oAuth for authentication.

Automate Group Management Delegation

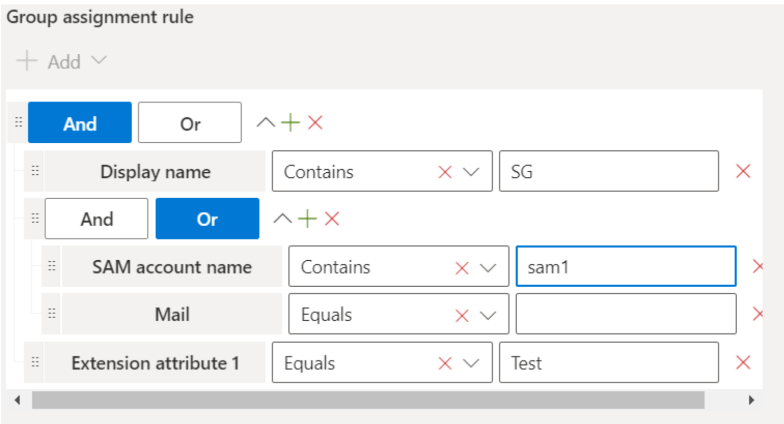
As a Nova administrator, you have the ability to automatically assign group management delegation based on properties of the group or group owner. This allows you to delegate responsibilities to localized IT support without granting them excessive access to your tenant(s).



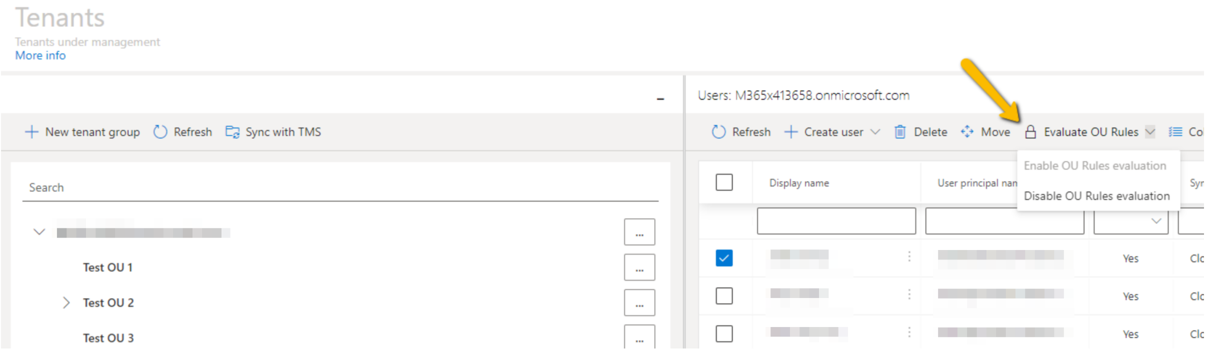
To automate group management delegation:

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.



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.



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.

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

For a service account to be effective:

- It needs to be a global administrator in the 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.

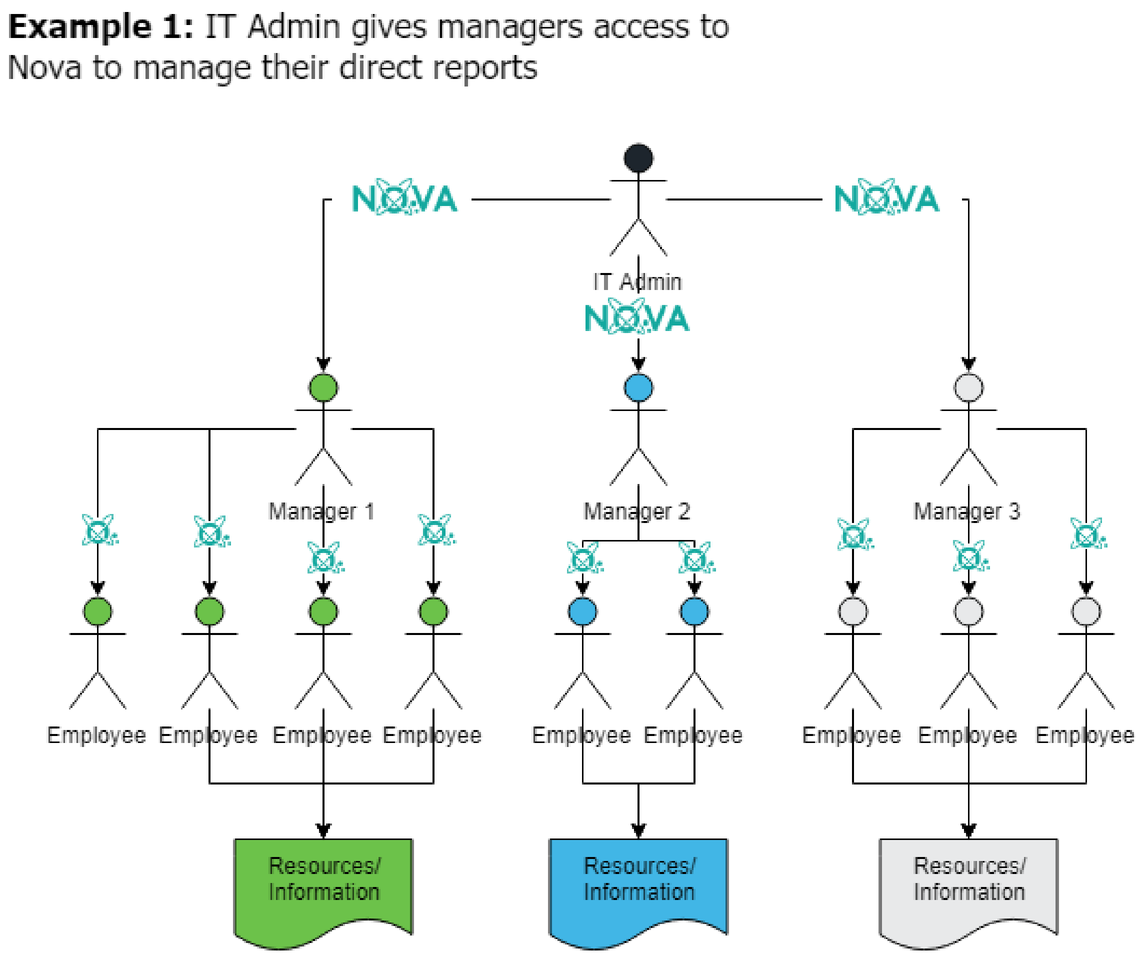
NOTE: If the password of the service account is changed, it must also be changed in Nova DPC.

Nova Delegated Administration

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

Managing Direct Reports

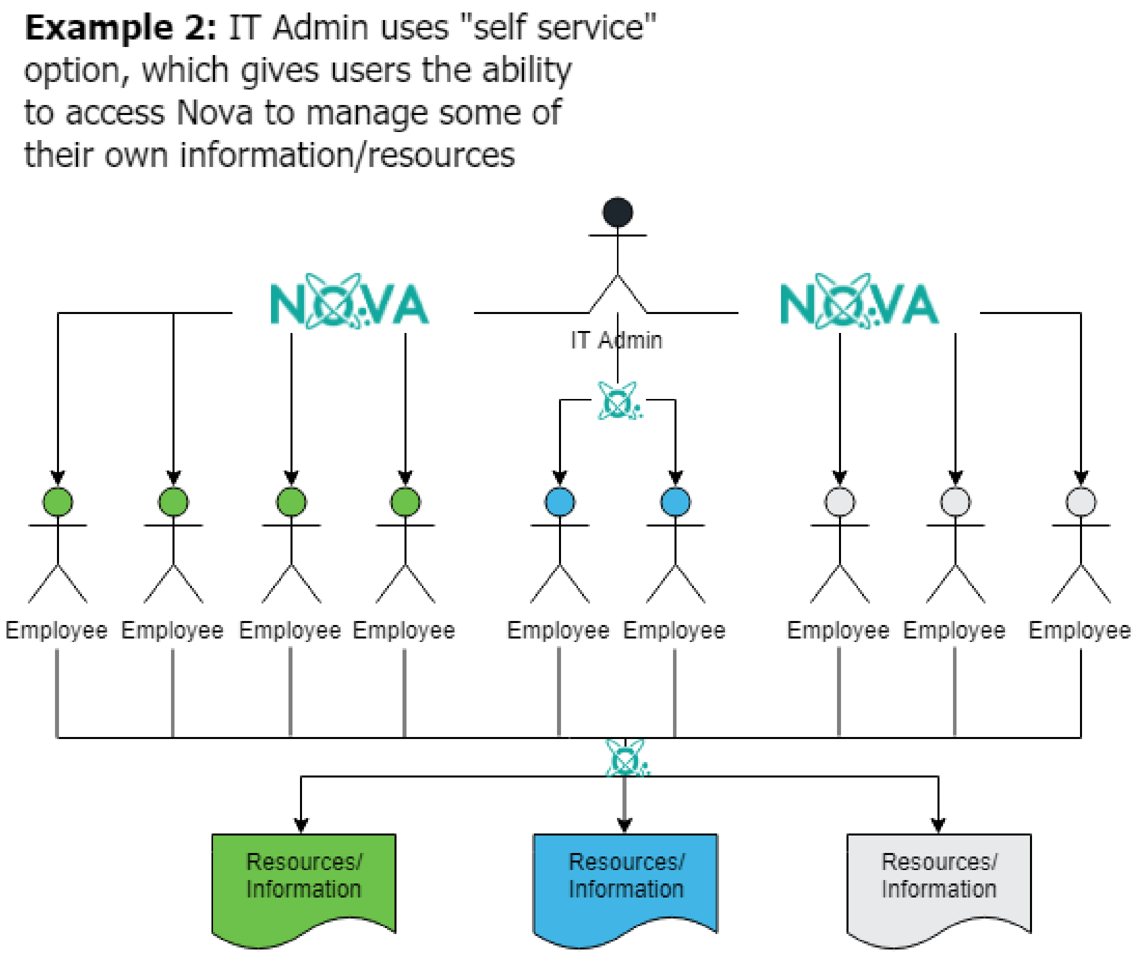
An administrator could give sales managers the ability to manage certain attributes and/or rights of the individual sales team members without any additional rights granted either on-premises or in Office 365 for those sales managers. Here's how it looks:



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.

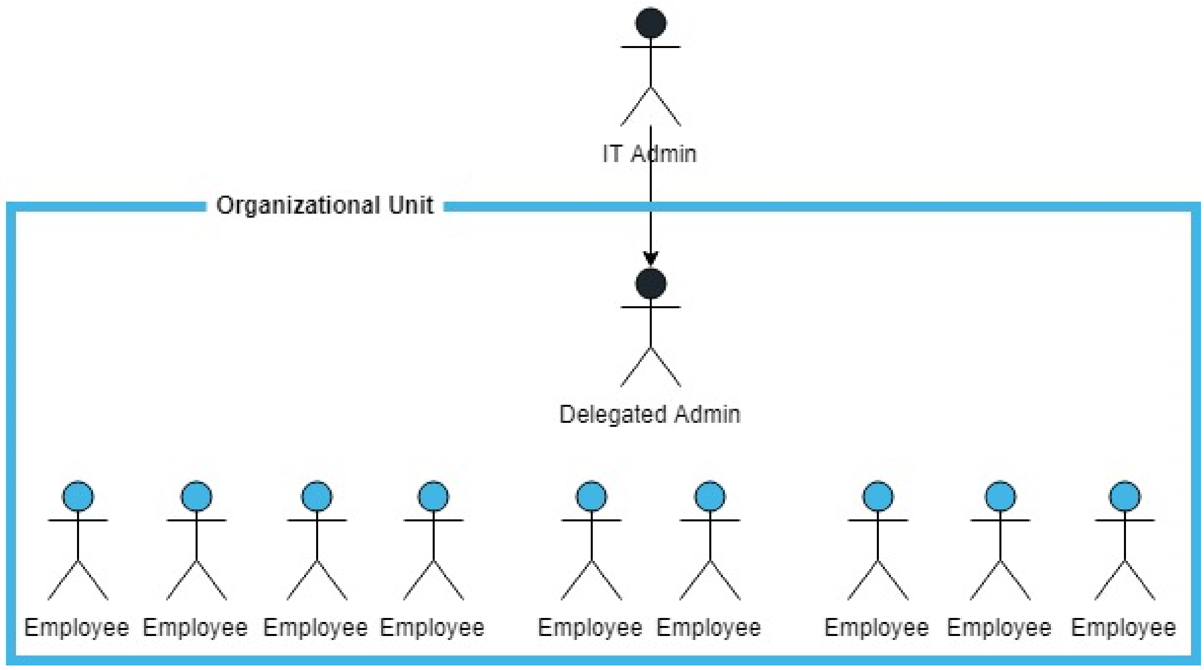
Similarly, you might configure a policy that enables all employees to use Nova to update some of their basic information (for example, their phone number and address). This is called the “self service” option, here’s how it looks:



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.
- A delegated administrator can manage Microsoft Teams.

Resetting a User Password

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

1. Locate the user.
2. Bring up more detailed information about the user by clicking the ellipsis and choosing **Detail**.
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:
https://youtu.be/R1cyDHvzjd4

Set an Out Of Office Reply

It's easy to set an Out of Office reply with Nova, here are the steps:

1. Locate the user.
2. Open the user's mailbox detail by clicking the ellipsis and choosing **Mailbox**.
3. Click **Automatic replies.**
4. Click **Set out of office.**
5. To set an Out of Office reply, change the status to either:

- **Always Enabled:** Enter reply messages.
- **Scheduled:** Choose the dates/times you want Out of Office replies to start and end, and enter reply messages.

6. Click **Save**.

Nova will make the update and a notification will be generated when the job is complete.
Take a look at how to do these steps in this quick video:
https://youtu.be/zOh4f5H_67k

Manage Microsoft Teams

It's easy to manage Microsoft Teams with Nova, here are the things that you can do:

- Create new Teams
- Modify settings on existing Teams
- Add or remove Channels
- Add or remove members of the Team
- Create logical groups of Teams and perform actions on the whole group

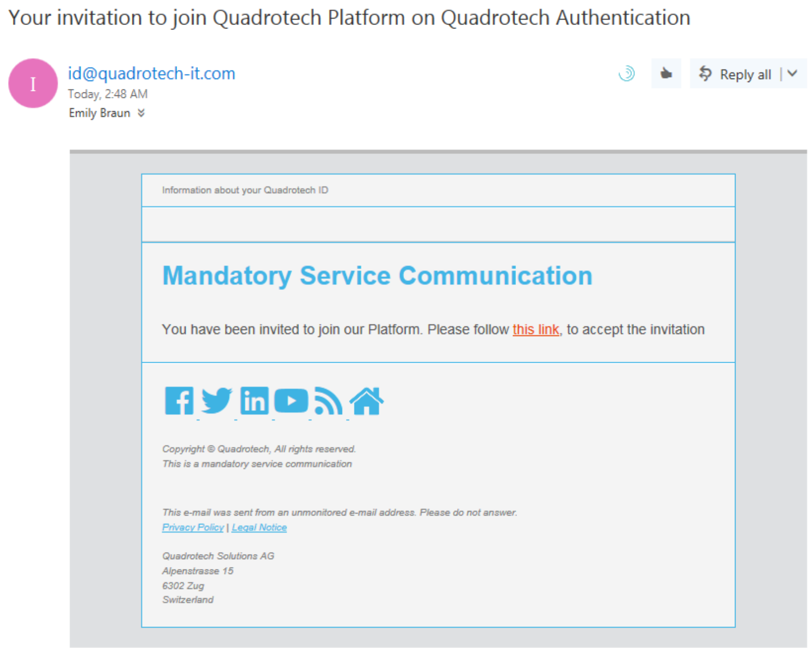
Take a look at video showing some of these options:
https://youtu.be/MIoB-JALc3c

Overview of My Invitation

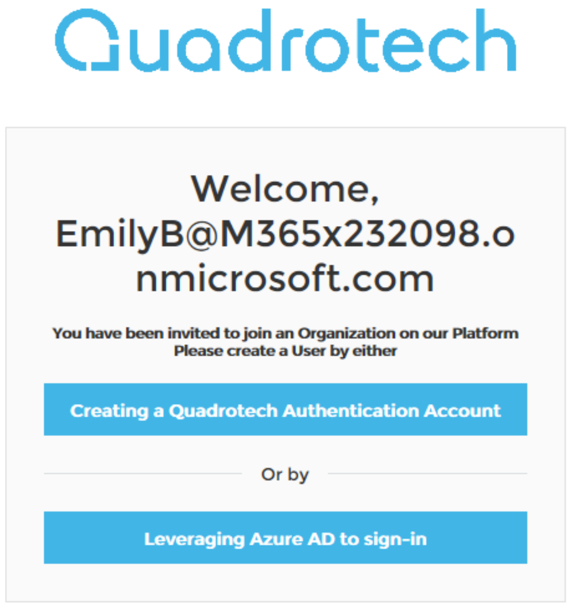
After someone invites you to associate with an organization and delegates management rights to you, you can use this page to see the status of your invitation and accept/decline it.
Click here for more information on the process of being invited to access Nova.
Click here to learn more about the Tenant Management System and adding tenant administrators.

Invitation to Access Nova

This article describes what a user sees when they're invited to access Nova.
First, the user receives an email invitation that looks similar to this:



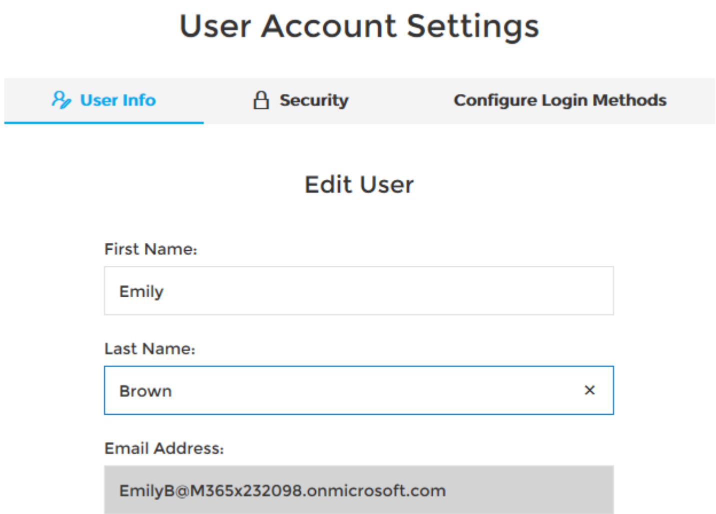
When they click the link in the email, they're prompted to create a user account:



Here's more about the options to create a user account:

- **Creating a Quadrotech Authentication Account:** Create credentials that are unique to their Nova/Quadrotech account.
- **Leaveraging Azure AD to sign in:** Use Azure Active Directory credentials to access Nova.

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



Overview of Custom Powershell

The Custom PowerShell page shows a list of PowerShell scripts which have been added to Nova. You can:

- Add new scripts
- Edit or delete existing scripts

- Execute a script

> **NOTE:** Only System Administrator and Account Administrator role holders can access this page and perform actions with custom PowerShell.

Click here to learn more.

Custom Powershell

The Custom PowerShell functionality in Nova allows almost any PowerShell scripts to be executed to perform custom tasks within your tenant organisations.
This functionality is accessible to users who have the any of the following roles:

- System Administrator
- Account Administrator

More details on the scripts, validation, parameters and so on, 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
2. **Manage Administration** > **Custom PowerShell**.
3. Click on 'Add'
4. Give the custom PowerShell script a meaningful name.
5. Select the online PowerShell-type that the script will run against. You can choose one of the following:
- Exchange Online
- Azure AD
- 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 Administration** > **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 Administration** > **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. **Note:** You may need to scroll down the page in order to see the list of parameters
6. Click on the ‘Execute’ button

Nova will now submit a job for this script to 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 Administration** > **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. For more information on the jobs page, click here.

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

Custom Powershell Additional Details

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.

Supported Types

The following is a list of the supported types:

PowerShell	Field	Notes
-none-	Text	
[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

Recognised 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]
Will be supported in the future.

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	
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 AzureAD module:

```
param(
[Parameter(Mandatory=$true)] $displayname,
[Parameter(Mandatory=$true)] $givenName,
[Parameter(Mandatory=$true)] $surName,
[Parameter(Mandatory=$true)] $upn,
[Parameter(Mandatory=$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" -UserPrincipalN
Set-AzureADUser -ObjectID $upn -UsageLocation $usageLocation
# Create the objects we'll 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).SkuI
# Set the Office license as the license we want to add in the $licenses object
$licenses.AddLicenses = $license
Set-AzureADUserLicense -ObjectId "$upn" -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"
```

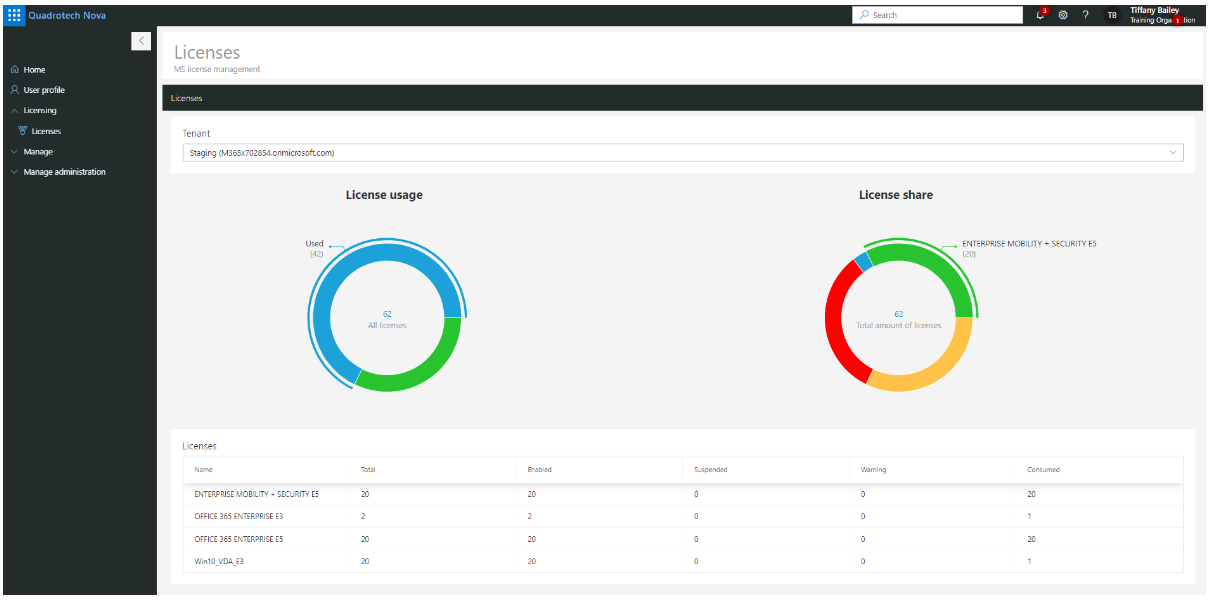
Overview of Licenses

The Licenses page shows information about licenses in tenants that you can access. On this page you can:

- View license information on the current or other accessible tenants
- View how those licenses are assigned
- Depending on license policies, you can assign licenses to users.

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. Take a look:



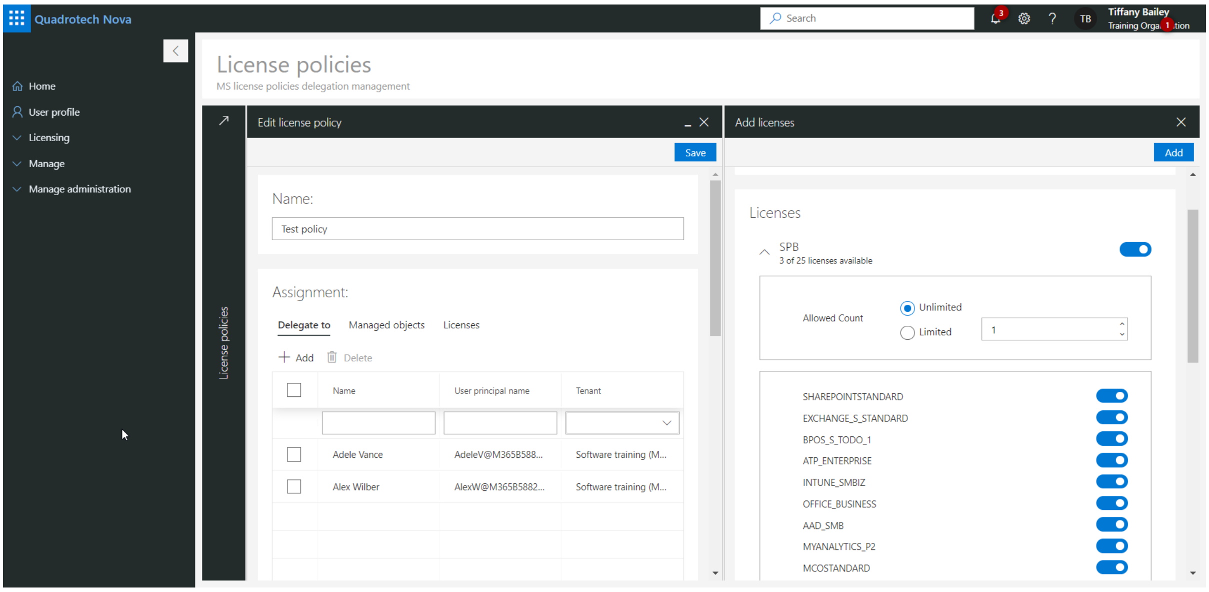
The Nova license policies and reports provide:

- The ability to apply licenses according to what has been budgeted and what's 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 Office 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 doesn't use Yammer, you can remove that workload, if desired, before assigning an E5 license to someone. You can also specify how many of a particular license delegated administrators can assign.

Here's what it looks like when you're setting up a license policy:



Setting up a license policy

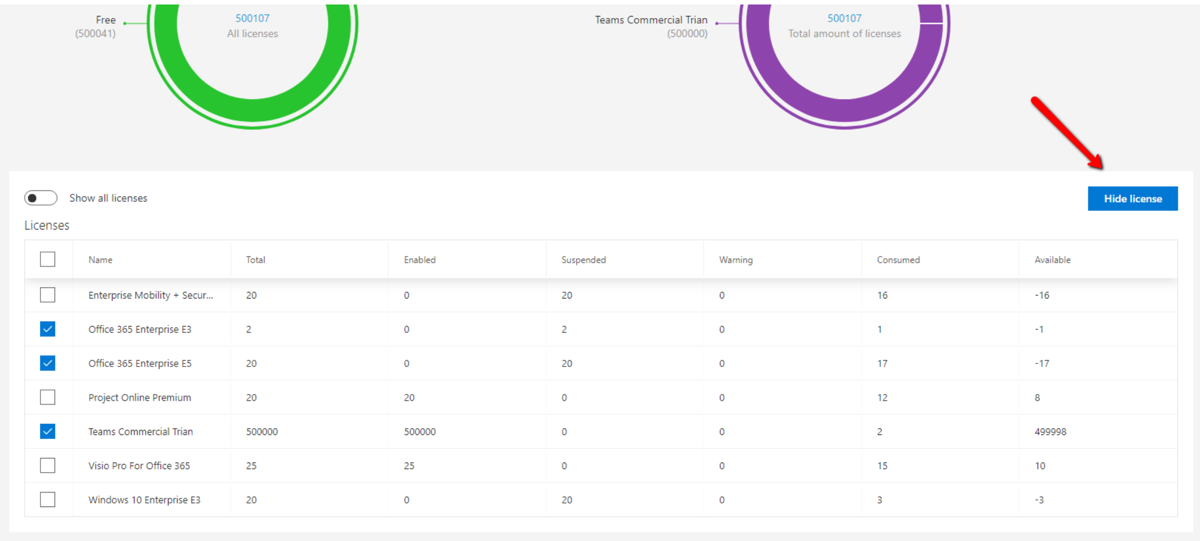
Follow these steps to create a new license policy:

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'll 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'll 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.

Hiding licenses

You can hide selected licenses from the licenses report, if desired:



And, you can show/hide any hidden licenses by using the toggle option located in the top left of the list.

Overview of Configuration Policies

Configuration policies bring standardization to a particular tenant (also called an 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.

Here’s more information:

Creating a policy
Assigning a policy to an organizational unit/tenant
Exporting or importing policies
Processing configuration policies in an organization

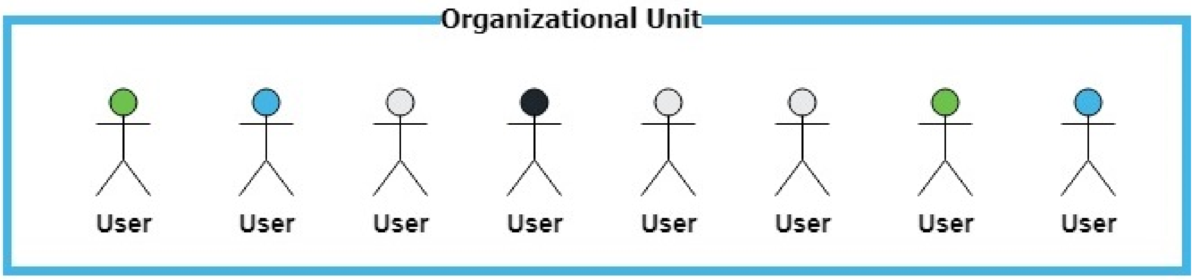
Creating a Configuration Policy

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.

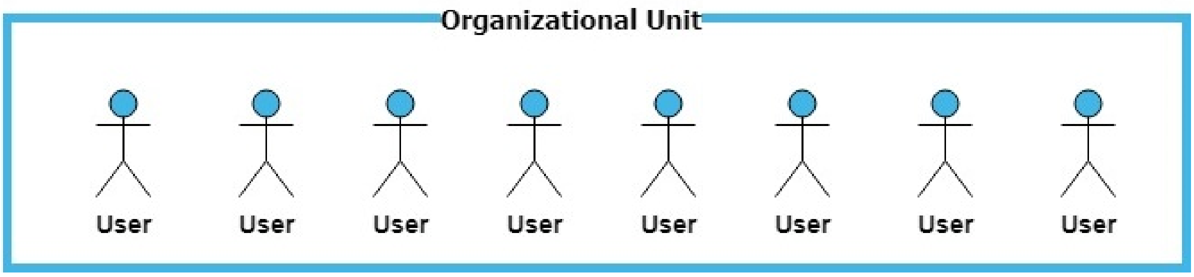
Or, you might manage two tenants. One contains people working in the United States, and the other contains people in the United Kingdom. You can create configuration policies to give users in the United States a Country attribute of US. And, another configuration policy gives users within the United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

https://youtu.be/wxvwsZgqCmo

Creating a Configuration Policy

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**.

Check out the video below for a video walkthrough:

https://youtu.be/FFq5KQTHSAA

Examples of Configuration Policies

Check out a couple of examples of configuration policies which may be helpful in your environment.
Assign a Manager to a vOU
Set a User's Country and Location Details

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.

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 Office 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 Office 365 user attributes.
- **Update On-Premises User**: Update on-prem user attributes.

Processing Configuration Policies in an Organization

Find out about the processing of the virtual organizational unit structure here.

Configuration Policy Example 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 the video below for a walk through.
https://youtu.be/D9Ck-BZu85A

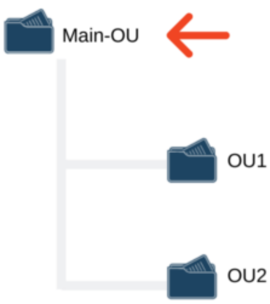
Configuration Policy Example Set a Users Usage Location and Country Details

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:
https://youtu.be/YFb5PG5bfQM

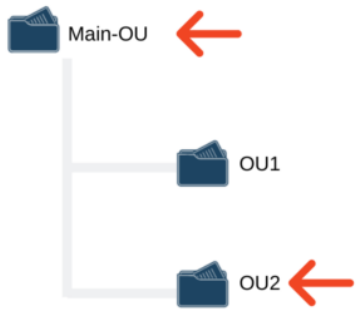
Processing Configuration Policies in an Organization

In many organizations a structure of organizational units will be built, and configuration policies in Nova Delegation & Policy Control can be used across this structure. In this article we'll see how the processing of those policies takes place.
In this example we'll use this simple organizational unit structure:

If we create a new policy and apply it to the Main-OU organizational unit we have the option to 'apply to child OUs'. If we select that option, when the policy is applied at the top level, any child OUs will also be affected by the policy:



In this case OU1, and OU2, will also use the same policy that was applied at the Main-OU level.
If we then create a policy and apply it to OU2, we can override any of the impact from the other policy:



In this case, Main-OU and OU1 will use the original policy, and OU2 will use the new policy.

Authorization Policies Overview

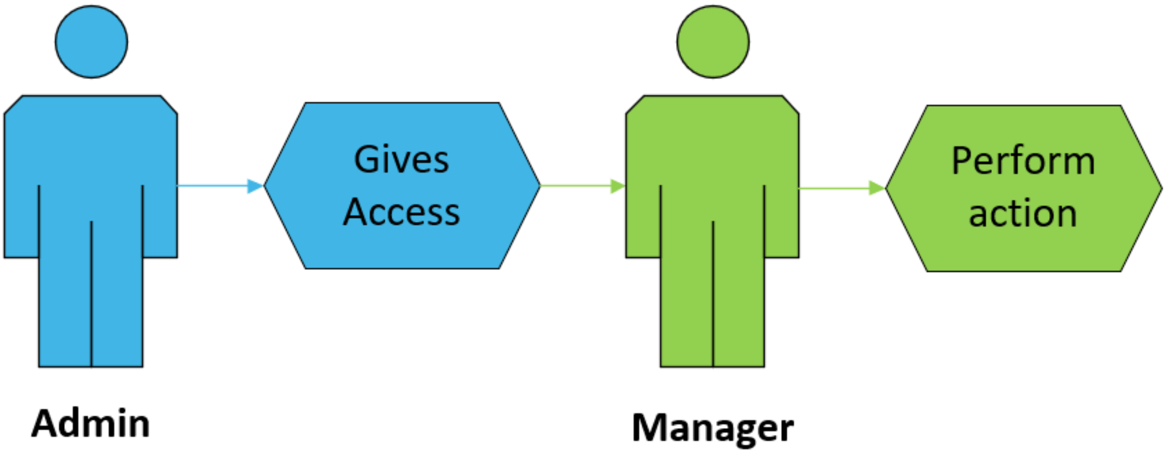
Nova authorization policies are used to set up Role-Based Access Control (RBAC). A Nova administrator configures authorization policies to specify who can perform certain actions within a tenant, and the conditions associated with those actions. They delegate the ability for users to do something, against something. Using the policy properties, you can get very granular in how you delegate access. 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 helpdesk) cannot read and/or edit certain information.

Here is more information about Authorization Policies:

More about authorization policies
Setting up a policy
Delegating action(s) to a policy
Setting policy properties
Exporting or importing policies
Delegation examples

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

There are 4 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, let's say 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 AAD 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's important to note the manager's Nova instance only shows options that are relevant to the activities they can perform in the application.

Here's a video overview of authorization policies:
https://youtu.be/-CrMNwCFNq8

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'll 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're 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 blue **Save** button.

Examples of Authorization Policies

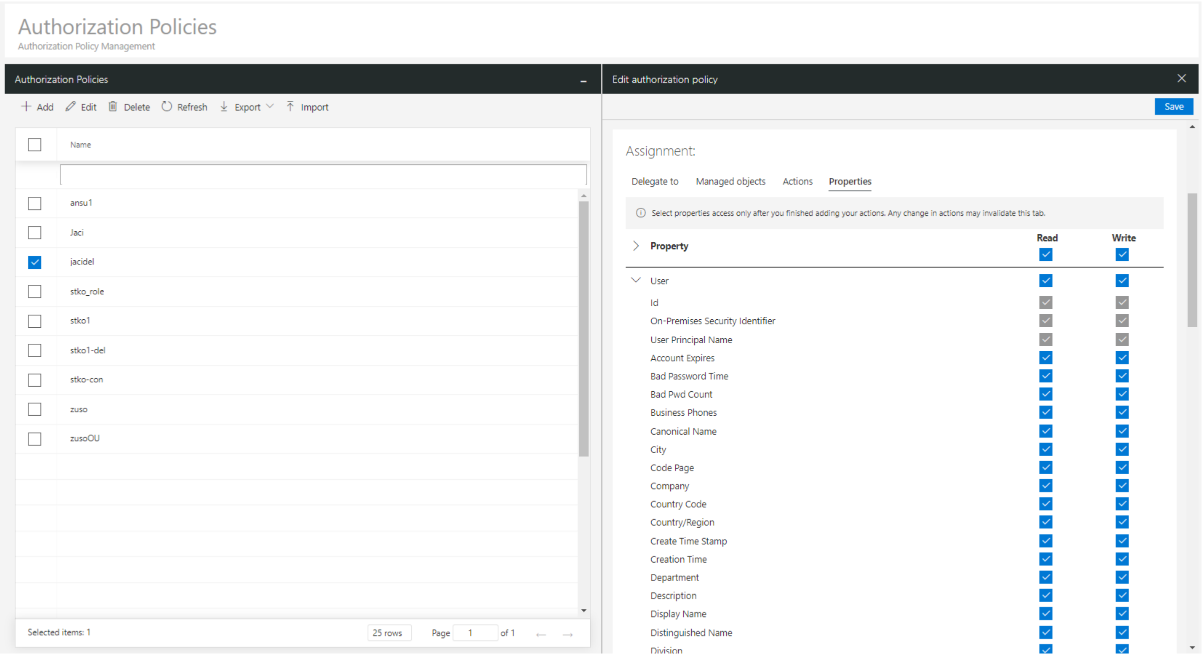
To see some examples of authorization policies, click here.

Which Policies Apply?

After you've gone through the work of setting up and assigning policies, here's how you can see which policies apply to a certain virtual organizational unit:
https://youtu.be/ypPLSeppY2c

Nova Policy Properties

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



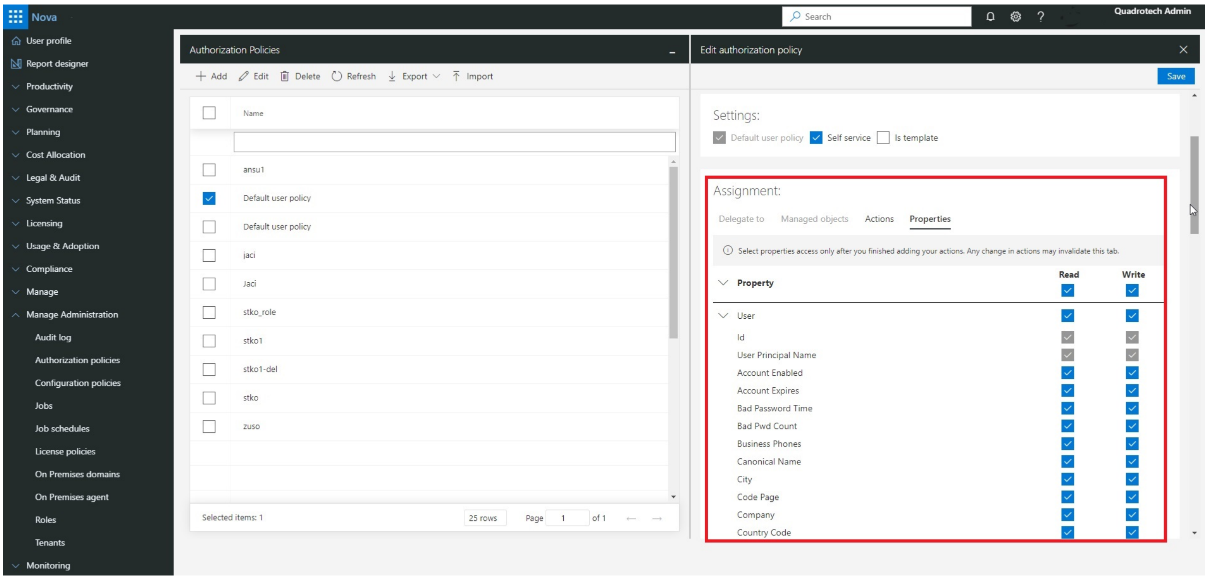
After adding actions to a policy, you can select whether delegates can see or edit information related to the assigned actions.

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's a video showing more about properties:
https://youtu.be/UTpd7BFJDrE

Nova Authorization 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, using the **Properties** tab, you can select whether delegates can see or edit information related to the assigned actions. This allows you to get really granular in how you delegate access.

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.

Examples of Authorization Policies

Below, you will find some examples of authorization policies in Nova. For more on authorization policies, click here.

Delegating password resets

In this video we see how to delegate the ability to perform password resets:
https://youtu.be/1yqf0WJckLY

Delegating Out of Office Administration

In this video we see how to delegate the ability to manage out of office (automatic replies) messages:
https://youtu.be/15Yyua2jfYM

Delegating Management of MFA

In this video we see how to delegate the ability to manage multi factor authentication settings for users:
https://youtu.be/cHL0YOEs944

Exporting and Importing Policies

You carefully fine-tuned an authorization policy or configuration policy. To ensure the policy doesn't become lost or corrupted, you might want to export/save the configuration to a safe location. Keep reading to learn how.

Exporting an authorization policy or configuration policy

Follow the steps below to export a policy file.

1. In Nova, 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**.
4. Click **OK**.

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

Importing an authorization policy or configuration policy

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

1. In Nova, 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.

Jobs Overview

Delegation & Policy Control (DPC) actions are completed via jobs. The Jobs page shows all Nova jobs, in various statuses. You can sort and filter the jobs list. You can add jobs, restart jobs, set priority, and more.
Some jobs need to be performed more than once. For example, you might want the Get Mailboxes job to recur, so it checks regularly to see if new mailboxes are added to your environment. Use the Job Schedules page to schedule recurring jobs, change the frequency at which they occur, and see when a recurring job was last performed.

Overview of Jobs Scheduler

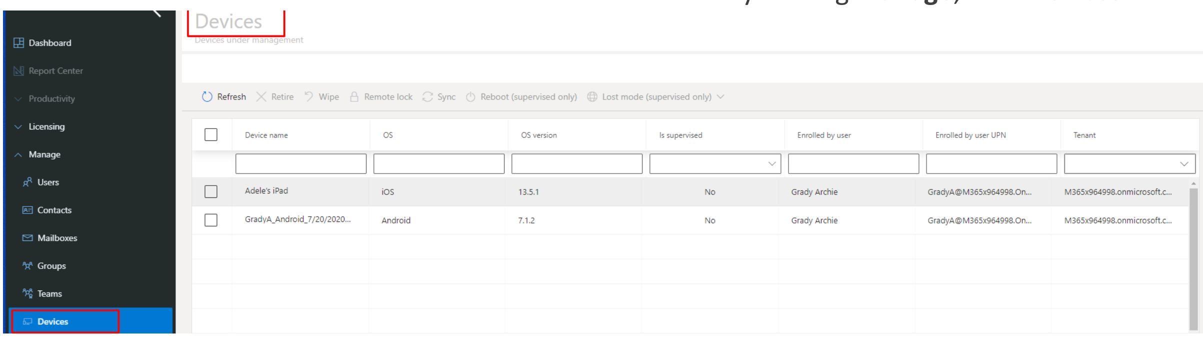
Delegation & Policy Control (DPC) performs several actions from time-to-time, on a schedule. Use the Job Schedule page to review the jobs, create new ones, and edit existing ones. You can sort and filter the jobs list. You can add jobs, run jobs now, and more.

Device Compliance Policies

In Nova DPC, 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, directly in Nova. Actions include:

- Syncing your devices
- Automatically locking them
- Instantly begin the process of wiping your devices
- Retire your devices
- Reboot your devices

The devices screen can be found within the Nova Dashboard by clicking **manage**, then **Devices.**



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

- Detail

- Users
- Group Membership

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

DPC On-Premises Filtering

Issue

One common request we get is how to design DPC policies that apply only to objects that are on-prem, or objects that are in the cloud. For example, I might want a policy to assign all on-prem accounts a particular custom attribute.

Solution

One way is to create a real or virtual organizational unit, or a security group, that contains only the on-prem or cloud users, then use that OU or group as the scope of the policy.
Another is to select either the “Update Cloud User” or “Update On-Prem User” action in the policy. Each of those actions will only target the related user type, so if you have a scope and condition set in the policy that includes both on-prem and cloud users but select the “Update On-Prem User” action, only the on-prem users that the policy matches will be affected.

> **NOTE:** if you create an OU or group for the scope, you still have to select the correct action type. The reason for creating the OU or group is to make clear what the scope is to both human users and auditing software.

DPC IP Addresses

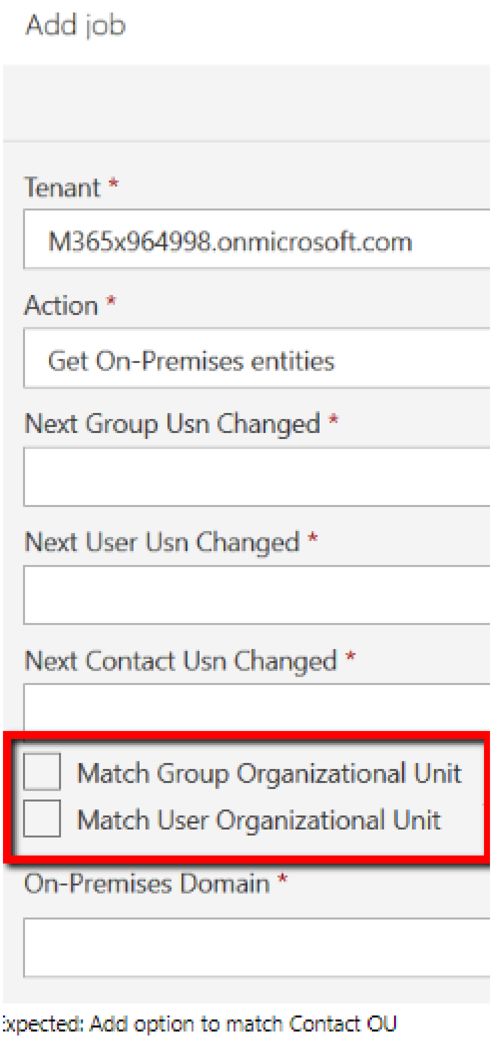
Some companies have Conditional Access requirements, to lock down the service accounts to only be able to access their environment from a whitelisted IP range. You can do the same for the Nova DPC service GA accounts by whitelisting the following IP addresses, dependent on the region your tenant is hosted:
US
40.71.213.40
EU
52.236.178.185

Additional Information About the get on Premises Entities Job Works

In Nova Delegation & Policy Control (DPC) an on-premise agent can be deployed to interact with Active Directory in a hybrid environment. The agent executes a task called ‘Get On-Premises entities’ and this has some important options which should be considered. These options are:

- Match Group Organizational Unit
- Match User Organiational Unit

These are visible on the properties of the job, as shown below:



These check boxes affect the way that objects are placed in the hierarchy. When the options are selected on-premise entities (like users, groups, contacts) from the Users container (in on-premise Active Directory) are placed in the **domain root** else they’re stored in the **tenant root**.

Here is an example to illustrate this:

Tenant1

Domain A
randomOUs1
Domain B
Domain C

Tenant2
Domain D
randomOUs2
Domain E

When ‘tenant 1’ is scanned and the check boxes are deselected – all entities are stored in the ‘Tenant 1’ Organizational Unit.

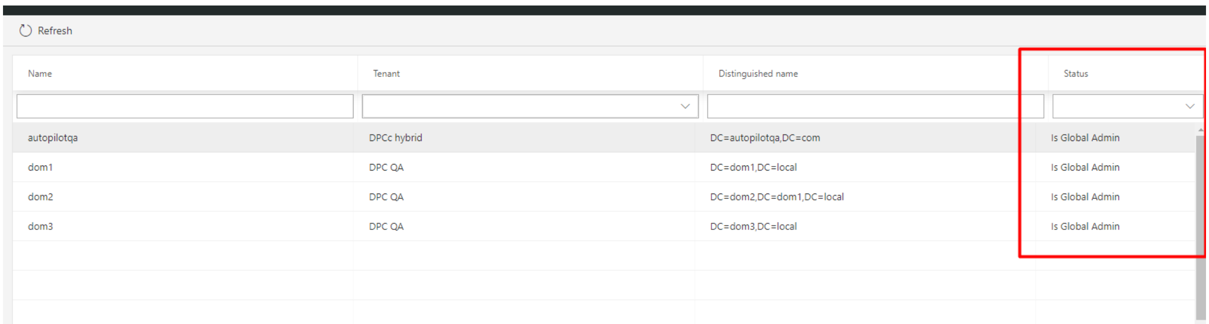
When ‘tenant 1’ is scanned and the check boxes are selected – all entities are stored based on their on-premise location in Domain A, Domain C, root Organizational Units.

Information About On-Premise Domains in Nova Delegation Policy Control

The **On premises domains** page in Nova Delegation & Policy control is accessible to System Administrator role holders and shows key information about domains which the on premises agent has discovered.

This page can be found by going to **Nova > Manage Administration > On Premises Domain.** You’ll need the correct elevated permissions to access this section, including administrator/delegated administrator access.

Here is an example of the page:



Name	Tenant	Distinguished name	Status
autopilotqa	DPCc hybrid	DC=autopilotqa,DC=com	Is Global Admin
dom1	DPC QA	DC=dom1,DC=local	Is Global Admin
dom2	DPC QA	DC=dom2,DC=dom1,DC=local	Is Global Admin
dom3	DPC QA	DC=dom3,DC=local	Is Global Admin

The column at the right hand side of the table indicates the status of the service account associated with the domain. The service account is the one which was used during the agent installation. The valid statuses are:

- Not tested
- Testing in progress
- Failed
- Is Global Admin
- Account is not global admin
- Testing failed
- Unknown

The service account can be manually retested by clicking on the status.

Getting More Detail on Mailbox Data in Nova Delegation and Policy Control (DPC)

In Nova Delegation & Policy Control we provide information which enables a user to review and amend information about users and mailboxes. Since the Office 365 and Azure platforms contain a lot of information only certain information is initially collected in relation to mailbox data. In this article we'll see what is initially collected, and, what additional information can be gathered on-demand.

Initial collection

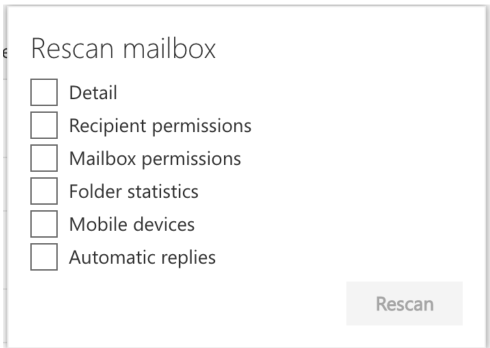
Nova collects information called 'Mailbox detail'. This includes things like:

- Primary SMTP address
- Name
- Forwarding SMTP address
- Type of recipient
- Whether an archive is enabled or not
- Whether mailbox auditing is bypassed or not

Rescan to get more

In the Nova DPC user interface when you have a particular mailbox information shown on the screen, you can perform a 'rescan' in order to get additional information.

The rescan button is over on the right hand side of the header, as shown in the above screenshot. When selected you'll see this pop-up:



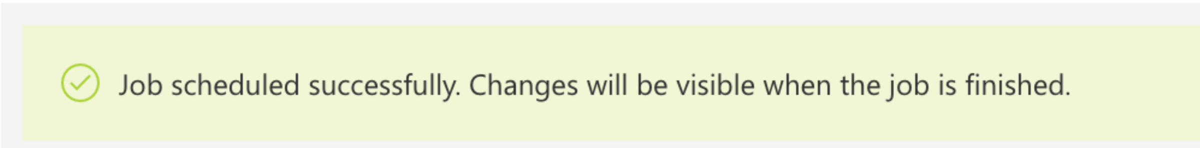
Each of this options (multiple can be selected) will collect additional information as described below:

Detail: Rescan of the basic data such as forwarding information, mailbox type, auditing status, archiving status.

Recipient permissions: Send-As information
Mailbox permissions: Who has Full Access, Read, Delete, Change Permission or Change Owner
Folder Statistics: Gathers folders in a mailbox along with folder size and item count. There is a sub-scan of folder statistics to get folder level permissions.
Mobile devices: Gathers friendly name, number, Operating System, Status and Last Sync information for mobile devices accessing this mailbox
Automatic replies: Gathers out of office information for this mailbox

NOTE: If you wish to obtain send-on-behalf-of permissions, you should scan using the 'Detail' option. In addition in order to see the send-on-behalf-of permissions a delegated administrator will need access to view the mailbox detail information.

When the options have been selected, and the 'Rescan' button clicked, Nova will submit a job to collect the additional data, and will confirm that on the screen:



Setting a Password Using DPC

When setting a password for a new user, or resetting a password for an existing user, ensure that the password meets the requirements of your organization in terms of length and complexity.
If you do not, then the job to set or reset the password will end in an error state.

Re-Authorizing Nova/DPC to Enable End-User Access

Summary

Some tenants need to re-authorize Nova Delegation and Policy Control (DPC) to enable end-users to log in.

Details

A Global Admin must run the following in a **private browser session** to do so:

- https://login.microsoftonline.com/common/adminconsent?client_id=1087d0ea-a372-4968-99a0-19e034bbbc57&redirect_uri=https://null.o365autopilot.com/signin-oidc

This prompts the Global Admin to accept the permissions needed for DPC. After permissions are accepted, end users should be able to access DPC.

NOTE: Since the redirect URI is not an actual address, it causes an error (that can be ignored) after the permissions are accepted.

CAUTION: Be careful to enter the correct credentials in a private browser session. Also, never do this for applications you don't trust.

Virtual Organizational Units

An important feature of Nova is the ability to set up and use virtual organizational units. If you're familiar with on-premises Active Directory, then you'll already be familiar with organizational units. The problem is that Azure Active Directory and Office 365 don't have this concept. The users are stored in a flat list, which can make working with multiple geographies and multiple departments much more difficult. So, in Nova we've re-introduced organizational units. We call them virtual organizational units. You can create a hierarchy of these just like you would in an on premises Active Directory environment.

Creating a Virtual Organizational Unit

Follow the steps below to set up a virtual organizational unit.
Note: Any organizational units set up in Nova are not pulled into Active Directory.

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'll 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.

Note: If you wish to make use of the 'User Assignment Rule' feature, review this article.

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's ellipses button (…) and select Users & Groups to see a list of users and groups that were added to the group within Nova. Note: You can see other objects as well, such as mailboxes and contacts.

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 organizational units until you find the one to which you'll add a new user or group.
3. Click the desired organizational unit's ellipses (…) button and select Users & Groups.
4. Select the checkbox next to the desired user or group and click the Move button.
5. Expand the tree until you find the desired target organizational unit, and then select it and click Save.

Deleting a Virtual Organizational Unit (Moving Assigned Users)

When deleting a virtual organizational unit containing users, those users can be moved to another vOU. Here's 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'll move any users from the deleted vOU, and then click OK to apply the changes.

Video

Here's a video showing the steps above:
https://youtu.be/jOsz2mE16G0

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. In Nova, 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.

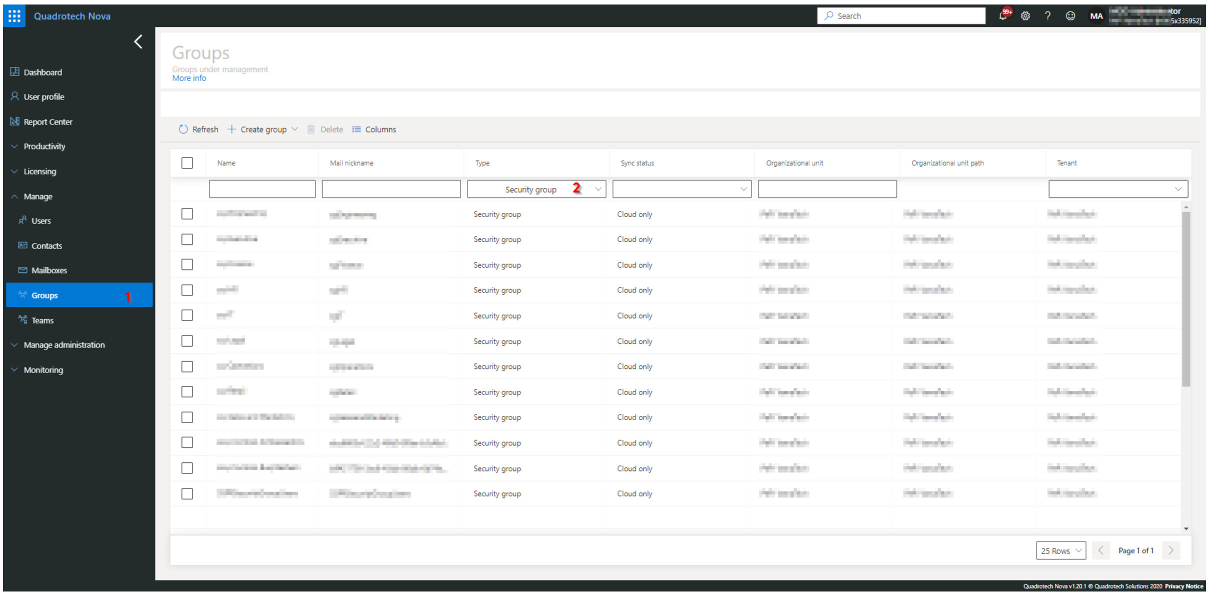
1. In Nova, go to Manage > Teams.
2. Find the desired Teams OU.
3. Click the ellipsis (…) and select Edit.
4. Enter a prefix that will be applied to all groups associated with newly created teams.

How do I take an Action on all Members of an Azure Active Directory Security Group

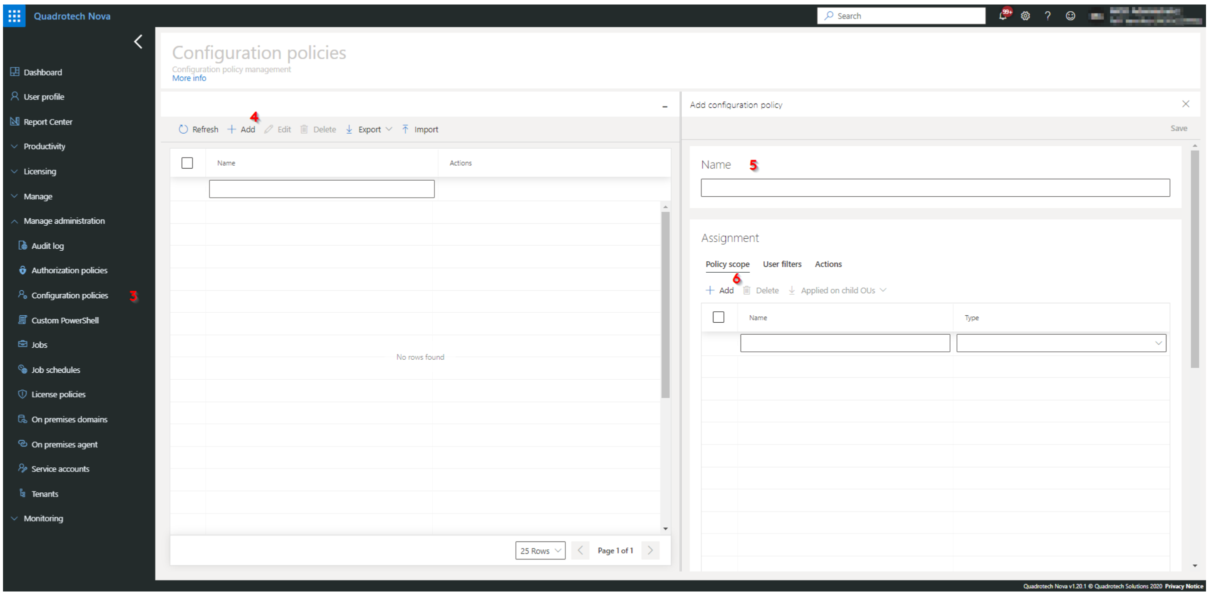
A configuration policy authorizes you to add actions onto groups or virtual organizational units to allow for standardization and consistency throughout your tenant. For example, you can change a users'/groups'/vOUs' Azure Active Directory details, add managers and so on. Look here for more information on configuration policies.

The best protocol in order to apply actions to a Azure Active Directory security group is to create a configuration policy scoped to the target group and **not** add a filter to that group. Let's go through how to do that.

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

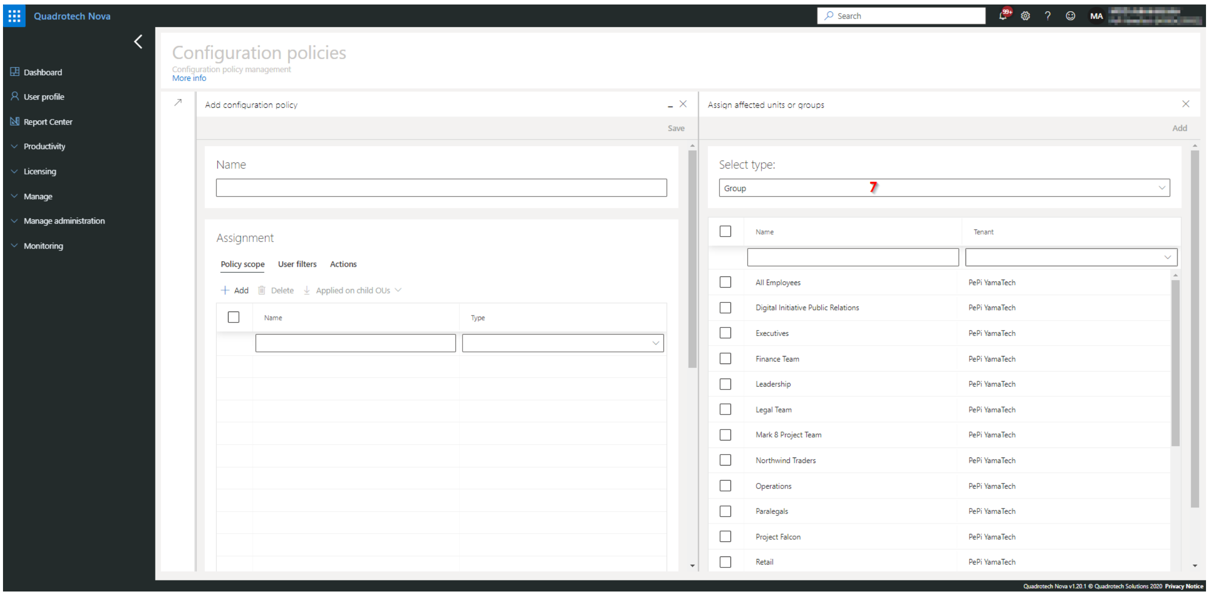


Now create the configuration policy for these groups/vOU. Go to **Manage Administration > Configuration policies,** then click **Add** then add a name to your policy. Then click **Add** on the *Policy Scope* section.



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.



Managing on Premise Active Directory Groups with Nova DPC

Introduction

In a hybrid Office 365 environment where there are still users and groups in a local (on-premise) Active Directory, groups can be added and managed to that local directory. There are some combinations of groups and user objects which aren’t compatible or allowed to be included in groups.

Details

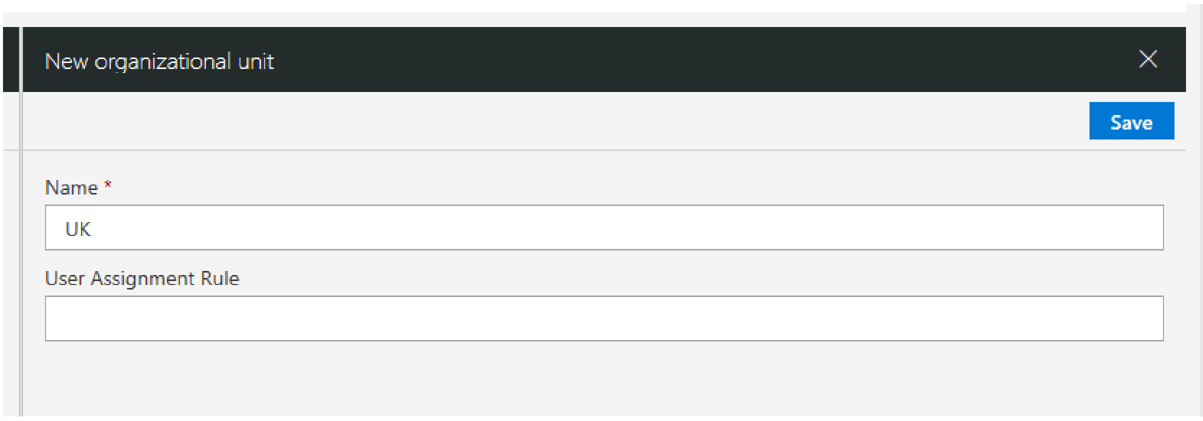
Some objects can not be added as a members to groups, it depends on a property call group scope. If you try to add group with invalid group scope, a job in Nova Delegation & Policy Control is scheduled but it ends with error. The correct / allowed combinations of users and groups is shown below:

The following table summarizes the objects that can be members of each group scope:

Group Scope	Members from the Same Domain	Members from Another Domain in the Same Forest	Members from a Trusted External Domain
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Universal groups Domain local groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups	N/A
Global	Users Computers Global groups	N/A	N/A

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.



Here are some example rules:
User.City = “Zilina”

This assigns users to this OU when the users city is set to Zilina.

User.AccountEnabled = false
This assigns users to this OU when the user account is enabled.

User.City=”Redmond” and User.AccountEnabled = true
This assigns users to this OU when the city is set to Redmond, and the account is enabled.
If you need further assistance in developing a rule to suit your business needs, reach out to our customer experience team.

4

Licensing

The Licenses page shows information about licenses in tenants that you can access. On this page you can:

- View license information on the current or other accessible tenants
- View how those licenses are assigned
- Depending on license policies, you can assign licenses to users

Overview of Data Sources in Nova

Nova gives you the potential to review data from many different data sources, and to combine them into reports. In the user interface, the individual data sources are organized into these groups:

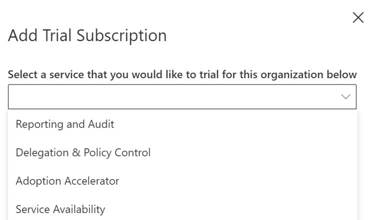
Data Source Category	**Description**
Adoption Accelerator	This includes data related to Nova Adoption Accelerator campaigns.
Alert Data	
Audit Data	This is audit data relating to Office 365.
Beacon Data	
Beacon Log Data	
Exchange Data	This is data relating to your Exchange environment, including data sources for Mailboxes and user activity.
License Data	This is data for your license management in your environment.
Mobile Data	This includes data for mobile usage, including devices used by your users and applications downloaded.
Office 365 Data	This is data in relation to your Office 365 environment, including Azure groups and members, as well as subscriptions.
OneDrive Data	This is data about your OneDrive environment.
Organization Data	
Other	This includes data about licenses and the System Lookup Service Status.
SharePoint Data	This is data about your SharePoint environment.
Skype For Business Data	This is data about your Skype for Business environment.
Teams Data	This is data about your Teams environment.
Test Result Log Data	

Workload Data	
Workload Log Data	
Yammer Data	This is data about your Yammer environment.
User Data	This includes Office 365 user-related data. For example, display names, job titles, location, etc. Here's an example of a report containing Office 365 user data.

Click here for more information.

License Types

In Nova 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

Service Availability

This gives access to the service health dashboard with Nova.

Adoption Accelerator

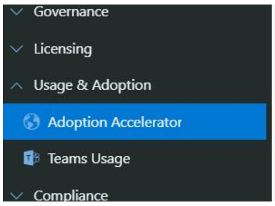
This gives access to the Adoption Accelerator features with Nova. It allows campaigns to be created and monitored whilst they are in progress.

Reporting and Audit

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

Example of License

As an example, if the Adoption Accelerator license is added, then users of Nova will see the following (provided they have been granted access, and the correct roles assigned):



Service Monitoring

Many organizations move their on premises services to the cloud in hopes of getting better service than they have—better up-time, security, resiliency, data protection, etc. Nova Service Health provides Office 365 workload availability monitoring that helps an organization see whether Office 365 is as reliable as the organization hoped. This is achieved through:

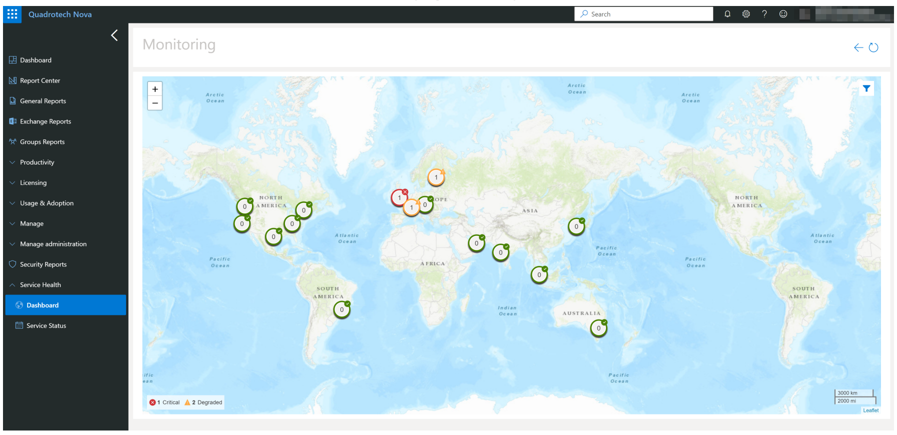
- Performance monitoring
- Outage location tracking
- Workload availability monitoring
- SLA reporting

This information is invaluable when troubleshooting Office 365-related problems. The service gives an organization quick answers to questions like:

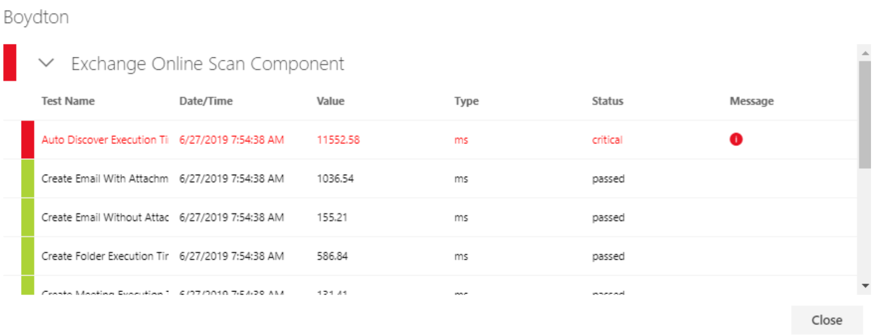
- **Is the service available?** Nova Service Health offers global awareness of Office 365 service status.
- **Is it performing like it should?** Find answers in SLA planned-versus-actual reporting.
- **Can a certain user *use* the service?** Helpdesk troubleshooting is easier with per-user visibility.
- **Are there any problems with the service that might affect my users?** Check per-location statuses to find out.

Nova Service Health gives you access to historical and real-time monitoring data, so you can see what's broken now, what was broken in the past (including when it broke and when it started working again), and a historical record of latency, uptime, etc. This allows you to make data-driven decisions.

You can monitor service availability globally:



Or, focus on a specific location:



Here's a video with more information about Nova Service Health:
https://youtu.be/3k0hyf_kwFg

What does it monitor?
Microsoft data centers are automatically monitored for Office 365 workload availability, outages, performance, etc.
Besides monitoring those data centers, Nova Service Health can be configured to track availability and performance of other services, as well.
For example, if you have a lot of users in a certain location, let's say Toronto, you could install a beacon on a virtual machine in Toronto. Then, Nova Service Health reaches out to a mailbox that you configure and tests the availability/performance.
In this example, it'll test the connection from Toronto to the data center where the mailbox exists

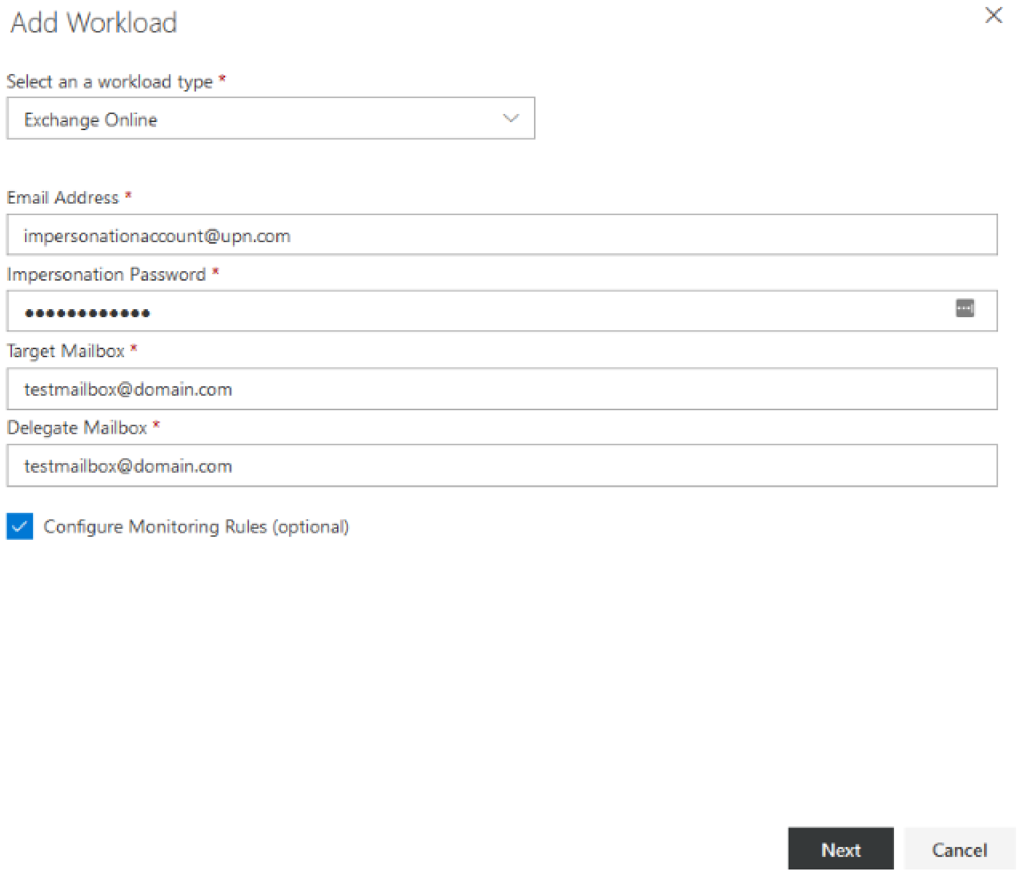
Adding a Service Monitoring Beacon

NOTE: The beacon requires .Net Framework 4.7.2.

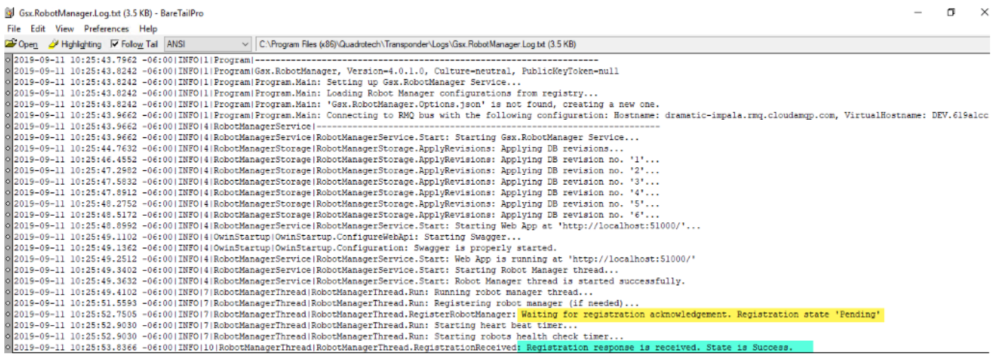
Follow the steps below to install your own beacons that will be monitored using Nova Service Health.

1. Log in to Nova.
2. Click the **Settings button** (a gear icon) located in the top right of the page.
3. Click **Monitoring,** which is located under Application Settings.
4. Select **Beacon Management**.
5. Click **Add** > **Beacon.**
6. Enter an email address, and then click **Send.** An email containing an installation code and a link to download the installer will be sent to the email address.
7. From the email, download the installer to your Windows server.
8. Run the installer. When prompted, enter the installation code from the email.
9. Review the logs to ensure the beacon was registered successfully.

10. In Nova, go back to **Settings** (using the gear icon) > **Monitoring** and add any desired workloads (by clicking **Beacon Management** > **Add** > **Workload).**

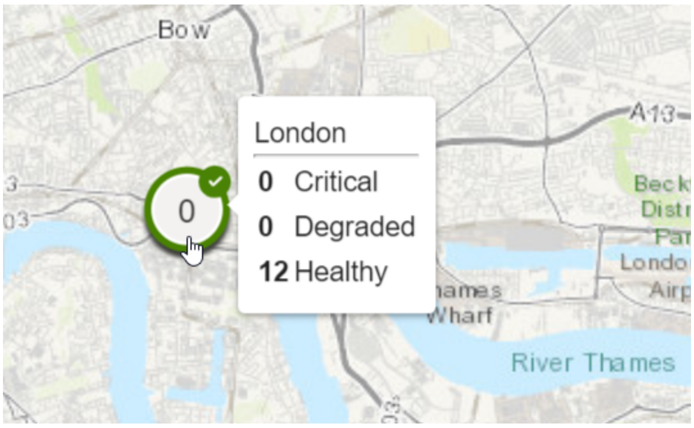


11. When registration is successful, you'll be able to see an entry in the logs indicating registration was successful. Here's how it looks:



Note

Until you add workloads to your beacon, the beacon icon on the Monitoring dashboard shows the NoData icon. After you add workloads to the beacon, you'll see test results in the dialog after 1 minute:

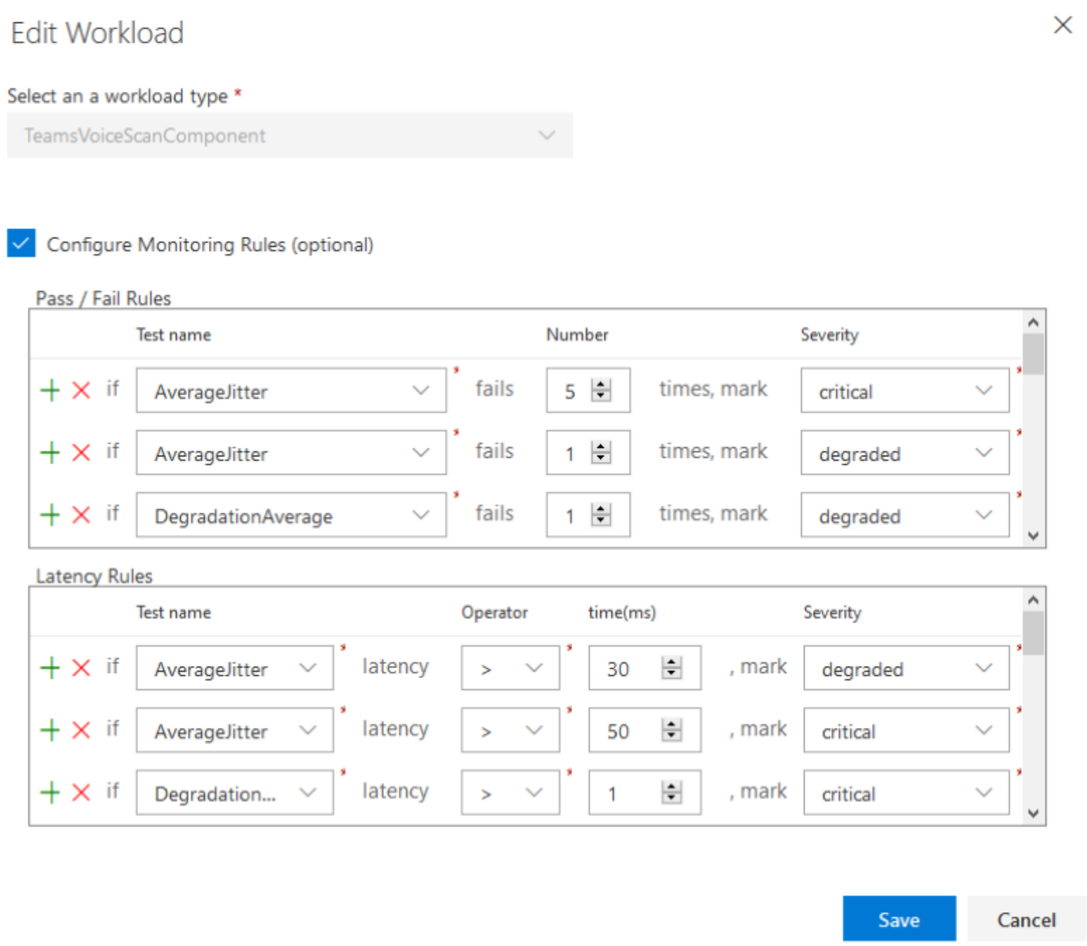


By default, a scan of the workloads occurs every 60 seconds. However, the status on the dashboard map only changes if the beacon status has changed since the last scan.

Editing a Workload

You can change monitoring rules (pass/fail and latency) by editing the beacon's workload:

1. Click the **Settings button** (a gear icon) located in the top right of the page.
2. Click **Monitoring,** which is located under Application Settings.
3. Select **Beacon Management**.
4. Select **Edit** > **Workload.**
5. Click the ellipsis button (…) and select **Edit.**
6. Make desired changes (using the screen shown below), and then click **Save.**



Stopping a Workload

You can stop a workload to stop future scanning.

1. Click the **Settings button** (a gear icon) located in the top right of the page.
2. Click **Monitoring,** which is located under Application Settings.
3. Select **Beacon Management**.
4. Select **Edit** > **Workload.**
5. Click the ellipsis button (…) and select **Stop.**

After a workload is stopped for about 5 minutes, the old test results are removed and the workload status changes to Critical. The beacon status changes to NoData.

Removing a Workload

Removing a workload removes it from the server running the beacon. Here's how to do it:

1. Click the **Settings button** (a gear icon) located in the top right of the page.
2. Click **Monitoring,** which is located under Application Settings.
3. Select **Beacon Management**.
4. Select **Edit** > **Workload.**
5. Click the ellipsis button (…) and select **Remove.**

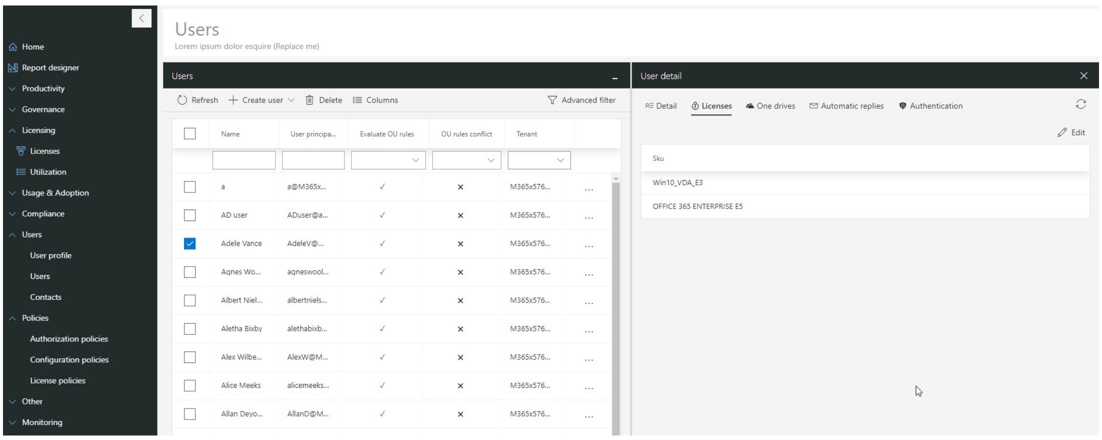
User License Changes Delayed

Summary

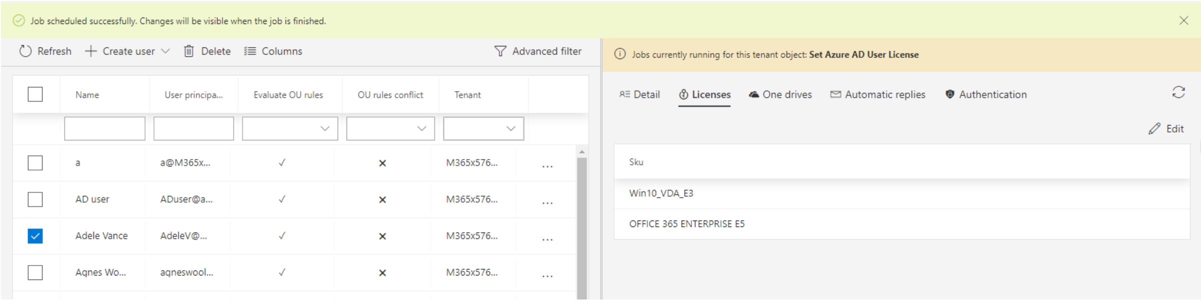
After you update a user's license, you might notice the change isn't immediately visible in the user interface. This article explains why, after you make user license changes, there is a delay in the **User details** > **Licenses** list being updated to reflect the changes.

Details

You selected a user and you're editing their license(s) using the **Users detail** > **Licenses** screen (shown below).



You made changes to the user's licenses, assigning/removing licenses. A notification displays (shown below), telling you the Set Azure AD User License job is running.



The notification disappears when the job is complete. This happens in real time without any need to refresh the screen. However, you notice even after the notification closes, your changes are not visible in the **Licenses** list.

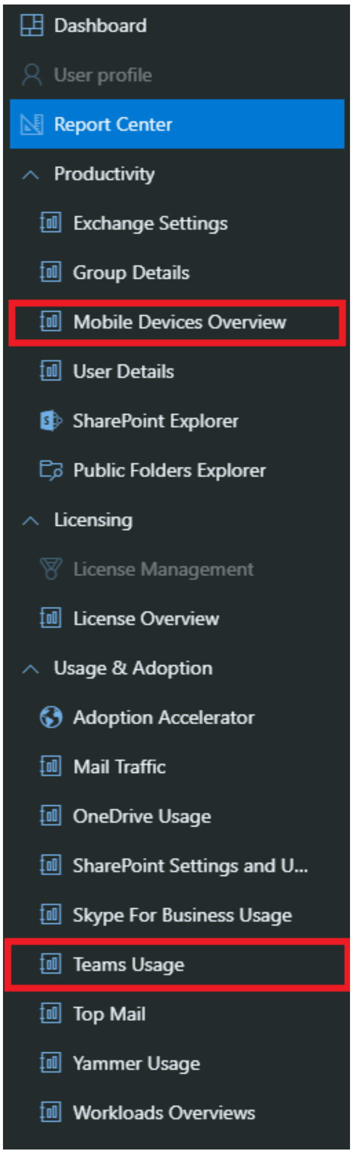
Explanation

The change is not visible in the **Licenses** list right away when the Set Azure AD User License job is completed since the webhook needs to detect the change, which then triggers the Get Tenant User job. Once both jobs (Set Azure AD User License and Get Tenant User) are complete, then the change displays in the user interface–no refresh needed.

5

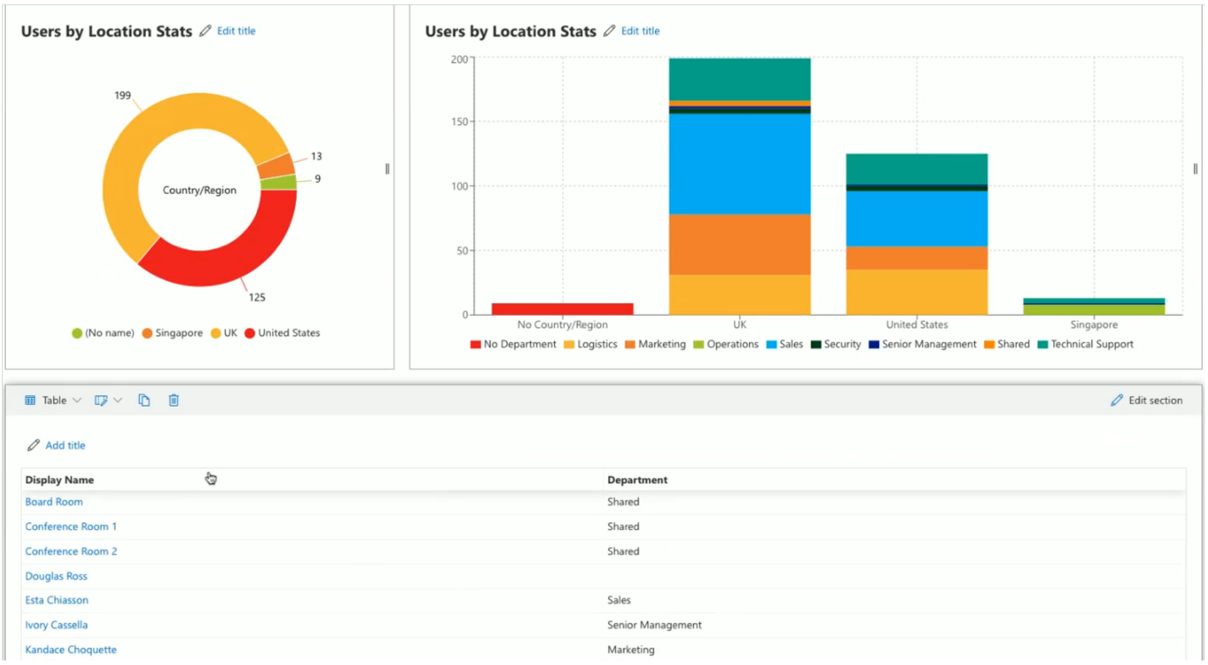
Reporting

You’ll find Nova built-in reports right where you need them. You’ll 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’s how it looks:



The highlighted boxes show reports

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:



Display Name	Department
Board Room	Shared
Conference Room 1	Shared
Conference Room 2	Shared
Douglas Ross	
Esta Chiasson	Sales
Ivory Cassella	Senior Management
Kandace Choquette	Marketing

Reports can be delivered by email, as well, 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.

Configuring Reporting for SharePoint Online Reports

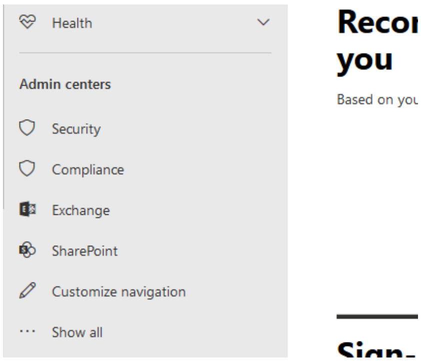
Overview

This article will explain the process you will need to follow in order to setup Nova/Radar for SharePoint Online reports. The process will take you through granting the existing Nova/Radar Reporting service account permissions to read SharePoint data and setting up the Site Collection reports with the Nova/Radar application.

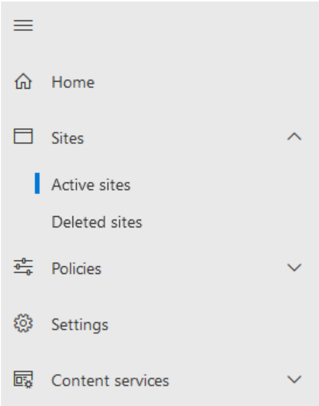
Granting Access to the Nova Reporting Service Account

1. Log into the Office 365 Portal

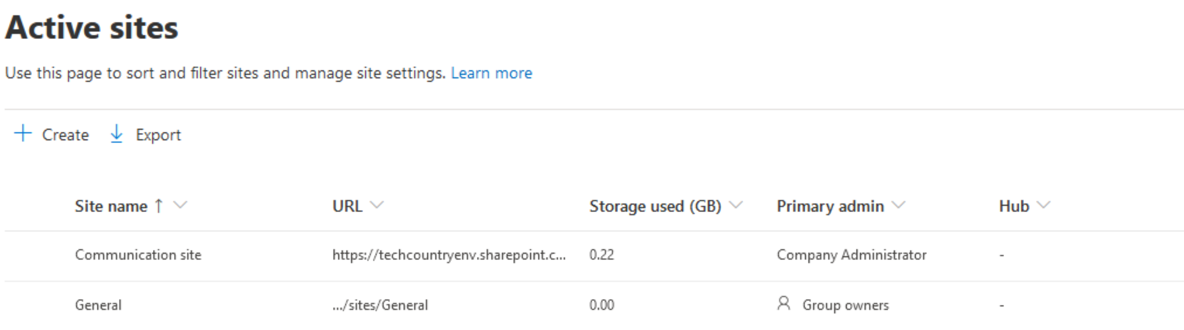
2. In the navigation pane on the left, Under **Admin centers,** select **SharePoint.** This will take you to the SharePoint admin centers in a new window.

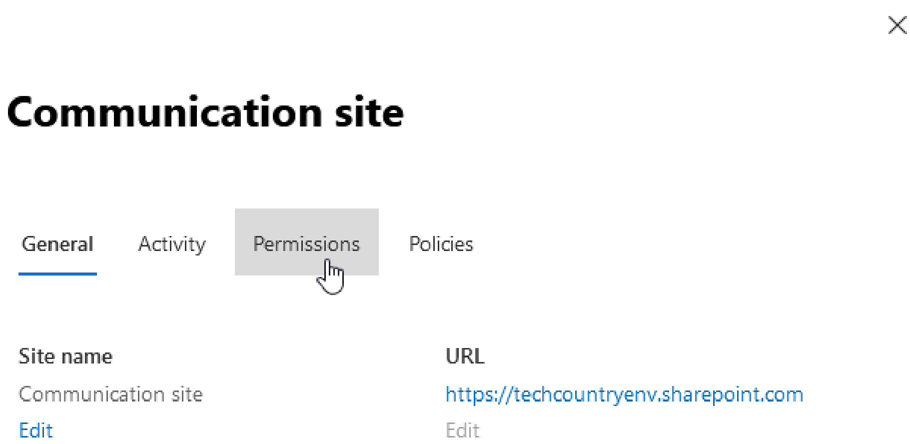


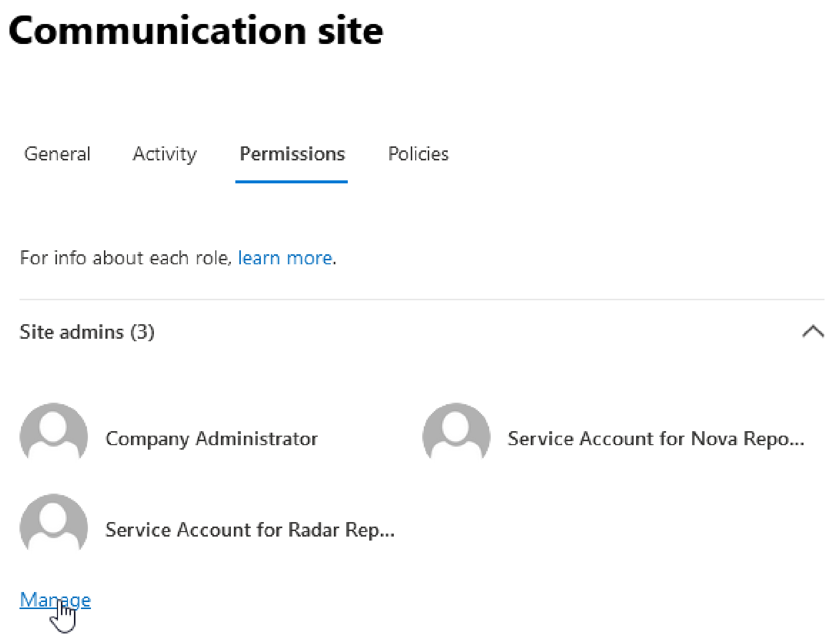
3. In the Admin center, Click on **Sites** and select the Active sites button:



4. An Active site need to be selected from the list in order to display the Information Blade. Once site you would like to add into Radar/Nova for Office 365 Reports is selected, choose **Permissions** and then **Manage**.

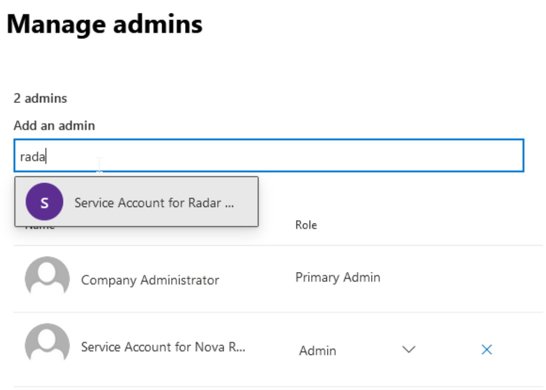






5. A new blade window will come up with two options. In the search box search for the name of the Radar/Nova Reporting service account you used when you initially signed up for Reporting, add the account and click on save.

NOTE: If when you signed up you chose ‘Automatic Signup’ then the service account will be called ‘RadarReporting’



6. The permissions should now be applied to the service account.

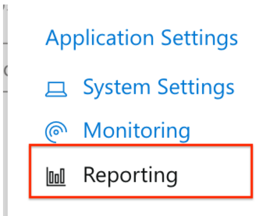
NOTE: Sometimes issues in the back-end replication can lead to this not always being the case. To confirm that all has been applied correctly on Microsoft’s servers, navigate to your site collection’s Administrator Management page. The service account should be listed in the box with the other admins.

More information could be found in Microsoft document.

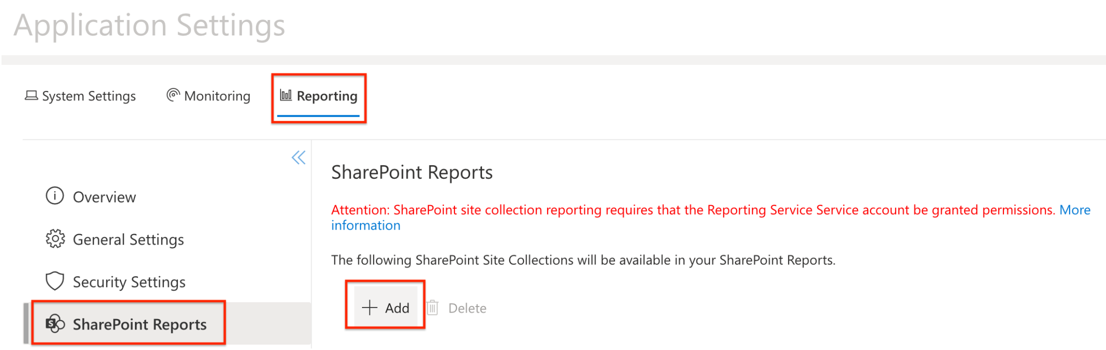
Adding In your Site Collection in Nova

1. Log into Nova and select Radar Classic or System Administrator role and go to **Setting** (cog icon in top right corner)

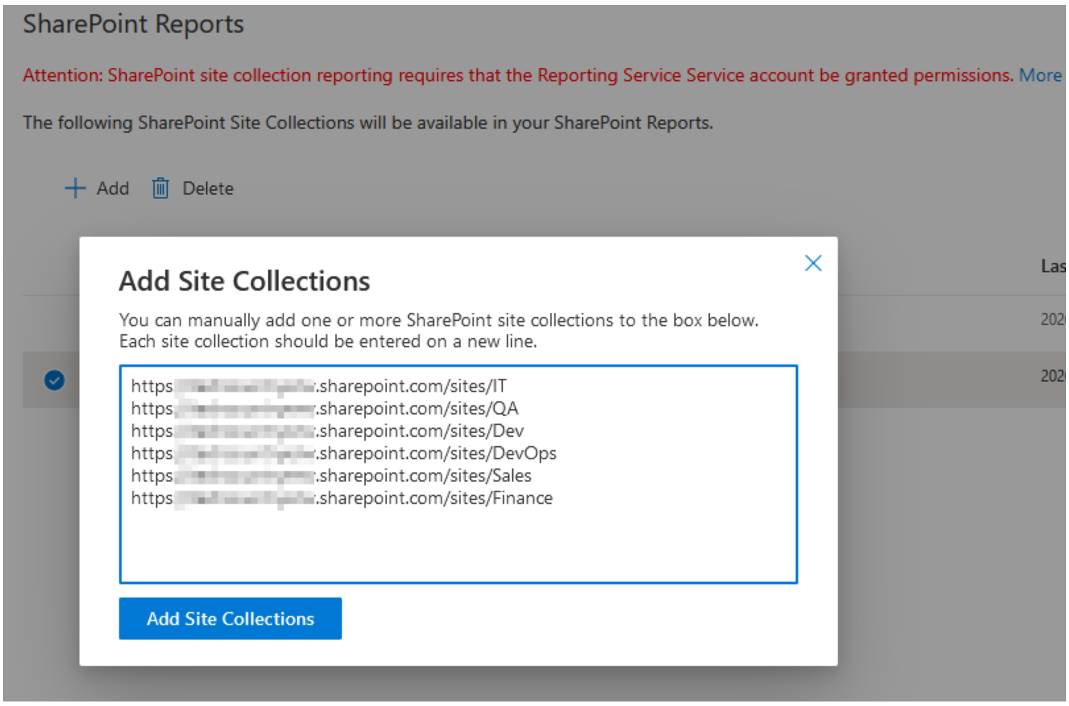
2. From opened menu select **Reporting** from **Application Settings** section



3. Select **SharePoints Reports** and add Site Collection you granted access in steps above with **+Add** button



4. You can add one or multiple Site Collections. If the rights are granted correctly the status will change from **Pending** to **Verified** after next collection



The following SharePoint Site Collections will be available in your SharePoint Reports.

+ Add   Delete

Site Collection	Last Updated	Status ↓
https[redacted]sharepoint.com	2020-10-18 22:33:11	Verified
https[redacted]sharepoint.com/portals/community	2020-10-18 22:14:06	Verified

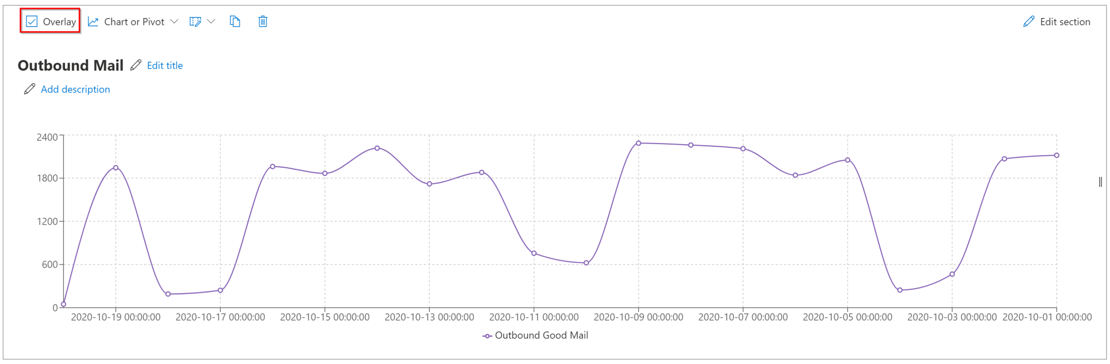
Combine Multiple Charts

Combining multiple charts in Nova Report Center 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:

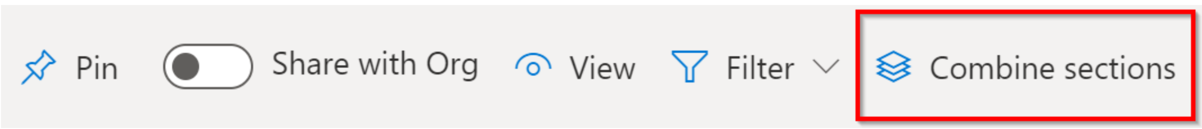
- The charts you would like to combine must be the same chart type e.g. bar, line, column. You are unable to combine pie charts.
- The axis types must be the same. This is your *applied to* and *series name* categories when creating your chart.

To combine your charts:

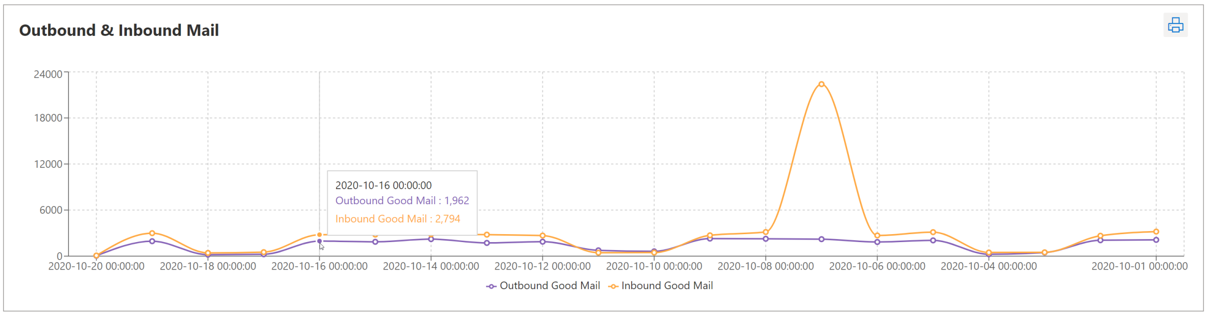
1. Create your chart. Remember that only bar, column and line graphs can be used for combining. To see how to create a chart, check out this article.
2. Click the **Overlay** checkbox to select the charts you would like to combine.



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't do so when your charts are combined.

Subscription Overview

The subscriptions overview page in the Nova user interface 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.

Subscription Overview

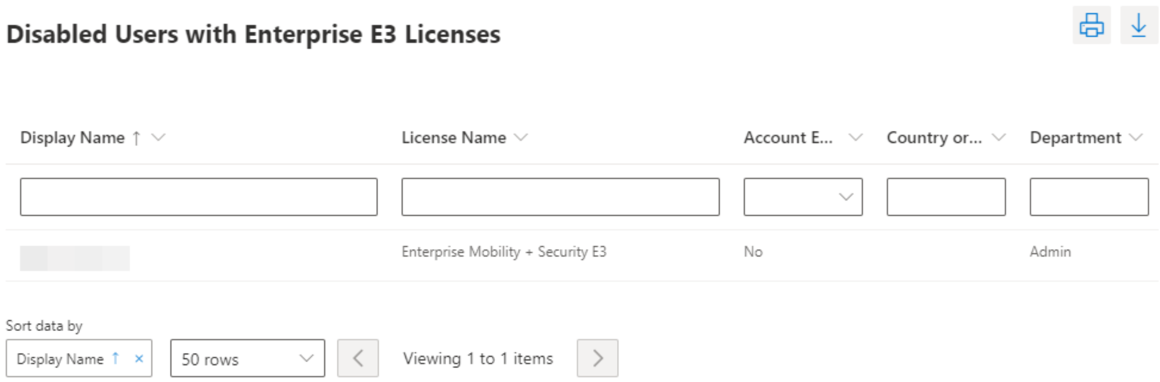
This report provides you with an overview of your Office 365 Subscriptions

Organization	License Sku Name	Percent Used	Total Licenses	Assigned Lice...	Unassigned Li...	Idle Licenses	Price / Unit / Month
Filter Organizations	Filter License Sku Name	Filter Percent Used	Filter Total Licen...	Filter Assign...	Filter Unassi...	Filter Idle Lic...	Filter Price
quadrotech.onmicrosoft.com	Enterprise Mobility + Security E3	74.5%	200	149	51	52	$8.80
quadrotech.onmicrosoft.com	Office 365 E5 Without Audio Conferencing	100%	150	150	0	0	$24.00
quadrotech.onmicrosoft.com	Audio Conferencing	94.4%	125	118	7	7	$4.00
quadrotech.onmicrosoft.com	Visio Online Plan 2	90.91%	11	10	1	1	$18.00
quadrotech.onmicrosoft.com	Power Bi Pro	5%	100	5	95	95	$9.99
quadrotech.onmicrosoft.com	MCOPSTN_5	100%	22	22	0	0	$0.00
quadrotech.onmicrosoft.com	Exchange Online (Plan 1)	100%	10	10	0	1	$4.00
quadrotech.onmicrosoft.com	Azure Active Directory Premium P2	100%	1	1	0	0	$9.00
quadrotech.onmicrosoft.com	Power BI for Office 365 Standard	1.5%	200	3	197	197	$0.00
quadrotech.onmicrosoft.com	MCOPSTNC	0%	10000000	33	9999967	9999967	$0.00

If the scope of your Nova access includes multiple tenants, you can filter and show just a subset, or one, tenant. Up to 20 tenants can be selected in that filter.
The price associated with each license can be changed by clicking on it in the user interface.

Reclaim and Redistribute Licenses From Disabled Users

As a license manager, you want to have maximum use of your purchased licenses. You don't want to see them assigned to users which, for example, may no longer be affiliated with your company.
You can reclaim licenses from disabled users after 14 days from their last previous activity. This report gives you an insight into which licenses are assigned to disabled users, so you can remove them and assign them to users who may need them.
If you are a Nova subscriber, you can find this System report in the Report Center, titled **'List Disabled Users With Assigned Licenses'**.

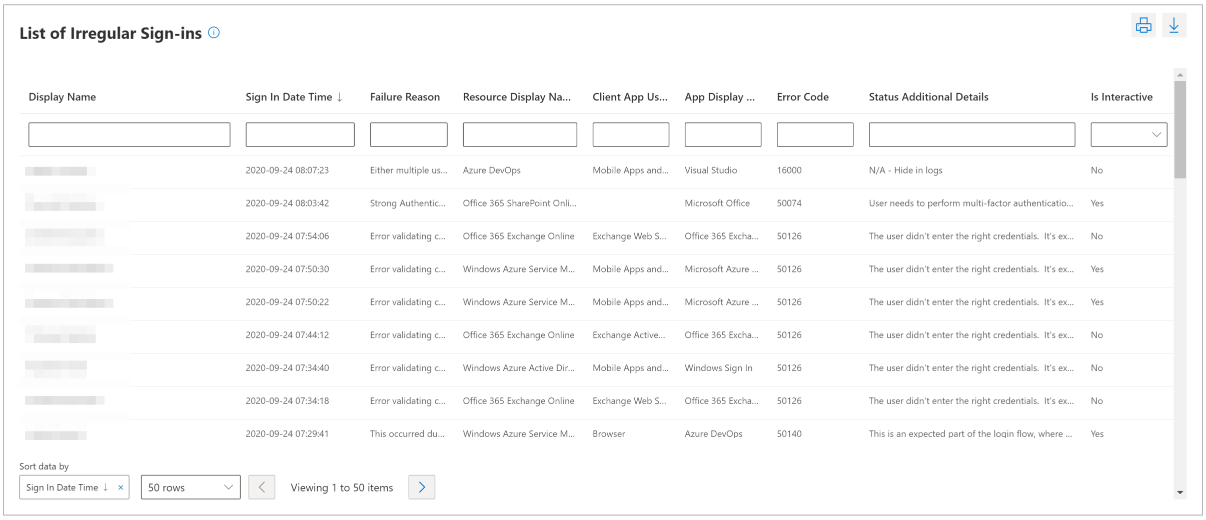


NOTE: If you are curious about accounts before your previousing of Nova, these accounts will be shown as disabled, but the activity date will be empty. This is because Nova hadn't began to ingest audit events prior to its provision date.

Irregular Sign In Activity in Nova Report Center

The Irregular Sign-Ins system report in the Nova Report Center allows you to see sign-in attempts from users both external and internal to your environment. This includes multiple sign in attempts and locking of accounts.
The table includes information that drills down into the details of the sign-in, including:

- Name
- Time and date
- Workload
- Application used (Internet browser/EWS etc.)
- Error code
- Additional status information – examples include login credential errors or if the log was an expected part of the login flow.



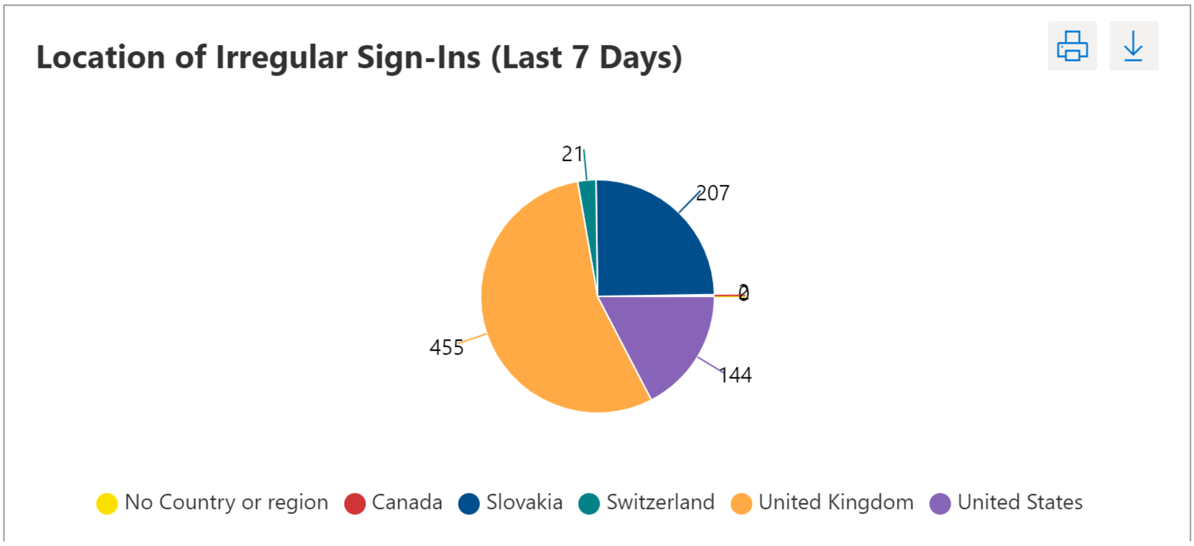
List of Irregular Sign-ins

Display Name	Sign In Date Time ↓	Failure Reason	Resource Display Na...	Client App Us...	App Display ...	Error Code	Status Additional Details	Is Interactive
	2020-09-24 08:07:23	Either multiple us...	Azure DevOps	Mobile Apps and...	Visual Studio	16000	N/A - Hide in logs	No
	2020-09-24 08:03:42	Strong Authentic...	Office 365 SharePoint Onli...		Microsoft Office	50074	User needs to perform multi-factor authenticatio...	Yes
	2020-09-24 07:54:06	Error validating c...	Office 365 Exchange Online	Exchange Web S...	Office 365 Excha...	50126	The user didn't enter the right credentials. It's ex...	No
	2020-09-24 07:50:30	Error validating c...	Windows Azure Service M...	Mobile Apps and...	Microsoft Azure ...	50126	The user didn't enter the right credentials. It's ex...	Yes
	2020-09-24 07:50:22	Error validating c...	Windows Azure Service M...	Mobile Apps and...	Microsoft Azure ...	50126	The user didn't enter the right credentials. It's ex...	Yes
	2020-09-24 07:44:12	Error validating c...	Office 365 Exchange Online	Exchange Active...	Office 365 Excha...	50126	The user didn't enter the right credentials. It's ex...	No
	2020-09-24 07:34:40	Error validating c...	Windows Azure Active Dir...	Mobile Apps and...	Windows Sign In	50126	The user didn't enter the right credentials. It's ex...	No
	2020-09-24 07:34:18	Error validating c...	Office 365 Exchange Online	Exchange Web S...	Office 365 Excha...	50126	The user didn't enter the right credentials. It's ex...	No
	2020-09-24 07:29:41	This occurred du...	Windows Azure Service M...	Browser	Azure DevOps	50140	This is an expected part of the login flow, where ...	Yes

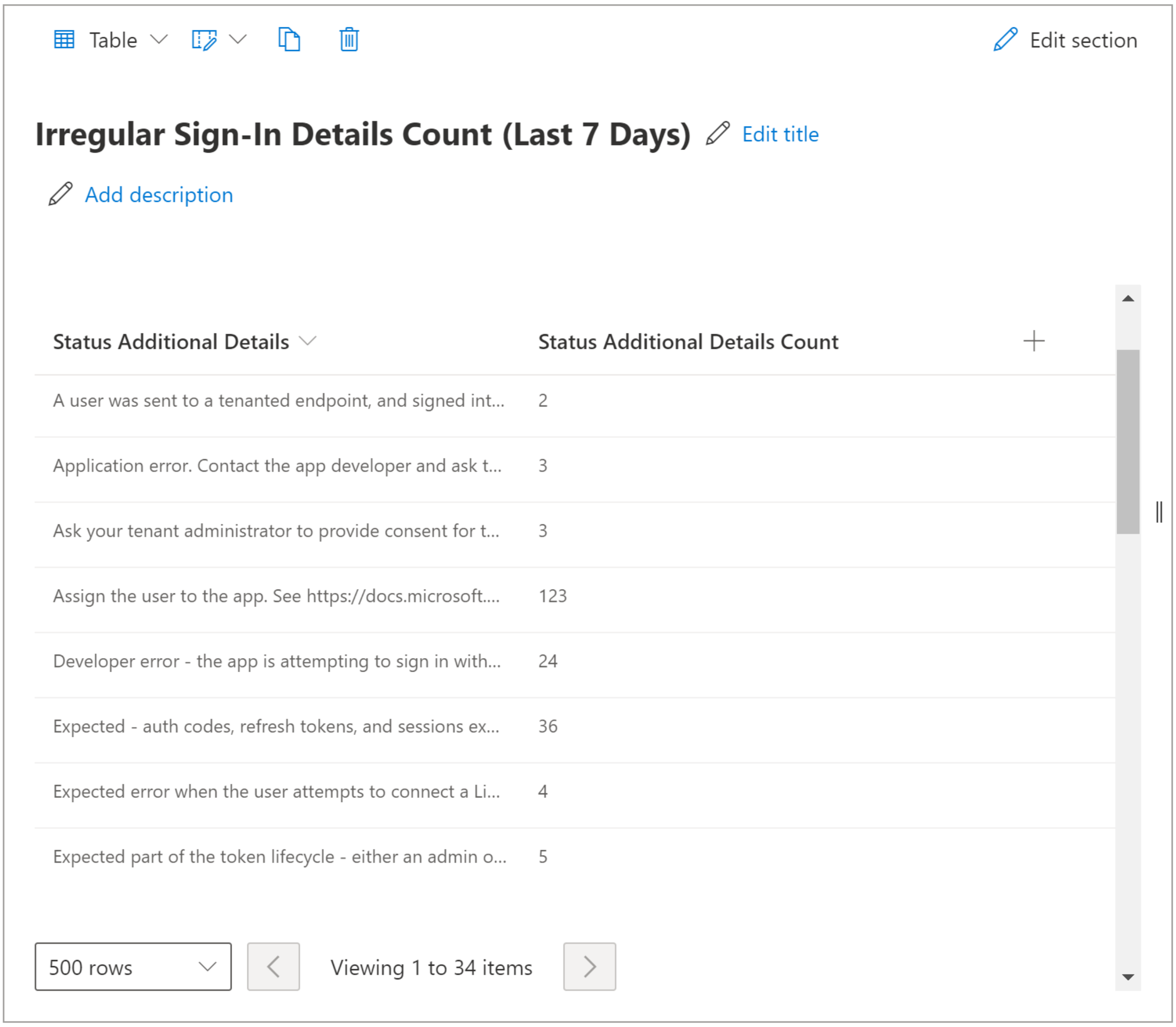
Sort data by

Sign In Date Time ↓ × | 50 rows | Viewing 1 to 50 items

Another section of the report gives you a pie chart on where the sign-ins have occurred by country. This is useful to quickly identify if sign-ins have happened in locations where your organization and its users aren't affiliated.



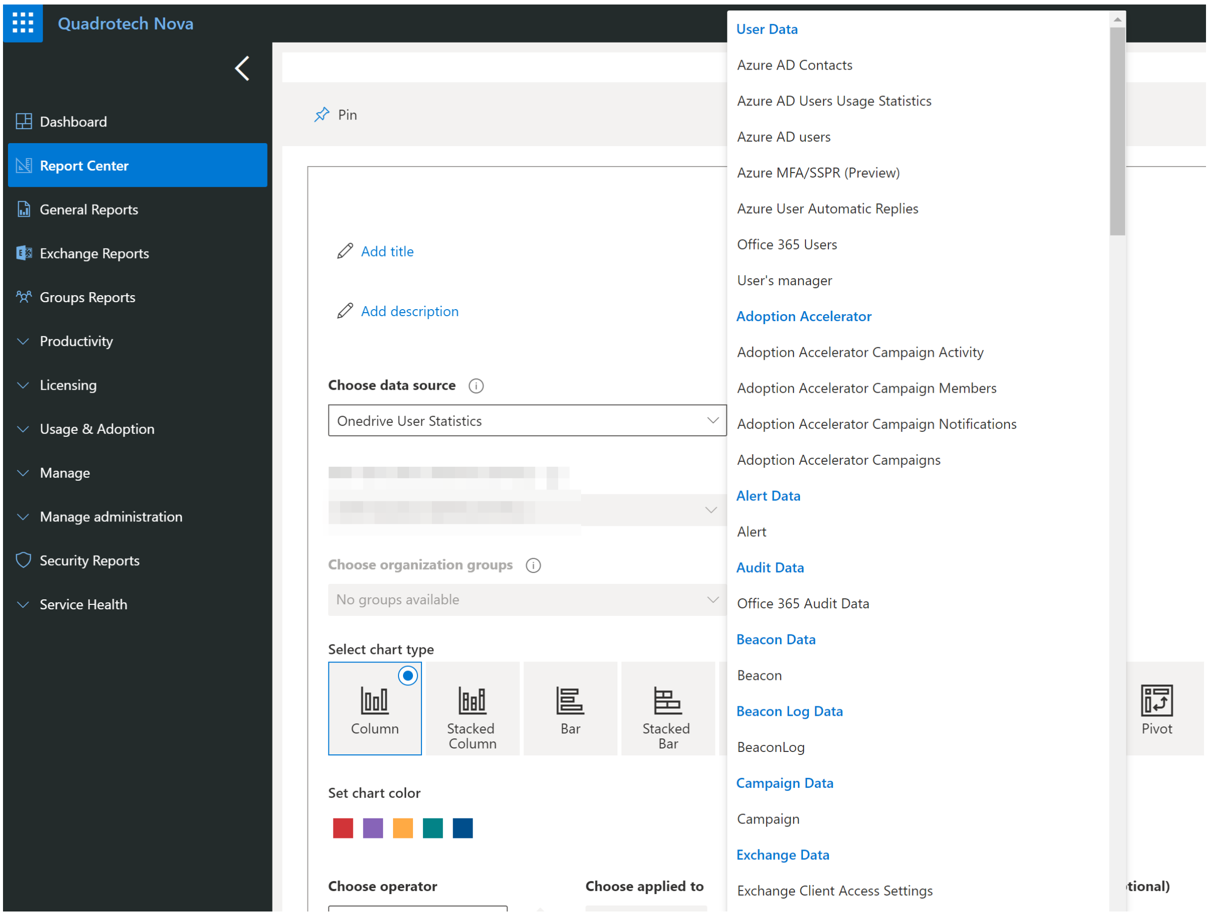
The final section gives you information on the main failure types and how often they occured over the previous seven days.



Remember, you can modify these system reports and tweak them to suit your needs. To do this, you will need to clone your report by clicking **Edit**, then **clone**. These will then be made private reports and only available to you.

Data Sources

Reports built using the Nova Report Builder contain information from from various data sources. For example, reports might contain data related to Microsoft Teams, Yammer, Skype, and more. Additional data sources will be added over time.
A data source is a specific subset of data fields that are collected into a grouping for report creation. Here’s an example. In the menu, data source categories are shown in blue and the actual data sources are shown in black.



As you see in the image above, data sources are separated into categories. Here's more about each category:

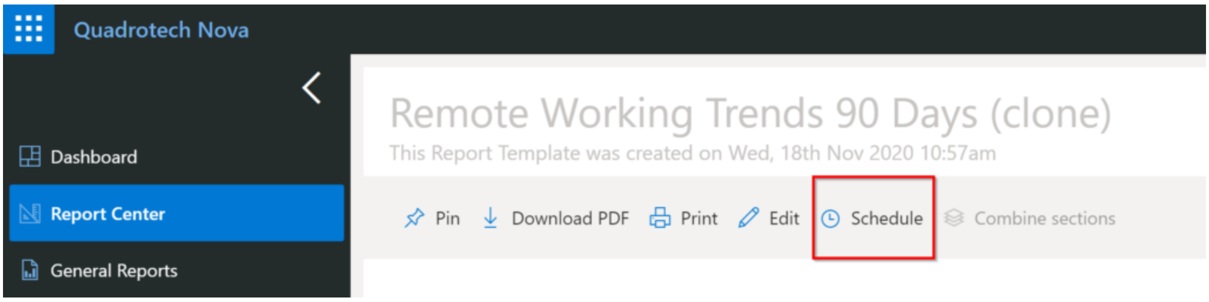
Data Source Category	Description
Adoption Accelerator	This includes data related to Nova Adoption Accelerator campaigns.
Alert Data	
Audit Data	This is audit data relating to Office 365.
Beacon Data	
Beacon Log Data	
Exchange Data	This is data relating to your Exchange environment, including data sources for Mailboxes and user activity.
License Data	This is data for your license management in your environment.
Mobile Data	This includes data for mobile usage, including devices used by your users and applications downloaded.

Office 365 Data	This is data in relation to your Office 365 environment, including Azure groups and members, as well as subscriptions.
OneDrive Data	This is data about your OneDrive environment.
Organization Data	
Other	This includes data about licenses and the System Lookup Service Status.
SharePoint Data	This is data about your SharePoint environment.
Skype For Business Data	This is data about your Skype for Business environment.
Teams Data	This is data about your Teams environment.
Test Result Log Data	
Workload Data	
Workload Log Data	
Yammer Data	This is data about your Yammer environment.
User Data	This includes Office 365 user-related data. For example, display names, job titles, location, etc. Here's an example of a report containing Office 365 user data.

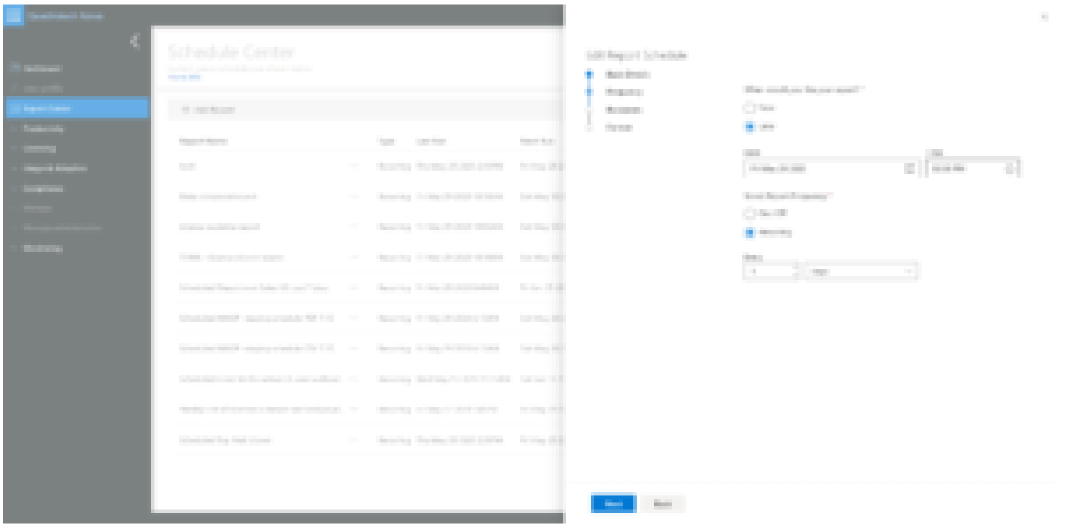
Report Examples
To see reports using these data sources, click here.

Scheduling Reports

You can schedule a report to be generated and emailed to a certain person or group.



You can send a report one time, daily, weekly, or monthly.



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 Office 365 licenses are being used and are available across the organization.

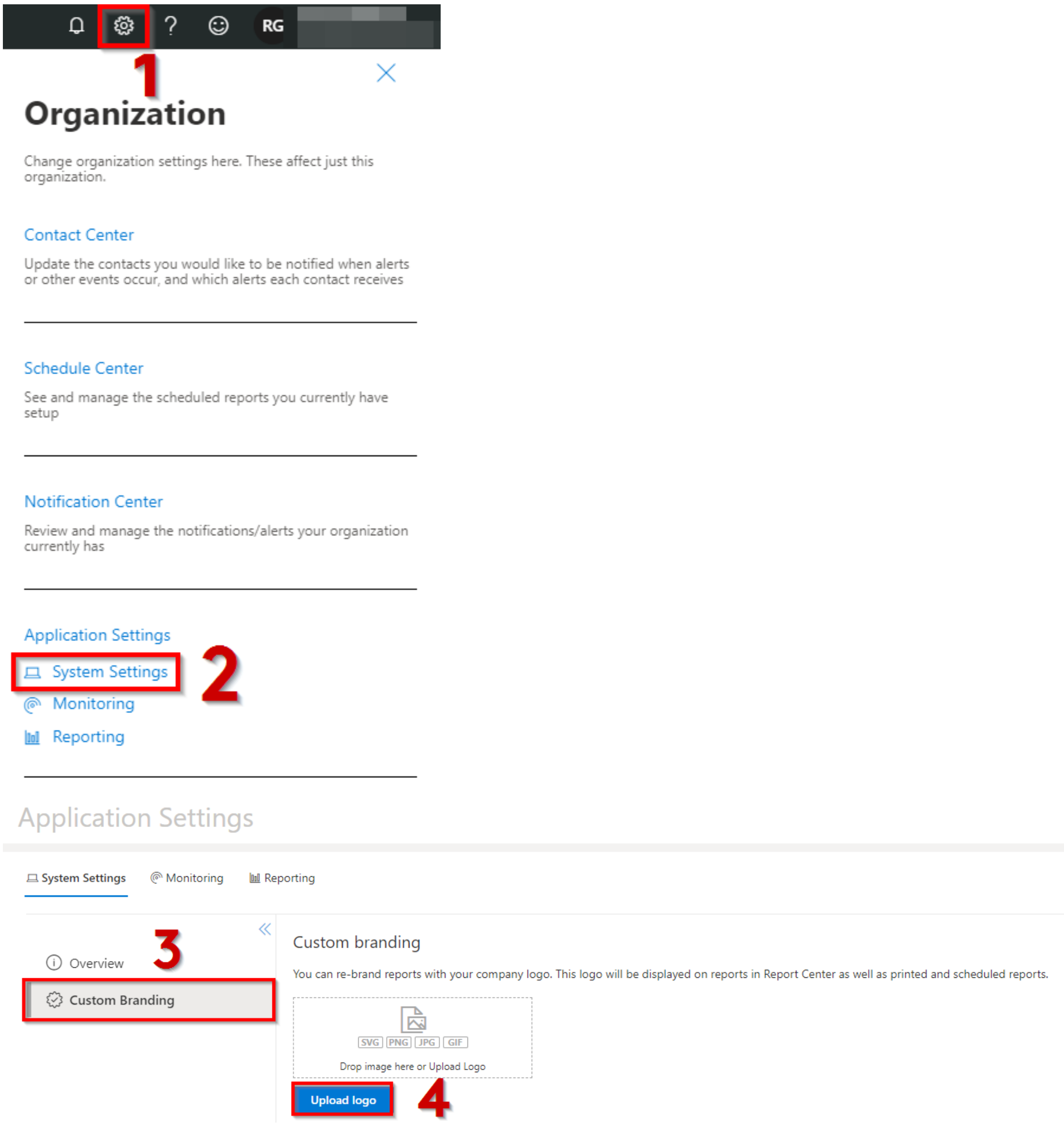
More on the schedule center can be found here.

Add a Logo to Your Report

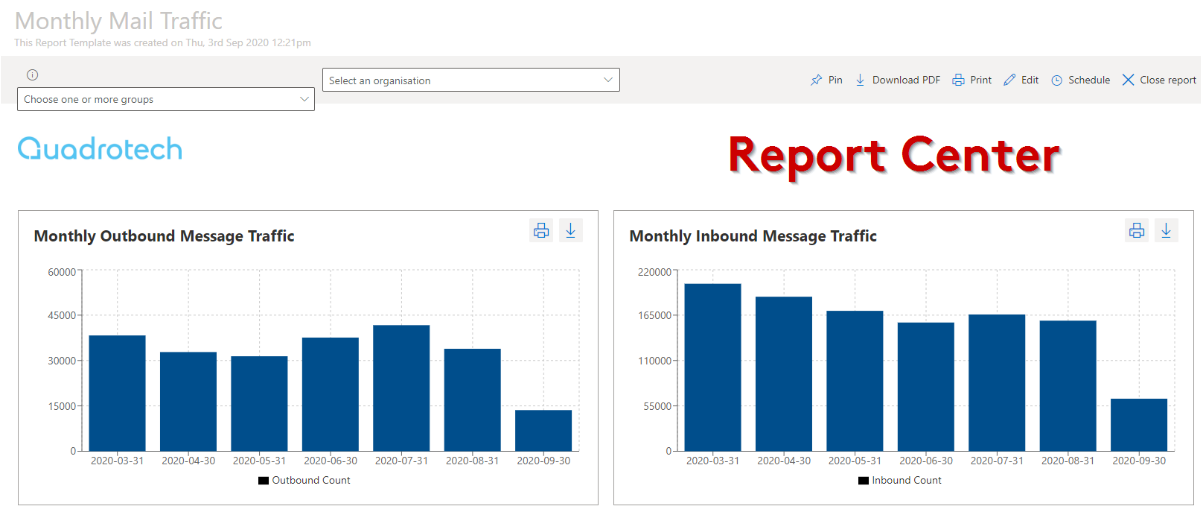
You have the option to add a logo to your report in the Nova Report Center. This allows you to add your own unique branding to each report, including system reports.
To do this:

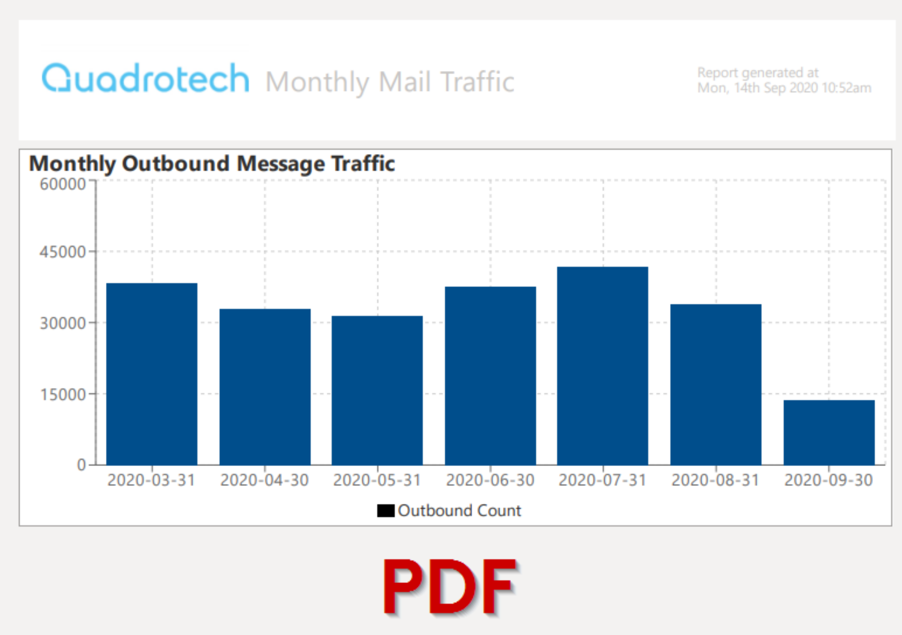
1. Sign in to the Nova Report Center as an administrator and click on the cog icon in the top right hand corner.
2. Click **System Settings** in the Organization sidebar.
3. In **Overview,** click **Custom Branding**.

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, like the Quadrotech logo as seen below, in both the Nova Report Center and when downloaded as a PDF.





You may only have one logo on your report at a time. To remove the logo, follow the steps above and click **Remove logo.**

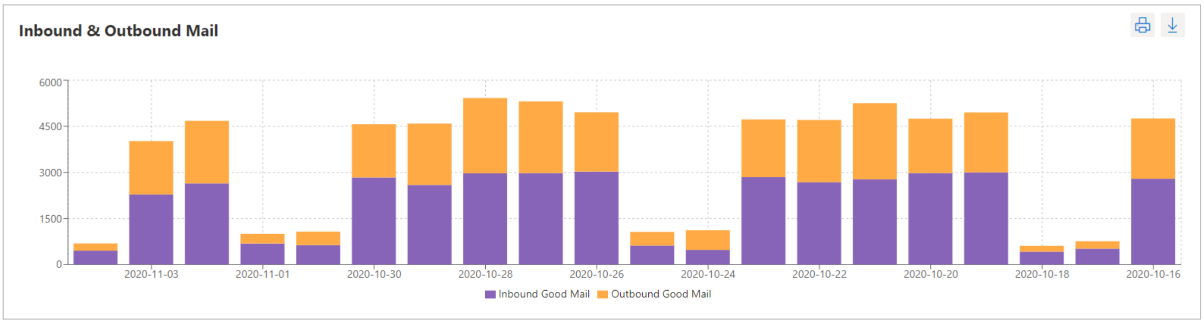
How to Create Stacked Graphs

Creating stacked graphs in Nova allows you to view multiple data fields in one easy to analyze chart. For example, in the chart below, we'll 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.
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.



NOTE: Currently, you can't download stacked charts as a PDF. We will update this article once this feature becomes available.

Nova IP Addresses

Some companies have Conditional Access requirements, to lock down the service accounts to only be able to access their environment from a whitelisted IP range. You can do the same for Nova service accounts by whitelisting the following IP addresses, dependent on the region your Nova account is hosted:

US
52.4.135.49
52.7.89.28

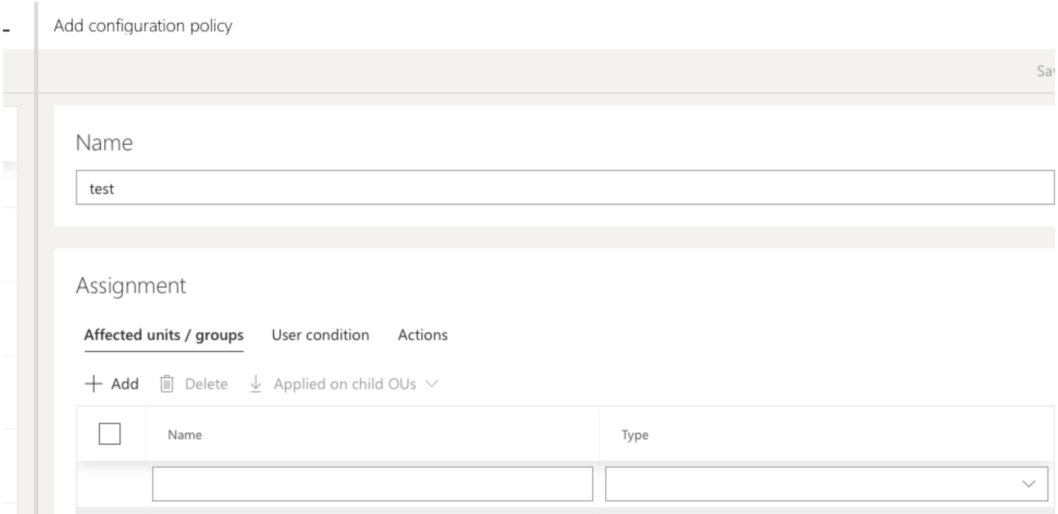
EU
52.17.100.102
52.18.76.133

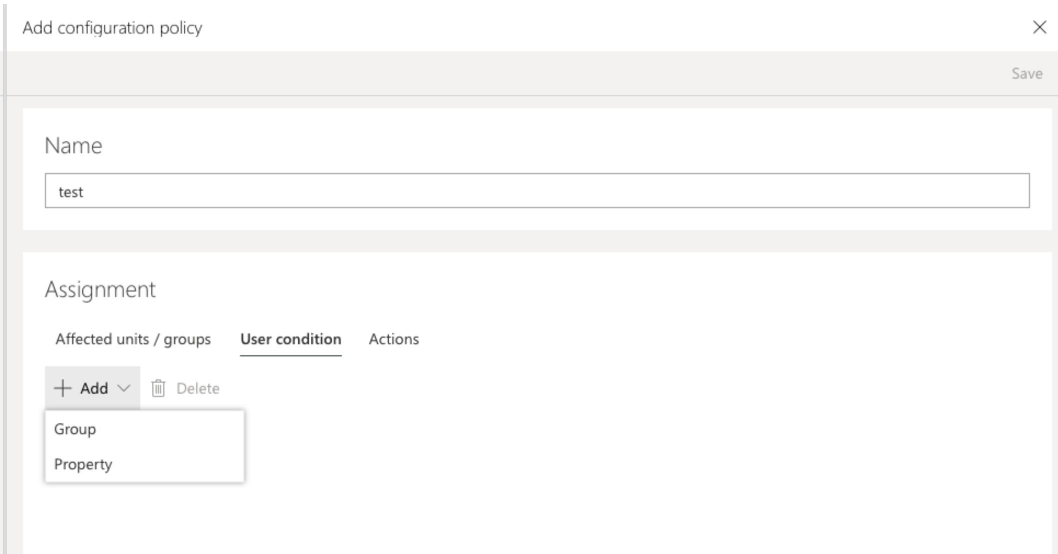
In order to send out scheduled reports, the following SMTP IP addresses also need to be allowed:
US SMTP IPs
52.6.218.113
52.21.158.57

EU SMTP IPs
54.72.208.154

Attribute Based Configuration Policies

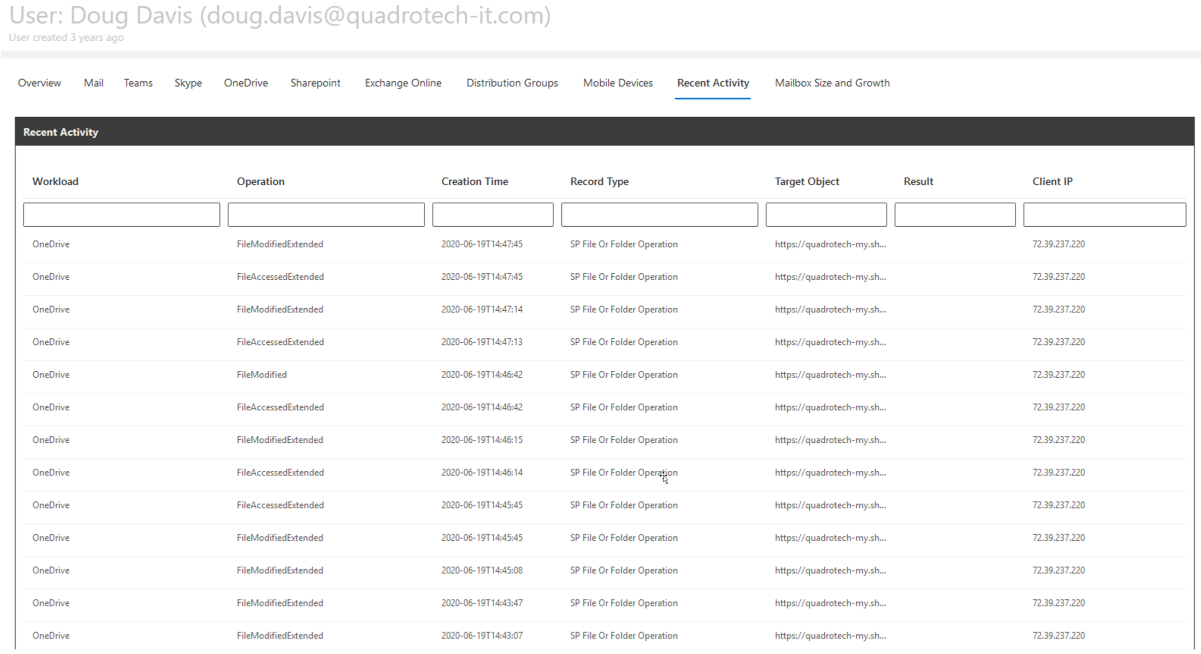
As of the 21st May 2020 release of Nova, configuration policies can now be based on attributes, which can be used to define who is covered by the policy.
For example, as a Nova administrator, you may want to automatically assign licenses to users based on which groups or Teams they are in to automate license management and assignment.


Add configuration policy
Name
test
Assignment
Affected units / groups
User condition
Actions
Add
Delete
Applied on child OUs
Name
Type


Add configuration policy
Save
Name
test
Assignment
Affected units / groups
User condition
Actions
Add
Delete
Group
Property

Populated Recent Activity in User Profile

As of the 6th July 2020 release of Nova, the Recent Activity section within User Profile is now more populated. This provides you a better and wider scope of information in fewer clicks.

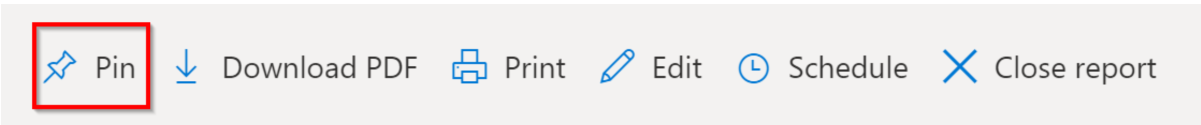


Workload	Operation	Creation Time	Record Type	Target Object	Result	Client IP
OneDrive	FileModifiedExtended	2020-06-19T14:47:45	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileAccessedExtended	2020-06-19T14:47:45	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:47:14	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileAccessedExtended	2020-06-19T14:47:13	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModified	2020-06-19T14:46:42	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileAccessedExtended	2020-06-19T14:46:42	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:46:15	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileAccessedExtended	2020-06-19T14:46:14	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileAccessedExtended	2020-06-19T14:45:45	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:45:45	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:45:08	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:43:47	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220
OneDrive	FileModifiedExtended	2020-06-19T14:43:07	SP File Or Folder Operation	https://quadrotech-my.sh...		72.39.237.220

Pin Reports to the Navigation Bar

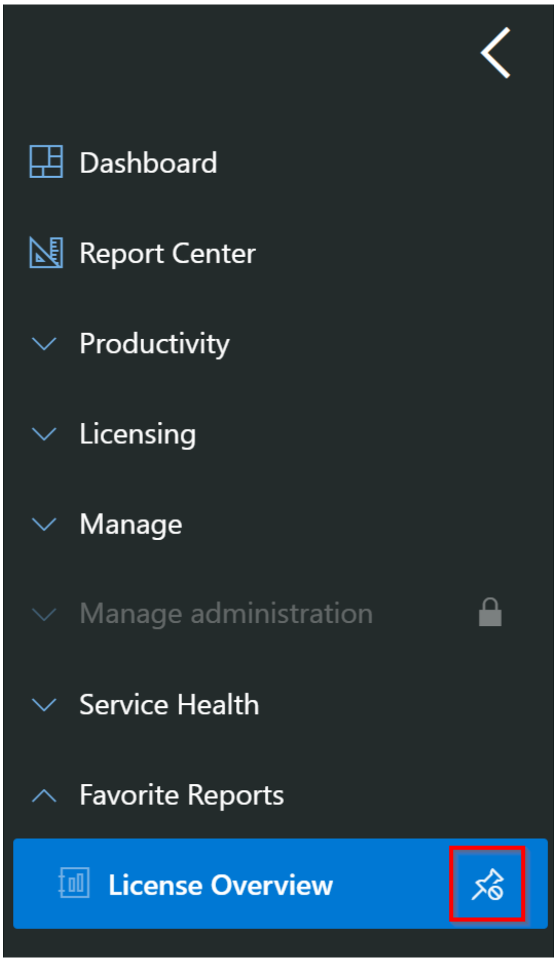
You can pin up to 5 reports to the navigation bar, for quicker access to frequently used or viewed reports.
To pin reports, click on the report you want to pin.

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.

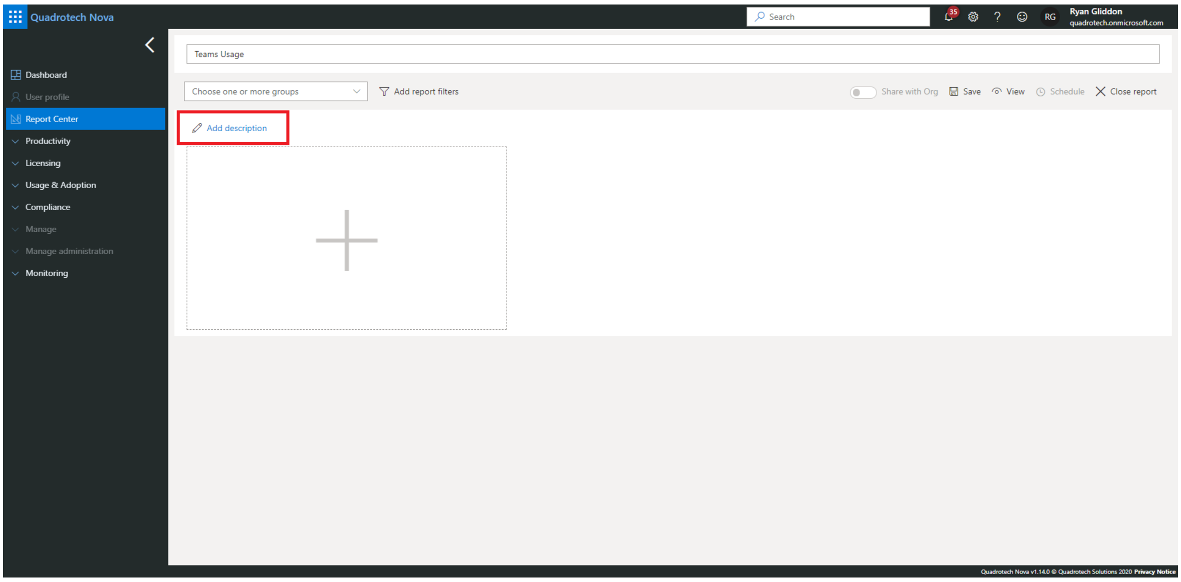


Describing Reports and Sections in Report Center

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's see how to do that below.

Adding a description to a report

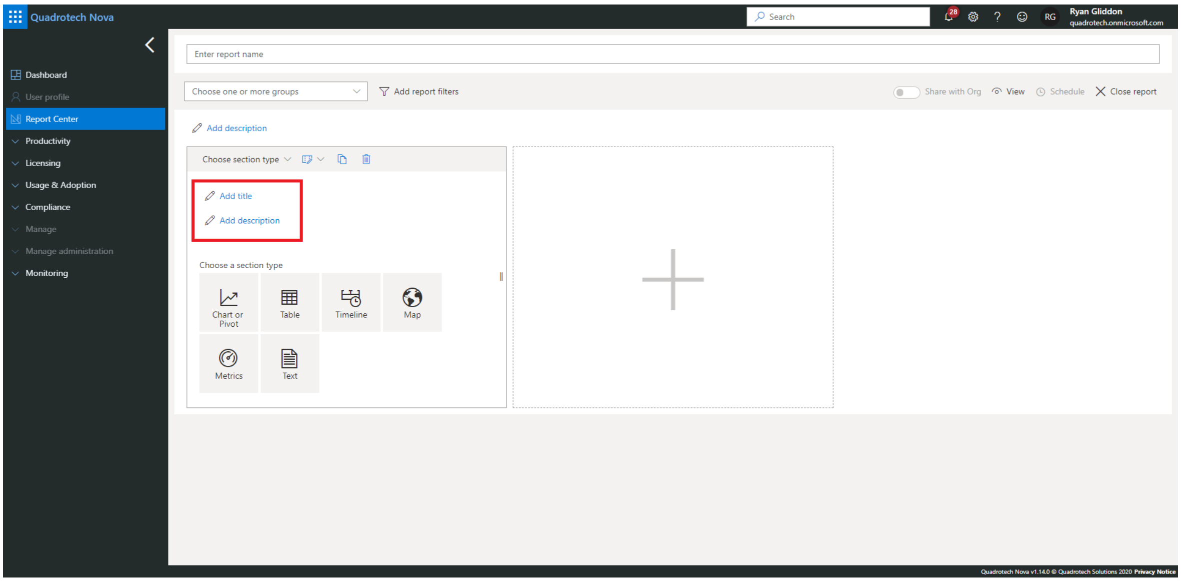
1. Open a report you have previously created, or start a new report by clicking '**Create Report**' in the top right hand of the screen.
2. Then click '**add description'** as highlighted below.



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. Now you can add both a title and a description to your section, as seen in the image below.



NOTE: If you're 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

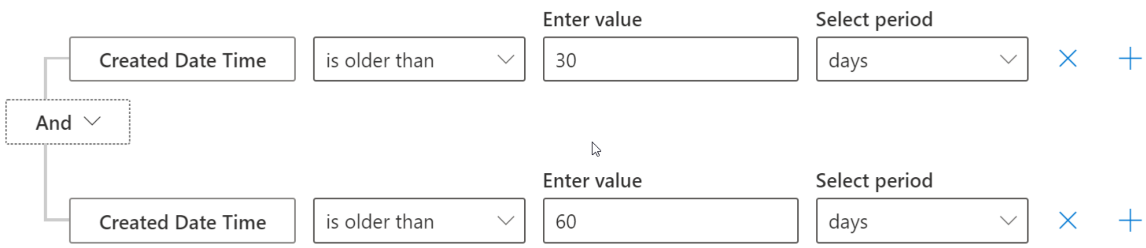
and so on. The toolbar can be found here.

Data Filtering in Nova Reporting

Filtering your charts and tables and dates is easy to do within the Nova Report Center. 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.
    a. 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.
    b. 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.



Reporting with Nova about Microsoft Teams Call Quality

Issue

Microsoft provides the capability to enable Microsoft Teams and Skype for Business Online Call Quality analysis and reporting. This is via the Call Quality Dashboard (CQD).
We are often asked if we can use Nova Reports to view this information.

Solution

Unfortunately at the moment this data is not available from Microsoft via an API call, so we are unable to collect this data. That means we can't currently create Nova Reports using this data. We review this capability from time to time, and will provide updates here.

Customize and Organize Reports

Nova reports can be customized and organized.

Customizing Reports

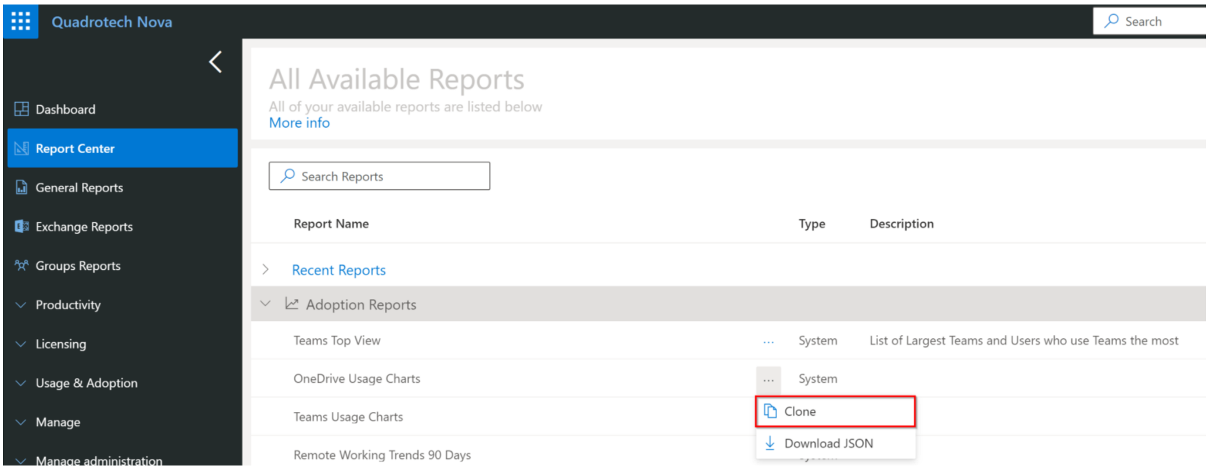
There are several ways to customize reports so they're specific to your organization. You can customize a report's sections and layout. You can customize the data source and fields used in each section. And, you can customize how information displays in each section by applying sorting and filters.

Searching Reports

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

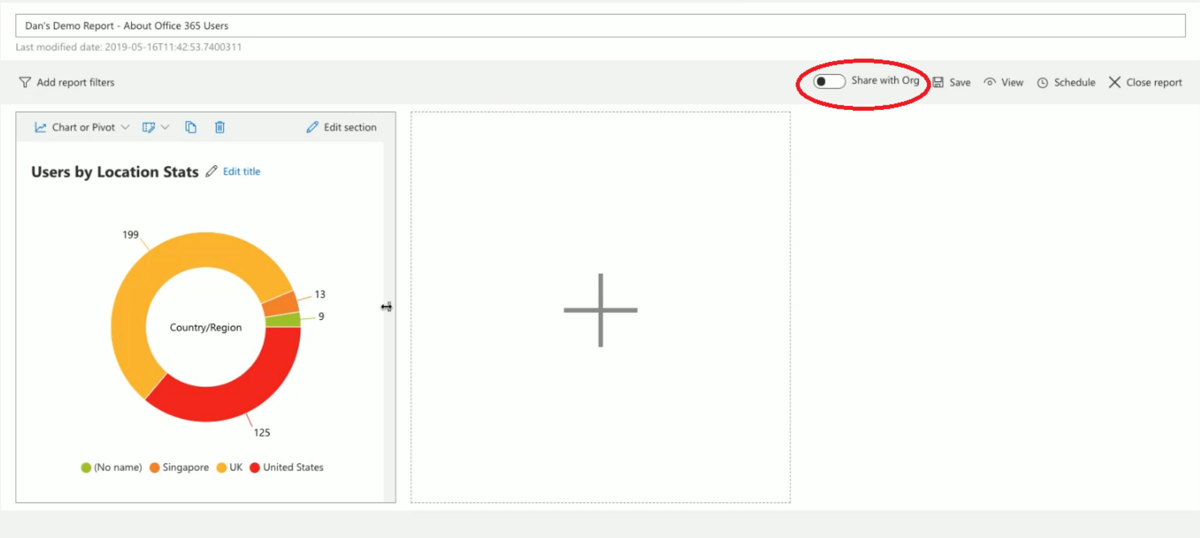
Cloning Reports

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.

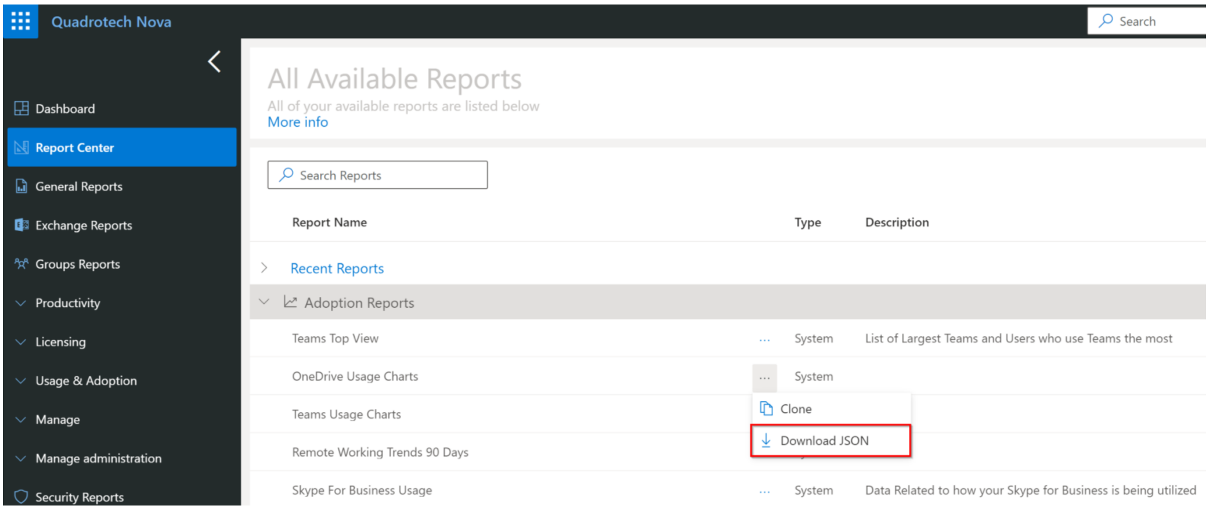


Scheduling Reports

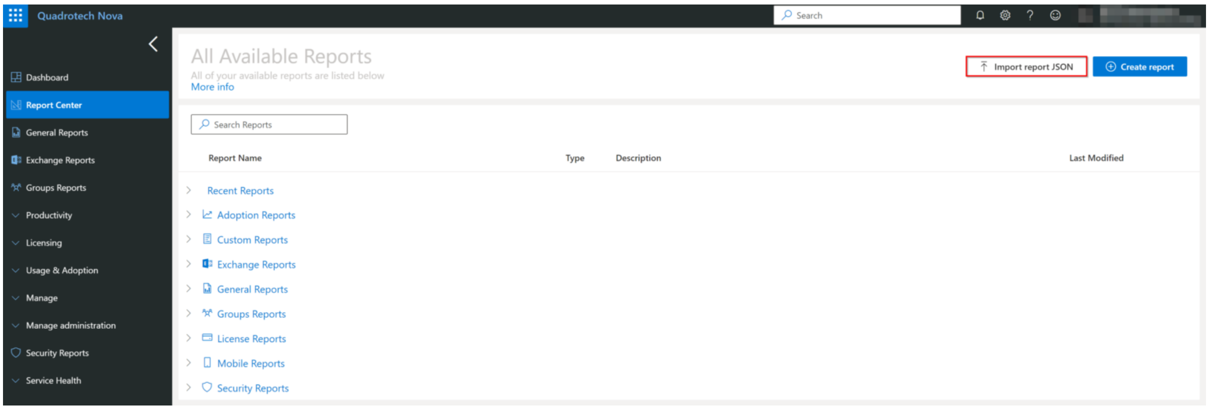
You can schedule reports to be sent one time or periodically to stakeholders.

Storing (Downloading/Importing) 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's how you can download a report definition:



And, here's how you import a report definition:



Service Accounts for Reporting

Overview

Nova Reporting uses service accounts to collect data from O365 tenants. Service accounts are used to collect data via PowerShell in cases where data can't be collected via GraphAPI.
This article explains how to create a Read-Only Administrator account in Office 365 for use with Nova. It is important that you complete all the steps. Service account can be created via:

- **PowerShell**
- **Microsoft 365 Admin Center**

It is recommended that you use the PowerShell method, as this contains less steps, however at the bottom of this article you can also find some steps on how to do this via the Admin Portal.
Your organization will not be charged by Microsoft for this account as it does not require an Office 365 licence.

Creating the Service Account Using PowerShell

Connecting to Office 365
Before we begin, you need to install the "Microsoft Online Service Module" onto your machine. See Connecting to Office 365 Using Powershell how instructions on how to do this.
Now open up Windows PowerShell and Copy & Paste in the following commands to connect to Office 365.
Please enter the username and password of an Office 365 Administrator account when prompted.

```
$Office365credentials = Get-Credential

Import-Module MSOnline

Connect-MsolService -Credential $Office365credentials
```

Creating the Service Account
Now that you are connected to Office 365 in PowerShell, we can create the Service account. Modify the line below and set the *company.onmicrosoft.com* part to match your own Office 365 *.onmicrosoft.com* domain and replace the password with a secure password of your own. We recommend a password of 10 characters or more that includes a mixture of capital and lower case letters, numbers and special characters.

```
New-MSolUser -DisplayName "Service Account for Nova Reporting" -UserPrinc
```

Next we need to add our new account to the ‘Global reader’. You can do this by copying and pasting the following line into the PowerShell window.
Remember to set the *company.onmicrosoft.com* part to match your Office 365 domain name

```
Add-MSOLRoleMember –RoleName "Global reader" –RoleMemberEmailAddress Nova
```

Please note that you will not receive any confirmation if the commands are successful. You can check if the service account was set correctly by running PowerShell commands below:

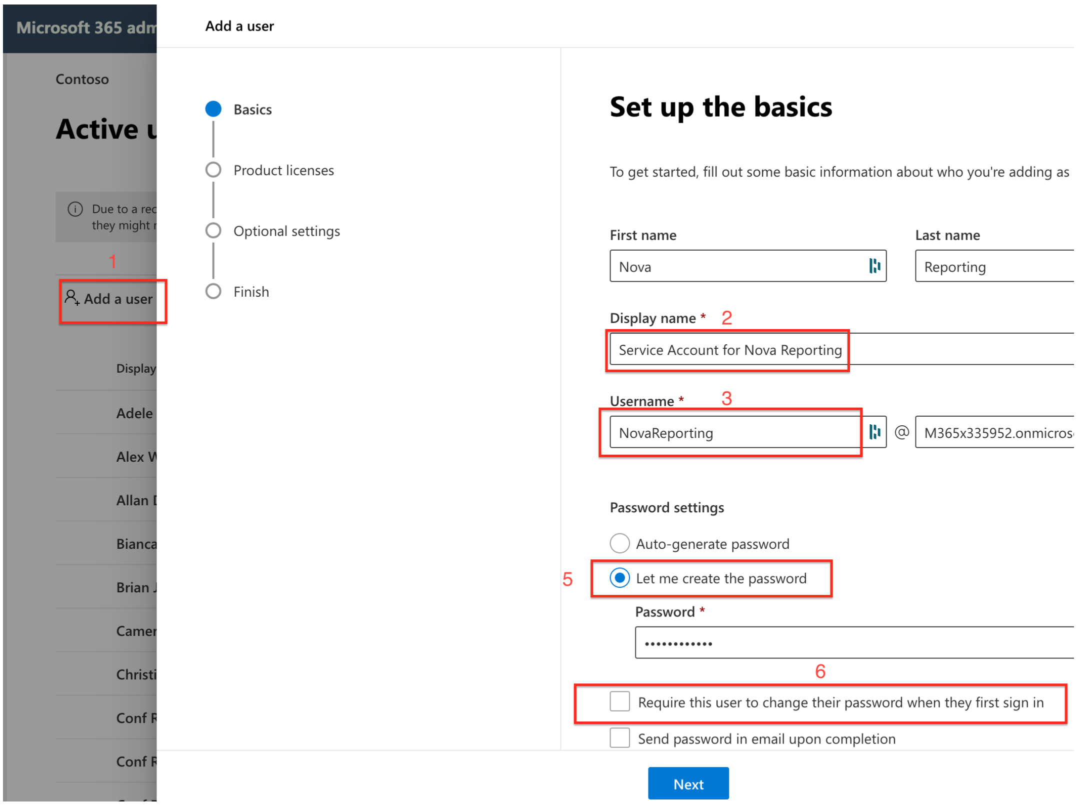
```
$role = Get-MsolRole -RoleName "Global reader"

Get-MsolRoleMember -RoleObjectId $role.ObjectId
```

Creating the Service Account via the Microsoft 365 Admin Center

You can also create the service account via the Microfost 365 Admin Center, however you would still need to run a final PowerShell cmdlet to ensure that the password does not expire.

1. On the Admin home page, go to *Users -> Active users* and click on button *Add a user*
2. Enter a Display Name (“Service Account for Nova Reporting”)
3. Enter a User Name (“NovaReporting”)
4. Ensure that the domain is the company.onmicrosoft.com one
5. Select “*Let me create a password*” and enter a strong one

6. Ensure “*Require this user to change their password when they first sign in*” is NOT ticked



7. In *Product licenses* page choose “*Create user without product license*”
8. In *Optional settings* page chose Admin center access and select Global reader
9. Review all your data and click *Finish adding* in last page

Note

If the password of the service account needs to be changed or is expired, it must be changed in Office and in Tenant Management System Client.

If your company policy allows passwords to never expire you can do it via PowerShell:

```
Set-MsolUser -UserPrincipalName NovaReporting@company.onmicrosoft.com -Pa
```

Connecting to Office 365 Using Powershell

Cogmotive Reports/Radar Reporting is now Nova! A highly sophisticated revamp of our same great Office 365 Management software, with a brand new look, feel and dimension. The most powerful way to manage Office 365.

Another great management option for Office 365 is to use PowerShell, a command line interface that connects to Office 365 via the Internet.
Whilst it may seem daunting to people unfamiliar with working on the Command Line, it really isn't as hard as it looks. This blog post will guide you through the basics of connecting to PowerShell.

Set up your computer to use Office 365 PowerShell

Firstly, you need to set up your computer with the necessary PowerShell modules. This only needs to be done once, however you need to have administrative permissions on the computer. Unfortunately, Microsoft has made this part very confusing, as there are multiple versions of the PowerShell module available.

The newest version is known as the Azure AD PowerShell module and is distributed via the PowerShell Gallery. This unfortunately means that you cannot download the module directly. Instead, you will need to use the PowerShellGet module, which might not be available on your system. In this case, you will have to install the module by using one of the methods detailed in this article.

An older version of the module, known as the Windows Azure Active Directory PowerShell or MSOnline module is also available. Like the Azure AD module, it's also being distributed via the PowerShell Gallery, however an MSI installer version can be downloaded from here.

Both the Azure AD and MSOnline modules also have a Preview version, further contributing to the confusion. What's even worse, some functionalities are only available in specific module versions, thus it might be necessary to have multiple versions installed and to use them interchangeably.

Connecting PowerShell to Office 365

Regardless of which version of the module you install, connecting to Office 365 is performed by executing a cmdlet. To connect via the Azure AD module, use:

Connect-AzureAD

To connect via the older MSOnline module, use:

Connect-MsolService

You will be prompted for credentials. Enter the full UPN (User principal name) value of your Office 365 administrator account as well as your password. Depending on the settings you have configured, you might be asked to perform additional verification via Azure MFA.

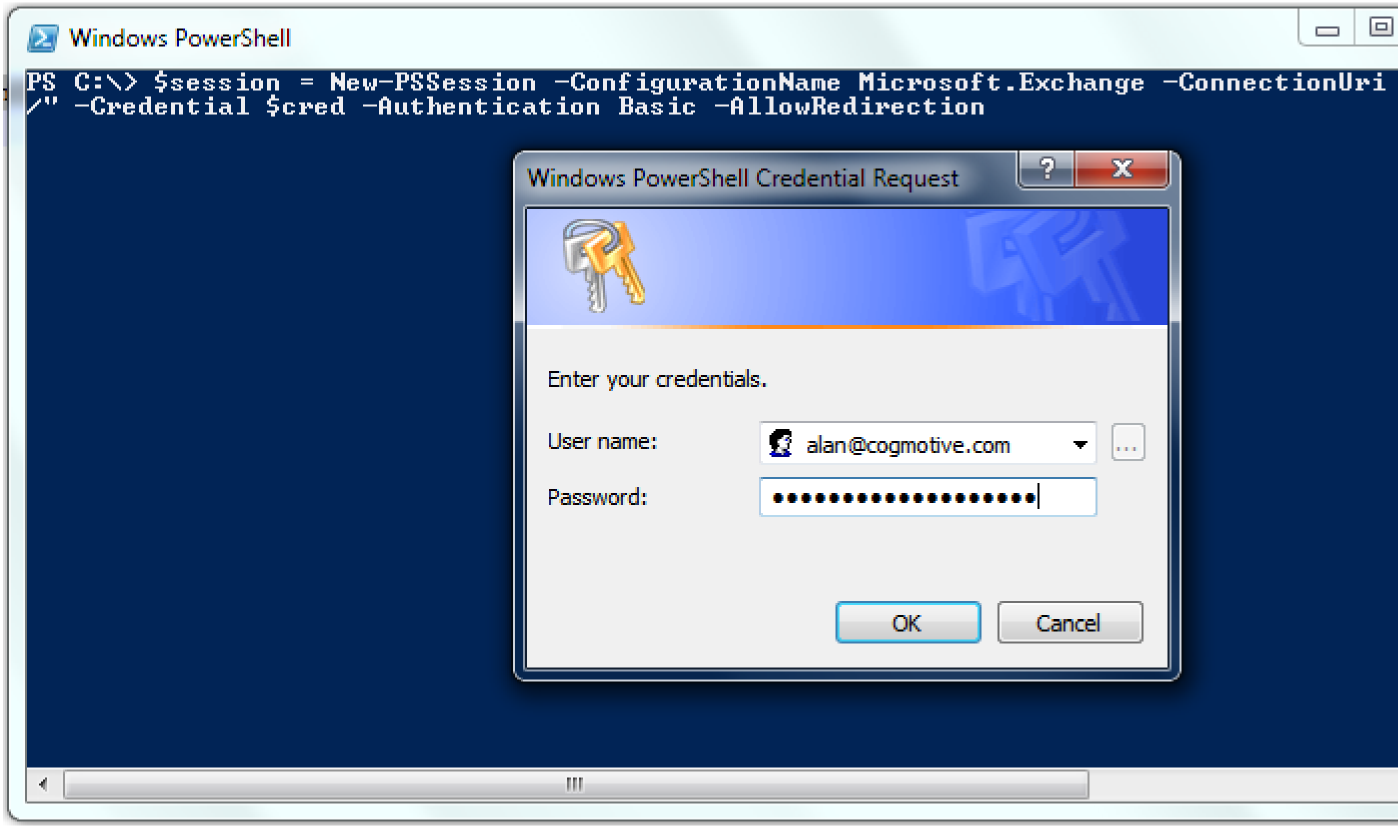
Connecting PowerShell to Exchange Online

To connect PowerShell to Exchange Online, you will need to configure the execution policy to allow execution of signed PowerShell script. You can find detailed steps in this article. You need to perform them only once on each machine you will be connecting fromOnce the execution policy is configured, you need to create a connection to Office 365. You can do this by typing (or copying/pasting) the following into PowerShell.

NOTE: To paste into PowerShell you use Right Click. Here is a **great video** on how to use Copy and Paste in PowerShell.

$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential (Get-Credential) -Authentication Basic -AllowRedirection

Once this is in the PowerShell window, press Enter to execute the command.

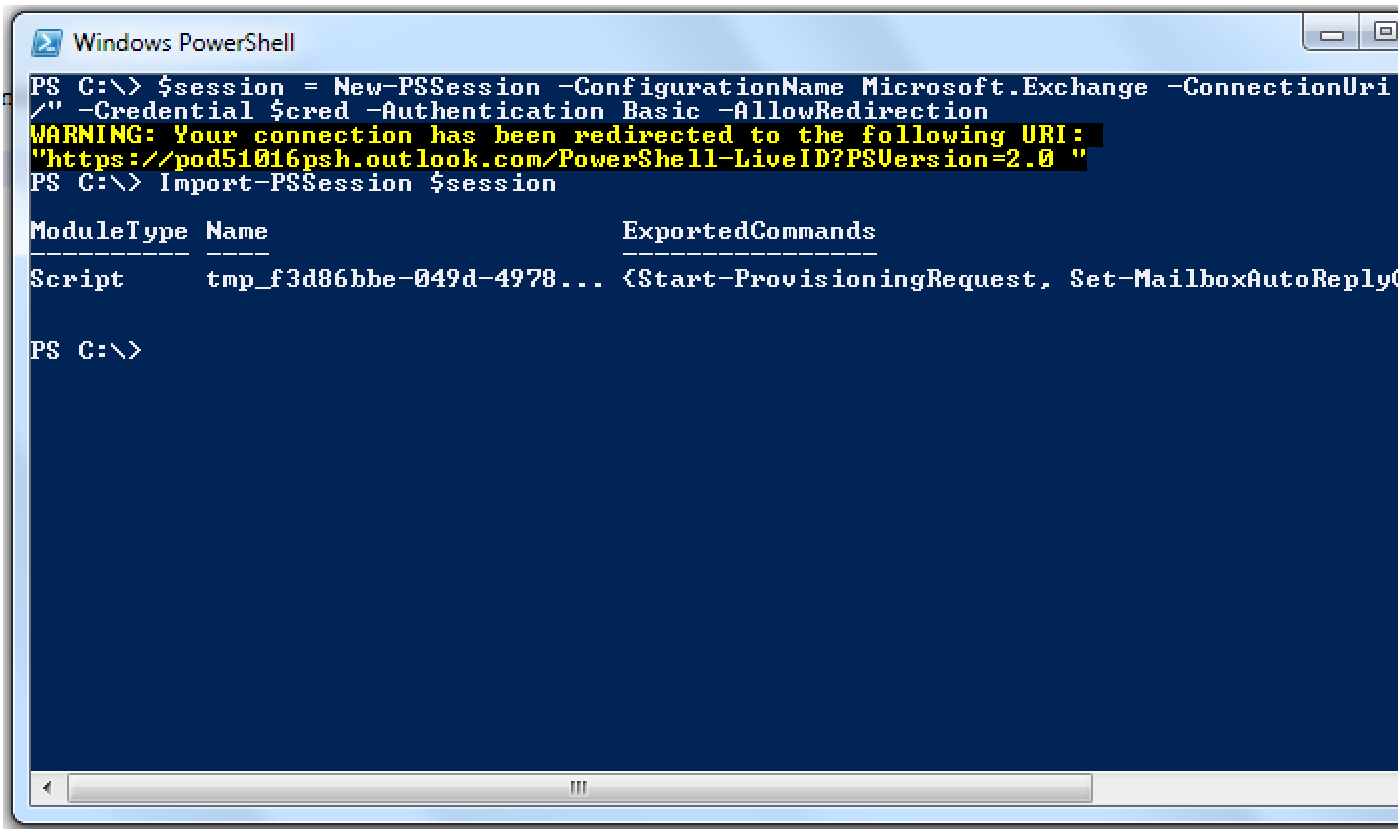


Now you simply type in the username and password for an Administrator account in your Office 365 and click OK. You will probably see some warnings. Don't worry, they are normal.

You are now authenticated into Office 365 and have a session open. The last step is to fetch all the available cmdlets by using the following PowerShell command:

Import-PSSession $session

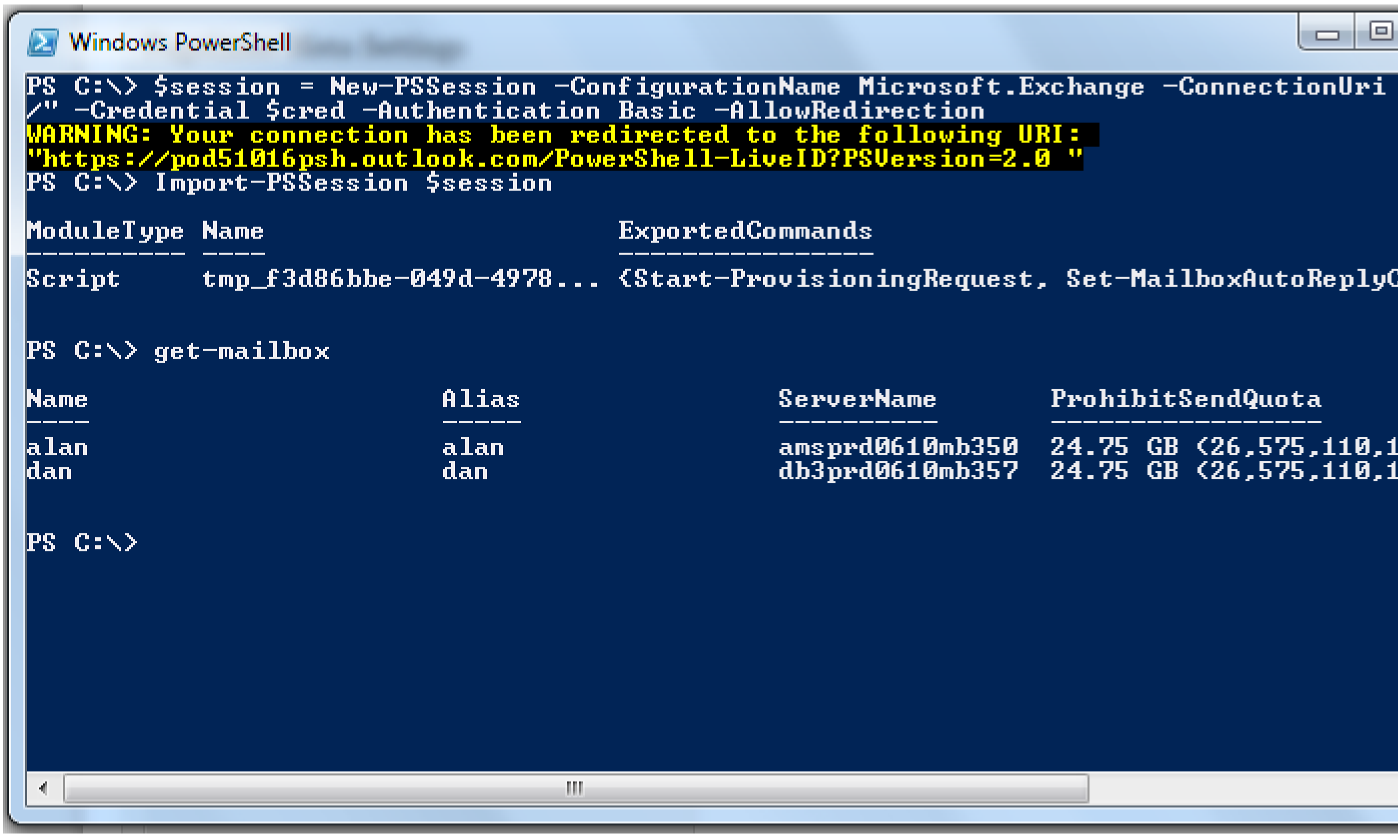
Congratulations! You're connected!



Now you've gone to all the trouble of connecting to PowerShell, let's do something to prove that it works. Type the following into the PowerShell window and press Enter:

Get-Mailbox

You should now see a list of all the users in your Office 365 account that have mailboxes



Nova Report Center

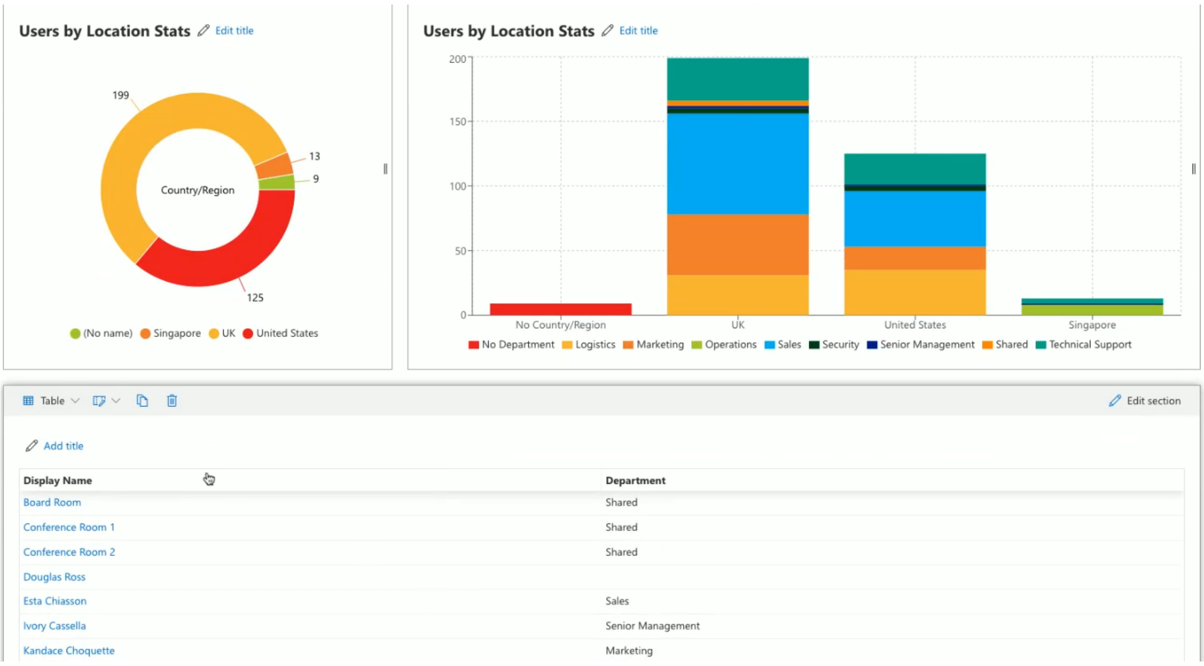
Microsoft has several different interfaces for tools used to perform Office 365 management, reporting, and auditing tasks. In contrast, Nova users perform that work in a single user interface. To achieve this, Nova gathers reporting and auditing data from Office 365. Reporting data is collected about 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 Office 365.

The flexibility and power of the Nova Report Center is ideal for organizations with custom reporting needs that can't 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 Office 365 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 don't want to build an entirely new report, you could even clone an existing report and customize it to meet your new needs.

Below is an example of a report built using Report Center.



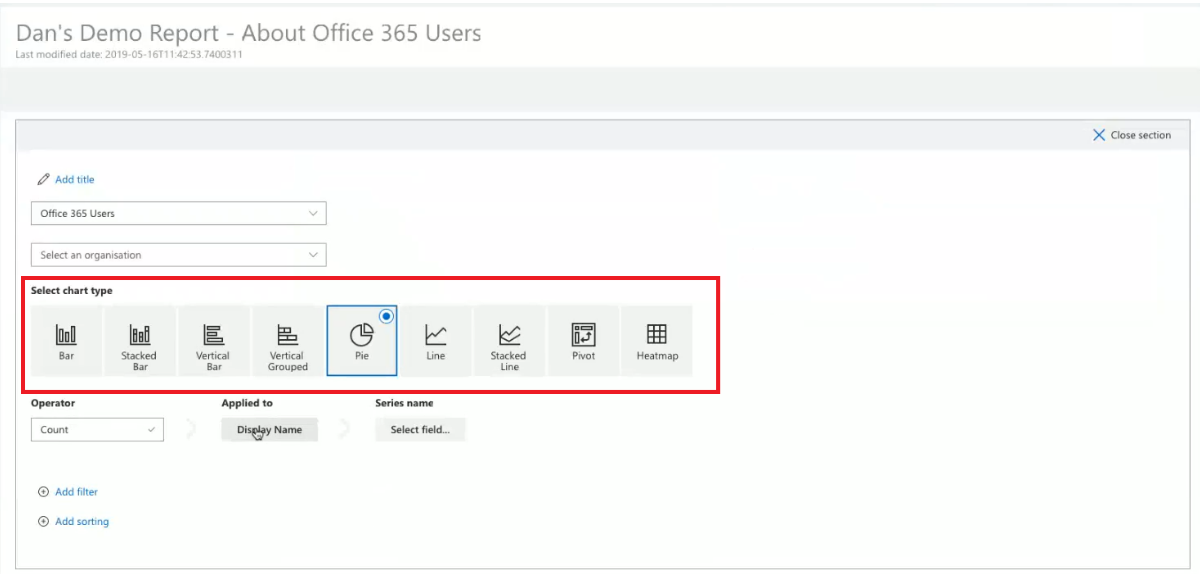
Here’s more about the steps to set up a custom report:

Step 1: How will the report look?

Give a custom report structure by adding sections to control how it looks. For example, you might add these sections to a report:

- A pie chart
- A heat map
- A table

Here’s where you select what section you’ll add to your report:



As sections are added to a report, you’re 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 article. Then, that data is collated, filtered, and displayed in the report. Here are a few possible data sources:

- A list of Office 365 users
- A list of Office 365 distribution groups
- Data source availability

After a data source is selected, you're 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's an example of the screen where you select the fields that display in a section:

Applied to

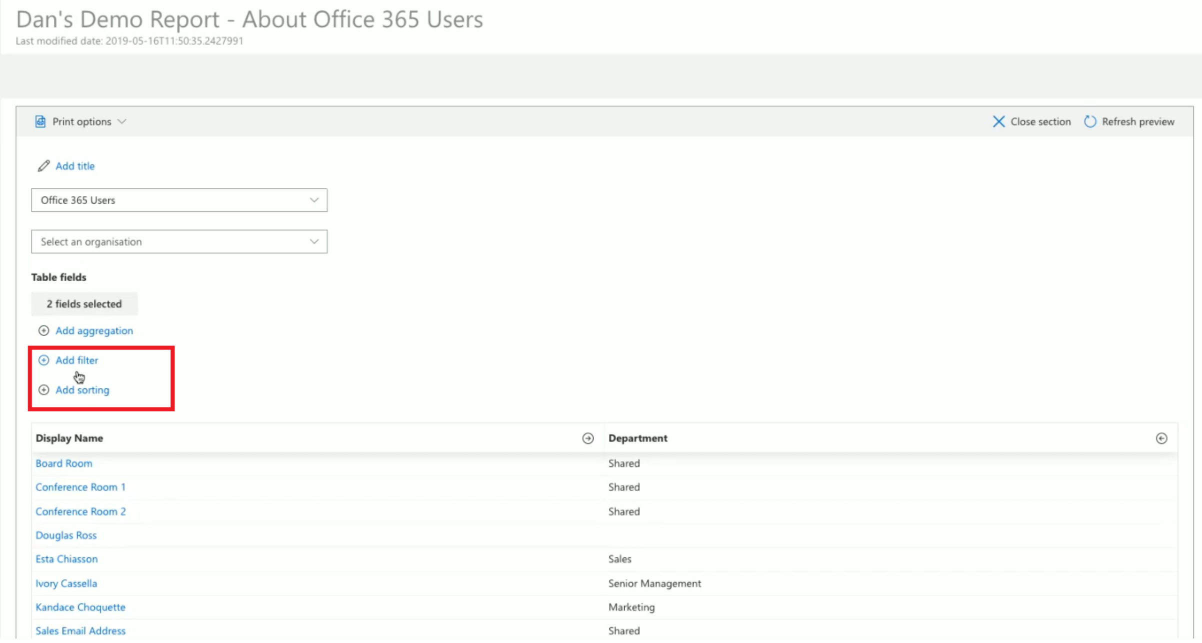
	Field Name	Description	Data Type	Data Source
	Field Name Filter / Search	Description Filter	String, Date, ...	Office 365 Mail Traffic
○	Inbound Good Mail		Number	Office 365 Mail Traffic
○	Inbound Spam Content Filtered		Number	Office 365 Mail Traffic
○	Inbound Spam Envelope Block		Number	Office 365 Mail Traffic
○	Inbound Spam IP Block		Number	Office 365 Mail Traffic
○	Outbound Good Mail		Number	Office 365 Mail Traffic
○	Outbound Malware		Number	Office 365 Mail Traffic
○	Outbound Spam Content Filtered		Number	Office 365 Mail Traffic
○	Outbound Spam Envelope Block		Number	Office 365 Mail Traffic
○	Outbound Spam IP Block		Number	Office 365 Mail Traffic

For more about data sources, go to this article.

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'll only have to configure them once.

To filter by date, check out this article.

Creating a new Custom Report

Expanding on the 3-step process above, here's an overview of the steps you'll follow to create a new report:

1. In Nova, 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 choose whether you want the section to contain a chart, graph, table, or map.
6. Choose a data source.
7. Customize the chart's colors, fields, and sort/filter.
8. When you're happy with the section, close it.
9. Repeat steps 4-8 for all tables/sections you want the report to contain.
10. Organize sections on the report, changing their size and location, if desired.
11. When the report is complete, save it.

Using the card section type in a report

Adding a description to your report

Report Center Terminology

The Nova Report Center has some terminology which you may not be familiar with. Check out this article for more information.

Custom Report Examples

Click here to see some examples of custom reports created using the Nova Report Center.

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.

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't 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's say you want to quickly see how many Azure AD 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 won't be organized into pages.

Overflow

It's 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.

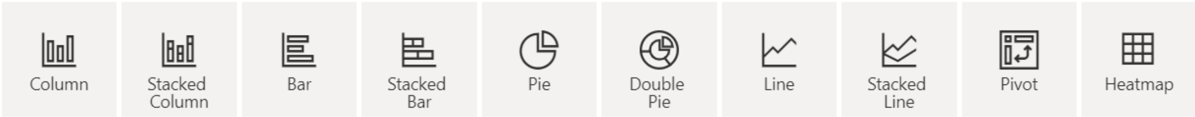
Which Type of Report Do I Need?

When you open the Nova Report Center, you will see a few chart types available. These are listed below, click on one to see more information about each chart type.
Check out this article for terminology related to the Nova Report Center.

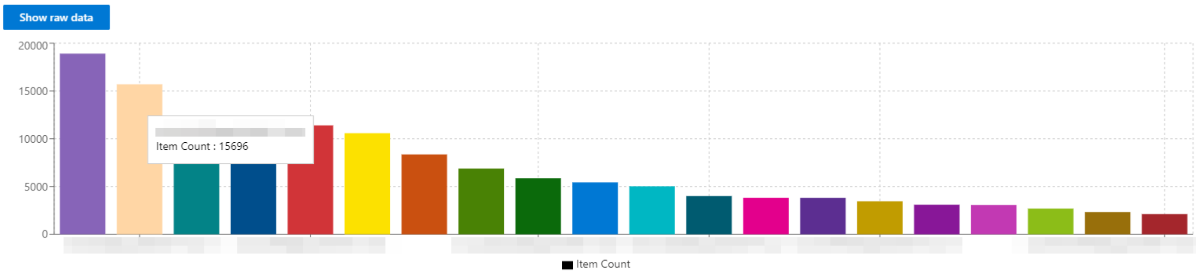
- Chart or Pivot
- Table
- Timeline
- Map
- Card
- Metrics
- Text

Chart and Pivots in Nova Report Center

Charts and pivots in Report Center are the most frequently used type of chart in Nova. 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. Available graph types are below. Choose charts that suit your users.



Nova's charts are easy to read and digest. They're customizable, with a range of sorting and filtering choices. Choose to show the raw data as a table, or hover over each segment to see the individual data, as shown below.



Check out some custom chart and pivot report examples below.

User by location

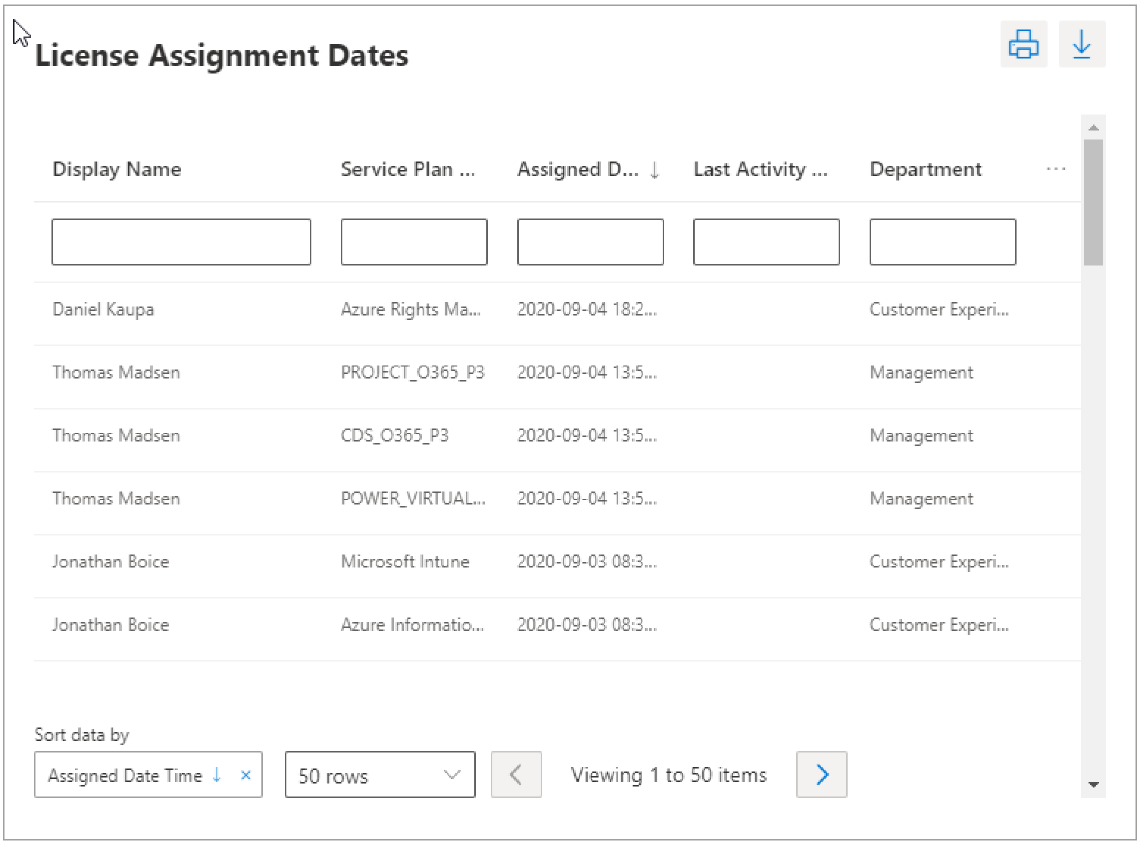
OneDrive Usage

License Utilization

Inbound and Outbound Mail

Using Tables in Nova Report Center

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.



License Assignment Dates

Display Name	Service Plan ...	Assigned D... ↓	Last Activity ...	Department
Daniel Kaupa	Azure Rights Ma...	2020-09-04 18:2...		Customer Experi...
Thomas Madsen	PROJECT_O365_P3	2020-09-04 13:5...		Management
Thomas Madsen	CDS_O365_P3	2020-09-04 13:5...		Management
Thomas Madsen	POWER_VIRTUAL...	2020-09-04 13:5...		Management
Jonathan Boice	Microsoft Intune	2020-09-03 08:3...		Customer Experi...
Jonathan Boice	Azure Informatio...	2020-09-03 08:3...		Customer Experi...

Sort data by

Assigned Date Time ↓ ×   50 rows   Viewing 1 to 50 items

Filtering in your reports can give you more specific results which could give you the exact information that you need quickly. Find out about this, including how to filter between dates, here.

You can also sort certain data fields by ascending or descending order.
You can limit the amount of data results within your table. To do this, set your offset and limit to suit your needs. Enable paging allows you to page your data results, for example in 10, 25 or 100 results per page. Disabling this feature gives you all of the results in one page.

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.

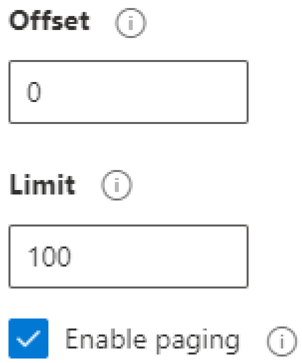


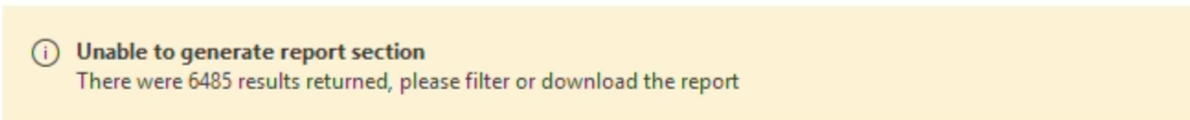
Table report examples can be found below:
Office 365 Spam and Malware
License Utilization
OneDrive Usage
Search within QTD/YTD parameters

Filtering Table Data in Nova

There are three ways that tabular (table) data can be filtered in Nova. We'll see how they're used in this article.

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:

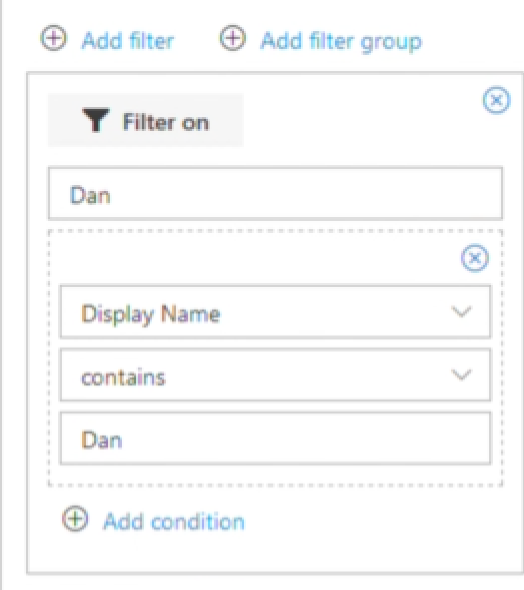
1. Clicking on 'Add Filter'
2. Choosing an appropriate field, like 'Display Name'.
3. Choosing an operator like 'Contains' or 'Begins with'
4. Entering the filter or search criteria.

You can see how to do it in this short video:
https://youtu.be/2M-diHeIzeM

Global Filtering

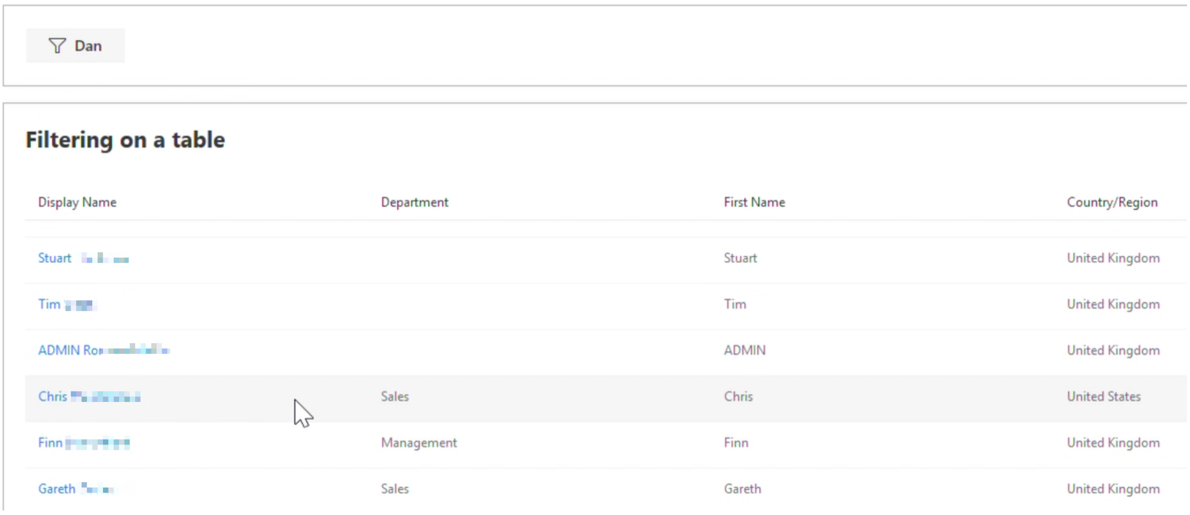
You can also do a global filter on a report to provide some helpful filtering to a user of the report. To do this you:

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’.



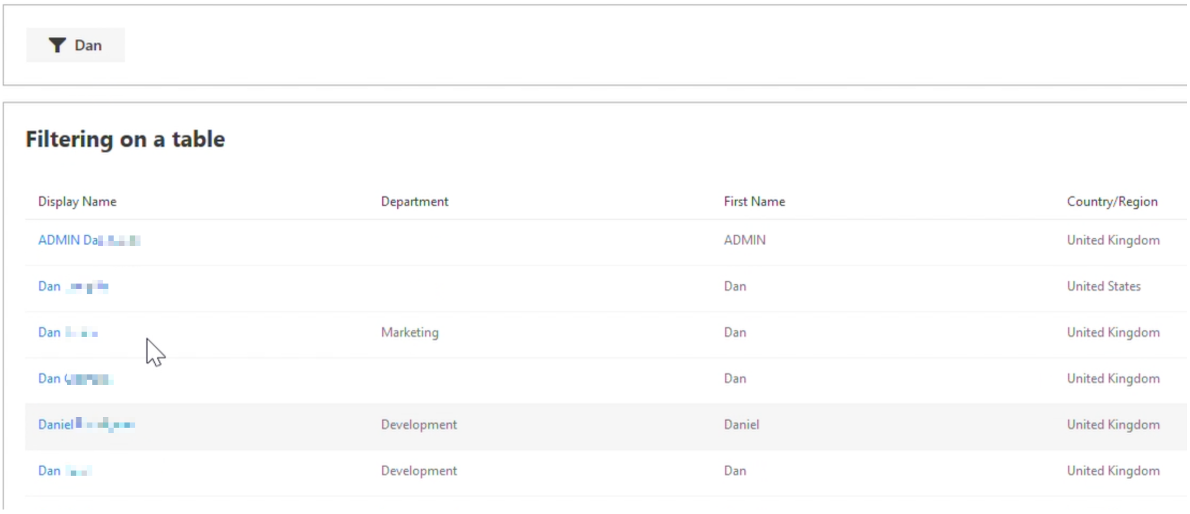
Now at the top of the report you’ll see the filter, and it can be applied at any time, and can also be disabled at any time; giving you extra flexibility.

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



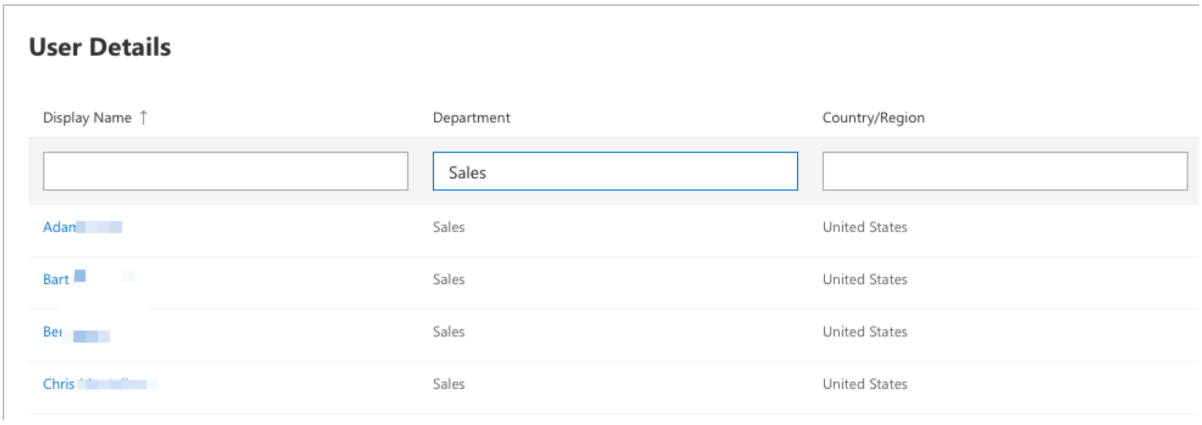
Display Name	Department	First Name	Country/Region
Stuart		Stuart	United Kingdom
Tim		Tim	United Kingdom
ADMIN Ro		ADMIN	United Kingdom
Chris	Sales	Chris	United States
Finn	Management	Finn	United Kingdom
Gareth	Sales	Gareth	United Kingdom

Filtered:



Searching/Filtering Afterwards

On table data in Nova you'll 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:



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:

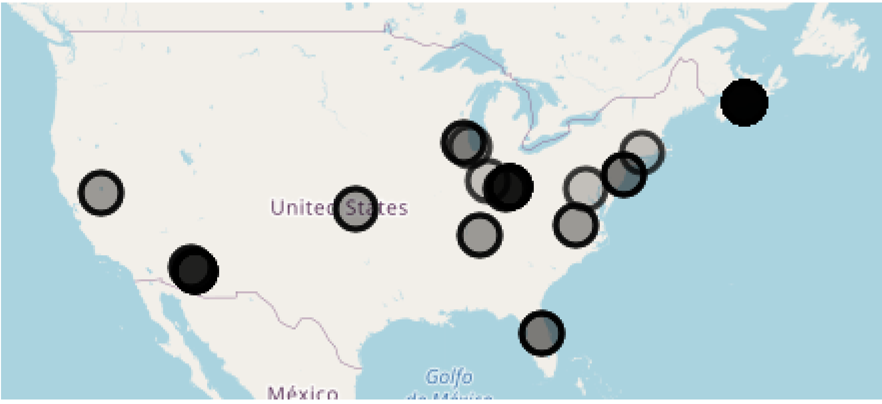
Date filtering

Using Timelines in Nova Report Center

Check out an example of a timeline report below:
https://youtu.be/JP85s3tZxc8

Using Maps in Report Center

Using the Map report in Nova Report Center 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:

1. Open a new section and select **Map**.
2. Add a title and description if necessary.
3. For the data source, choose **Office 365 Audit Data.**
4. Select your organization and organization group if necessary.
5. For select field, select **Geo Location.**
6. Your audit map should now appear. Click close section.

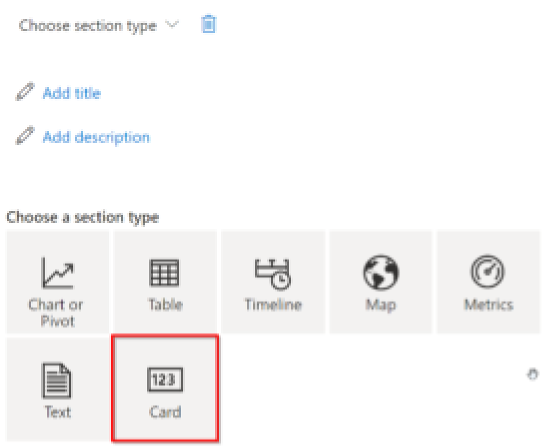
Using the Card Section Type in Nova Reports

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 article we’ll see an example of how this can be done.

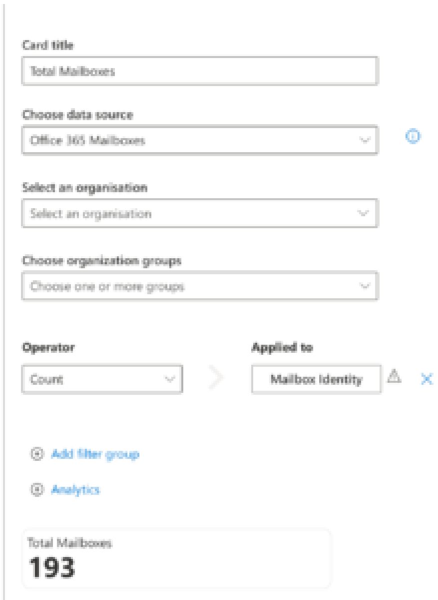
How to Create a Card

When creating a new section choose card:



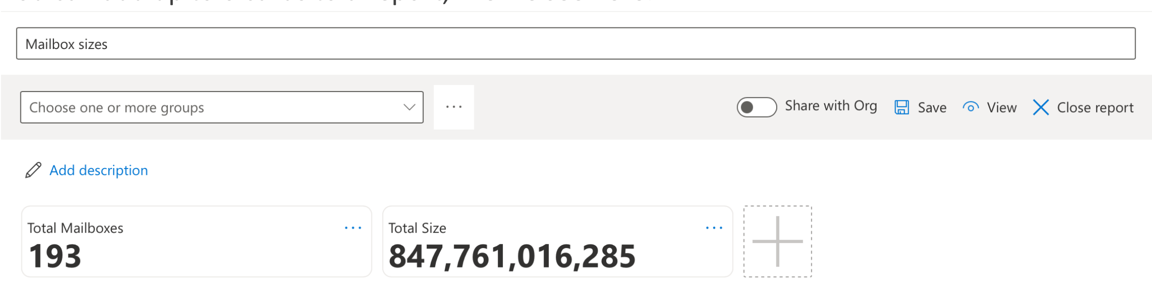
You can then choose an appropriate datasource, and other attributes related to the card section type.

For example:



As you can see at the bottom of the section, as you begin to build it, Nova will show you what the section will look like.

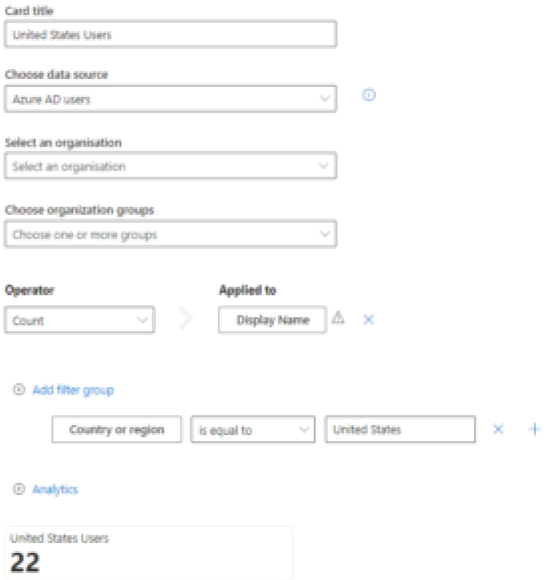
You can add up to 6 cards to a report, like we see here:



Filtering

You can also filter data sources to create cards that displays the information you want automatically.

For example, let's say you want to know how many Azure Active Directory users have their 'country or reigon' parameters set to the United States. This is easy to do by following the steps in the image below.



This is just an example, so feel free to explore the filtering system with our great range of data sources and filtering services.

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, perhaps you 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, like we can see below.

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

- OK severity
- Warning
- Critical

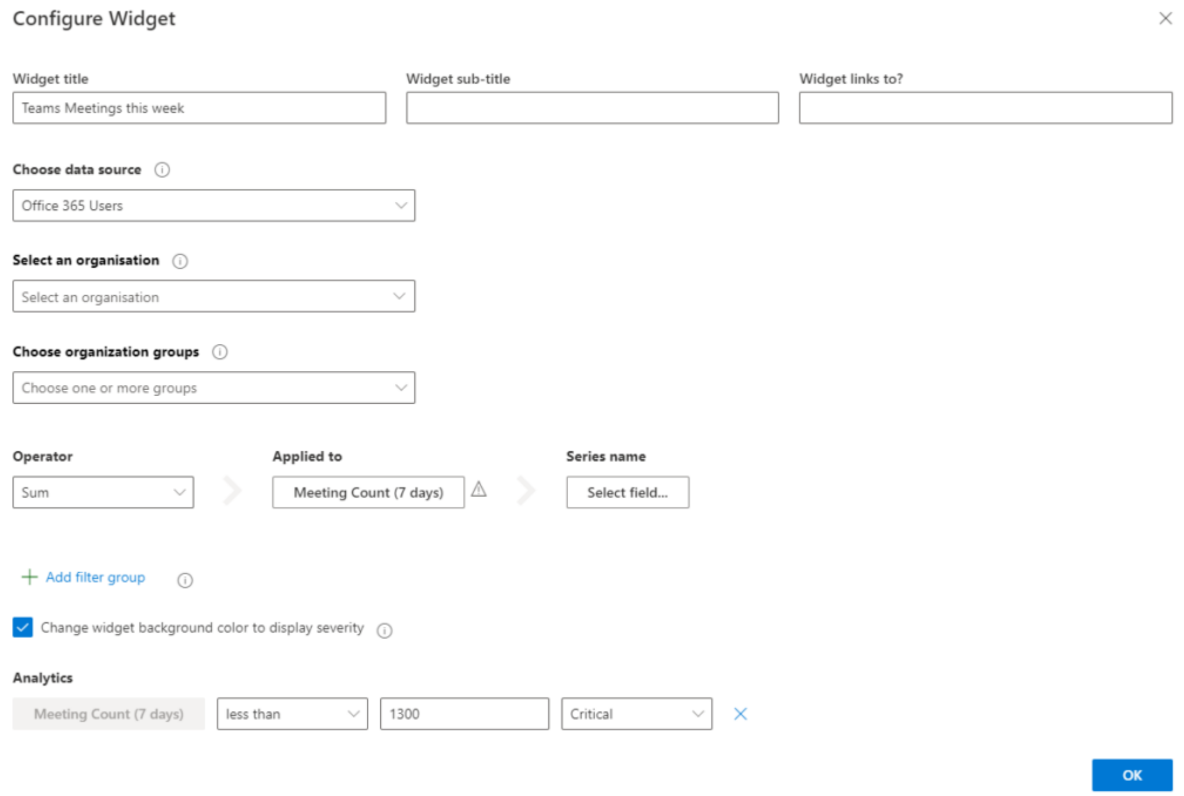
Check the image below for an example.

These analytics are immediately displayed on the dashboard, so you get this information quicker.

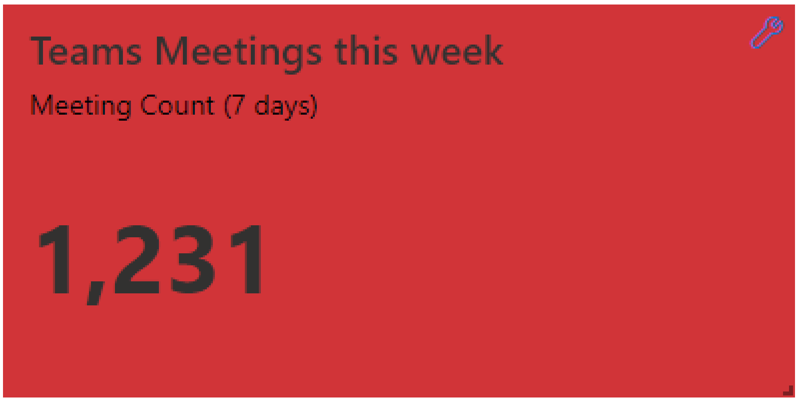
Adding a Card to the Dashboard

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.**
3. Click **Card Widget.**
4. Name your widget, and give it a sub-title if necessary.
5. Create your card as you would within the Report Center, 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.



NOTE: that 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.

Using the Report Metric Report in the Report Center

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 data is a gauge, as shown below. 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.

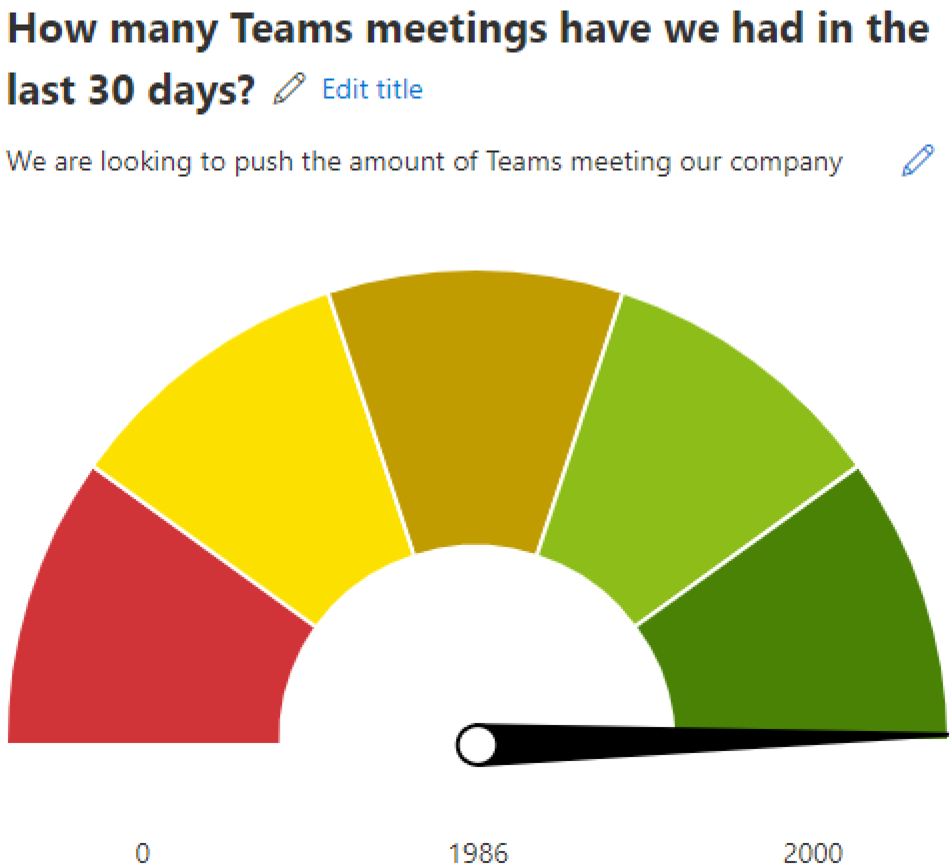
> **NOTE:** Your data sources need to be a numerical value. If you're looking for a report with information about departments, locations, license names, etc., select another report type. Check out this Report Center article for more information

Let's look at an example.

Report Example: How many Teams meetings did we have in the last 30 days?

For example, 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:

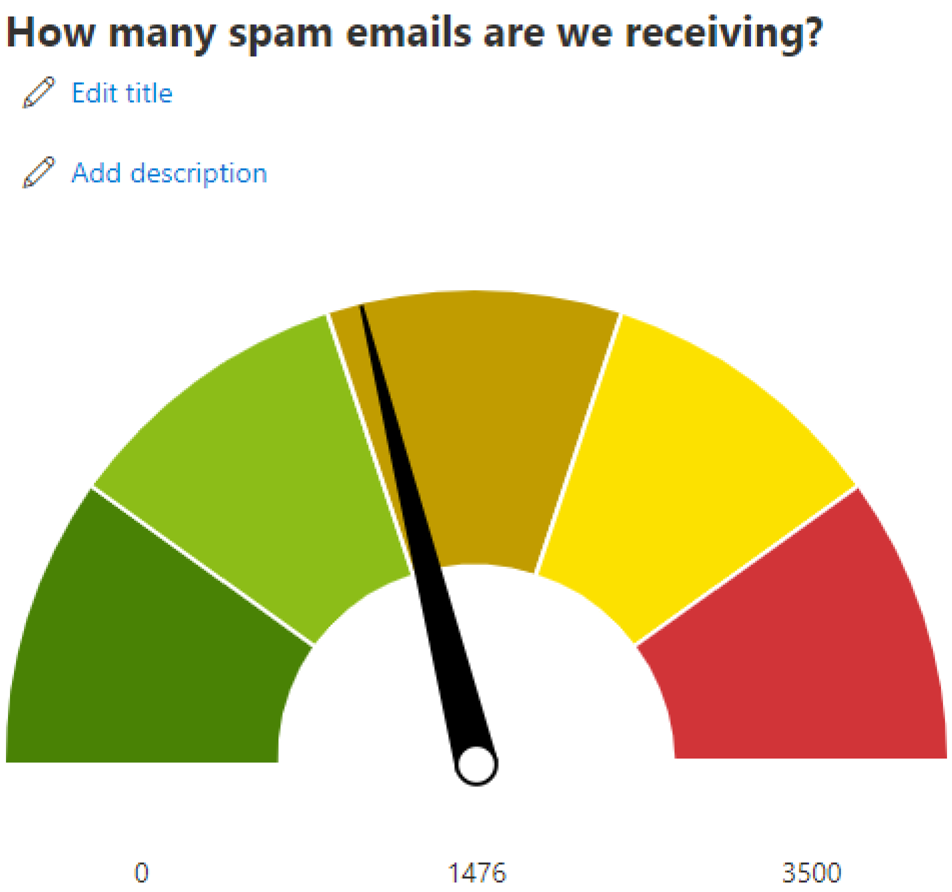
1. Open the Nova Report Center and create a new report.
2. Add a title and a description, if necessary.
3. Click **Metrics**.
4. For your data source, click **Office 365 Users.**
5. For select chart type, click **Gauge.**
6. For select operator, click **Sum.**
7. For **choose applied to**, select **Meeting count (30 days)** under the Teams User Activity Aggregate category.
8. 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.
   - **Note:** You may need to increase your maximum value to show your data.
9. Ensure the Reverse Colors checkbox is selected.
10. Close the section. Your report should now appear as a section.



Report Example: How many spam emails are we receiving?

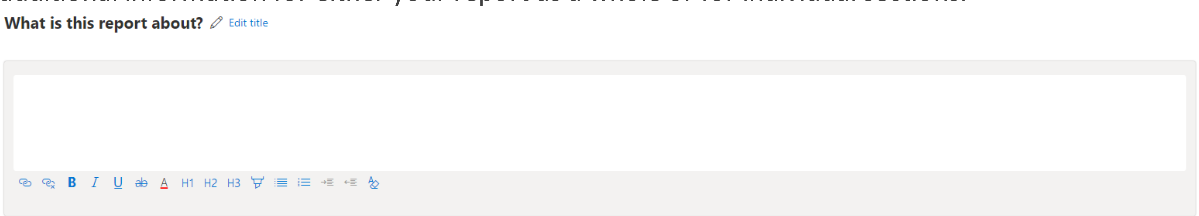
Perhaps you are looking to get a clear metric on how many spam emails are coming in to your tenant, with a limit on what is acceptable. This metric gives a clear image on whether this limit is being reached. To create it:

1. Open the Nova Report Center and create a new report.
2. Add a title and a description, if necessary.
3. Click **Metrics**.
4. For your data source, click **Office 365 Mail Traffic.**
5. For select chart type, click **Gauge.**
6. For select operator, click **Count.**
7. For choose applied to, select **Inbound Spam Content Filtered** under the Office 365 Mail Traffic category.
8. Set your minimum and maximum numbers. Your maximum number in this example should be the number of spam emails your administrator deems as acceptable.
    - **Note:** You may need to increase your maximum value to show your data.
9. Ensure the Reverse Colors checkbox is not selected.
10. Close the section. Your report should now appear as a section.



Using Text in Nova Report Center

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.



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

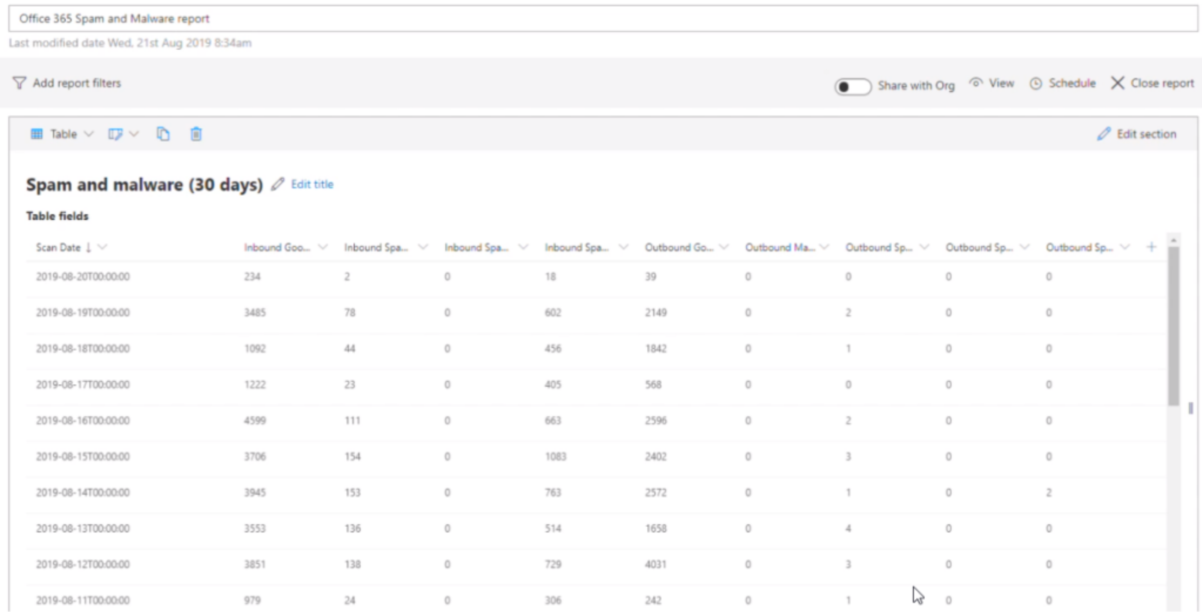
- adding hyperlinks to words or phrases. Add additional links to external information.
- use headers to highlight different sections.
- use numbered lists or bullet points

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

Custom Report Examples

We’ve got several sample reports which will help you get a feel for what can be done in the Nova Report Center. Here they are:

Shows spam and malware over a period of time.



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

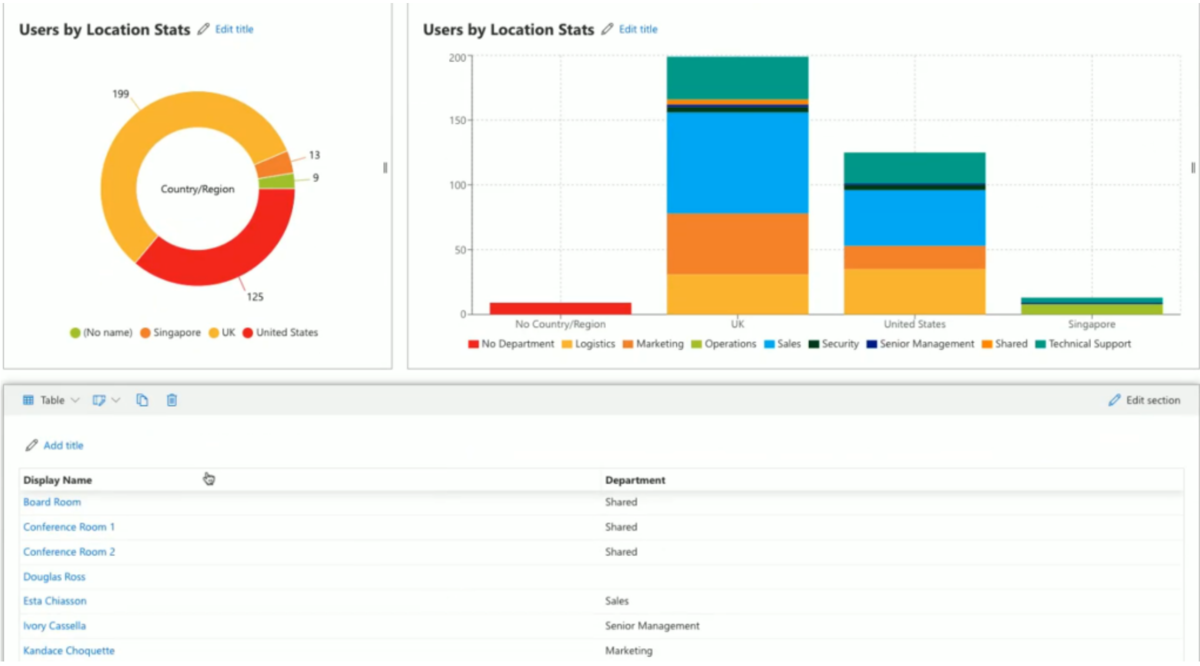
Spam and malware (30 days) Edit title

Table fields

Scan Date	Inbound Goo...	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

Office 365 spam and malware.

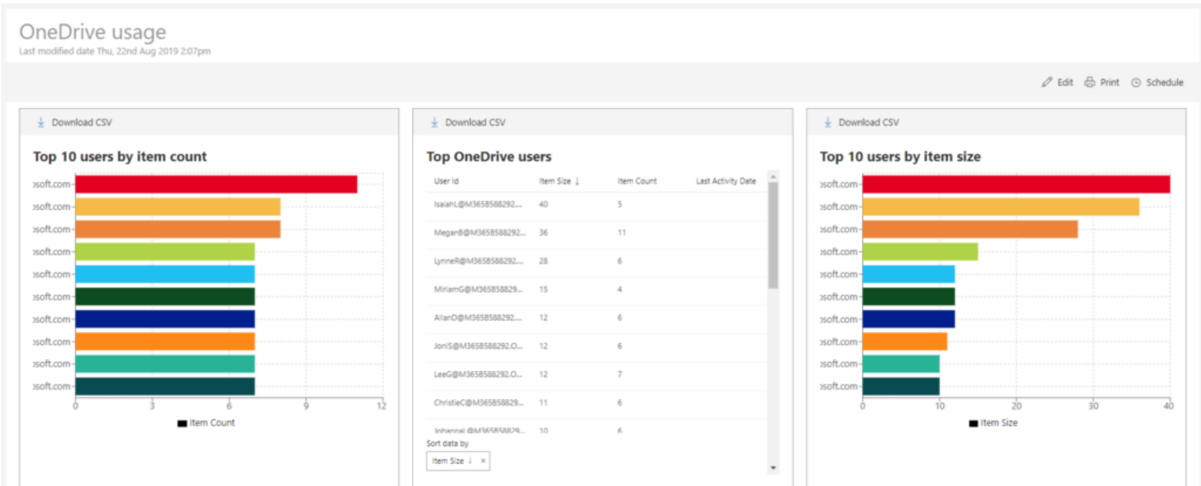
Shows users by their geographical location



\

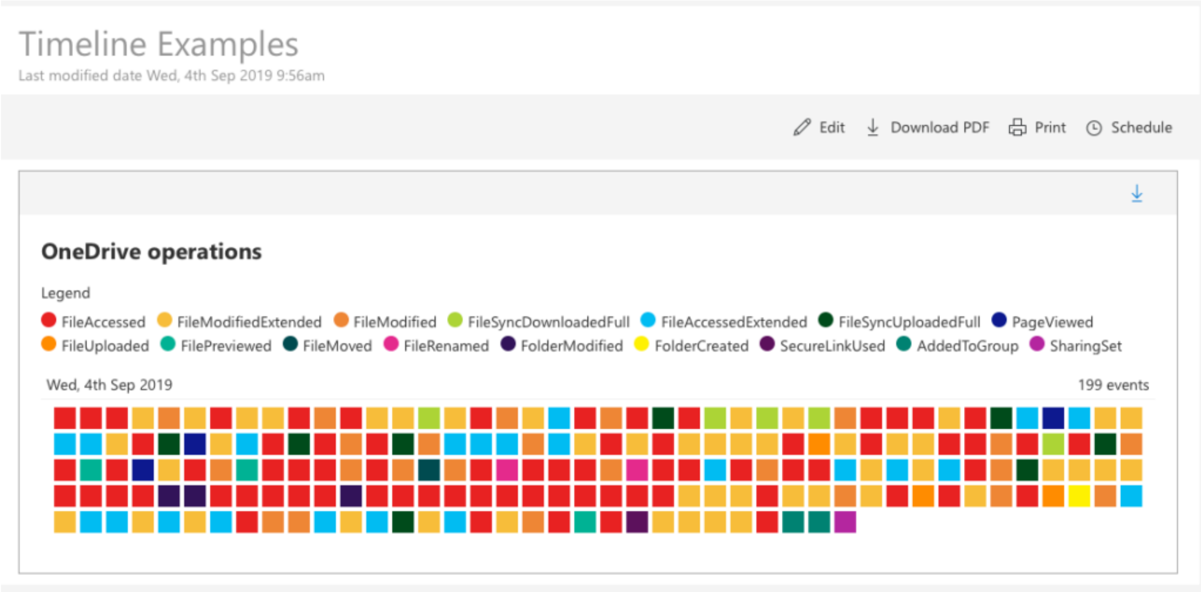
User by location

Shows how users are using OneDrive for Business



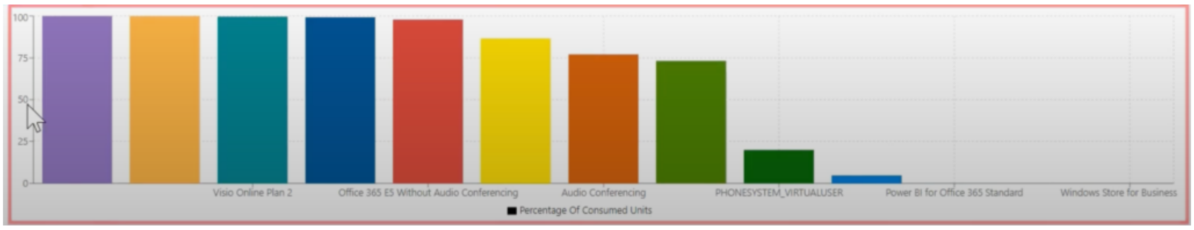
OneDrive usage

A timeline of operations and activities that have been performed by users in OneDrive for Business



OneDrive timeline

Shows licenses used over a period of time.



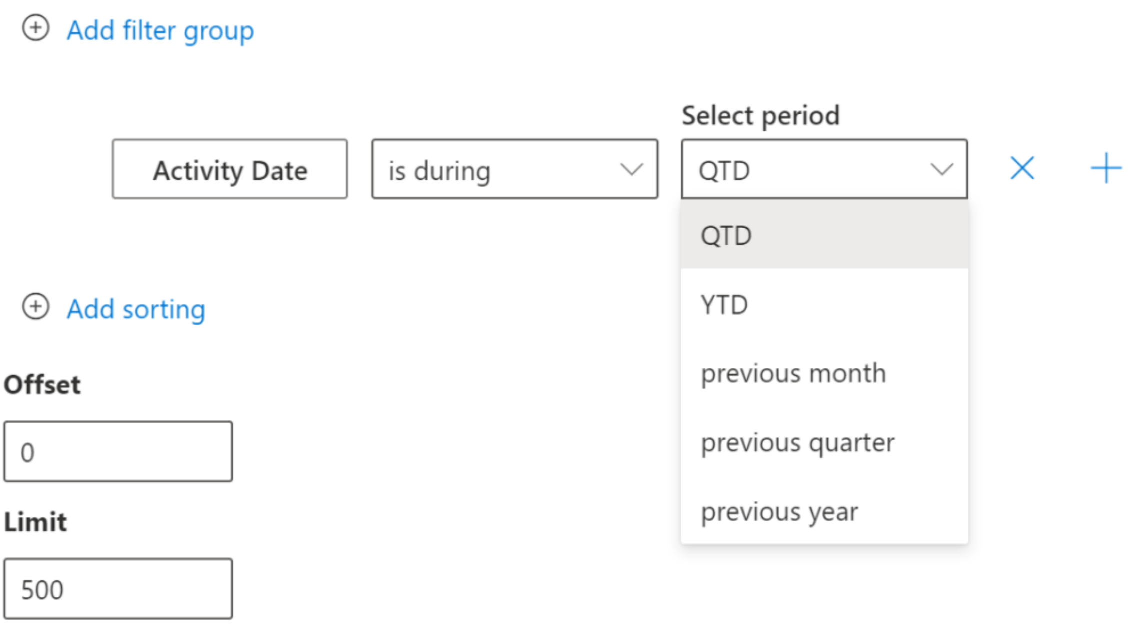
License utilization

Shows licenses consumed over a period of time, but in a tabular format

The date of the statistics snapshot ↓	License Name	Assigned Units
2020-08-11	Power Bi Pro	5
2020-08-10	Power Bi Pro	5
2020-08-09	Power Bi Pro	5
2020-08-08	Power Bi Pro	5
2020-08-07	Power Bi Pro	5
2020-08-06	Power Bi Pro	5
2020-08-05	Power Bi Pro	5
2020-08-04	Power Bi Pro	5

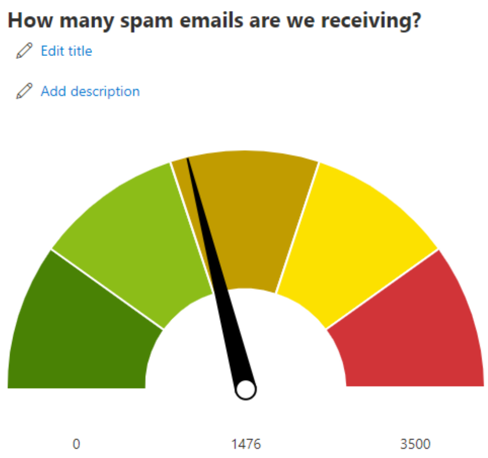
License utilization

Search by Quarter to Date (QTD) or Year to Date (YTD) in table data with date-specific fields.



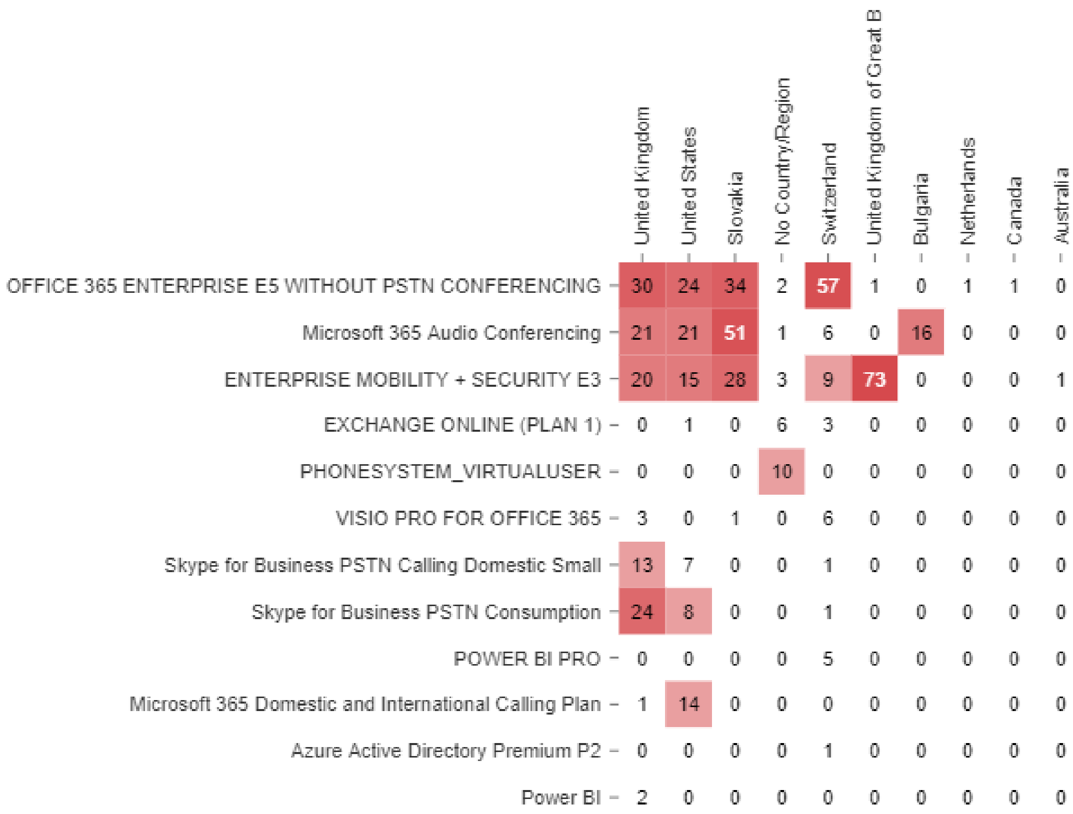
Search within QTD/YTD parameters

Metric gauges allows you to see how you are tracking your goals and limits within your tenant.



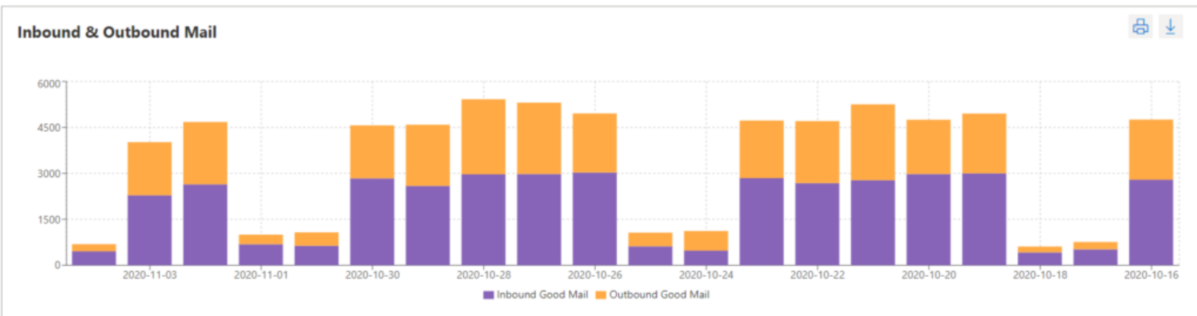
Using metrics

See which of your base licenses have been distributed by country in an easy-to-read heatmap.



License Assigned by Country Heatmap

View inbound and outbound mail statistics in one graph.



Inbound and Outbound Mail

Custom Report Example License Assigned by Country HeatMap

The heatmap shows a breakdown of all of your main base licenses distributed by country. The color coding helps you identify which license has been assigned to which country the most.

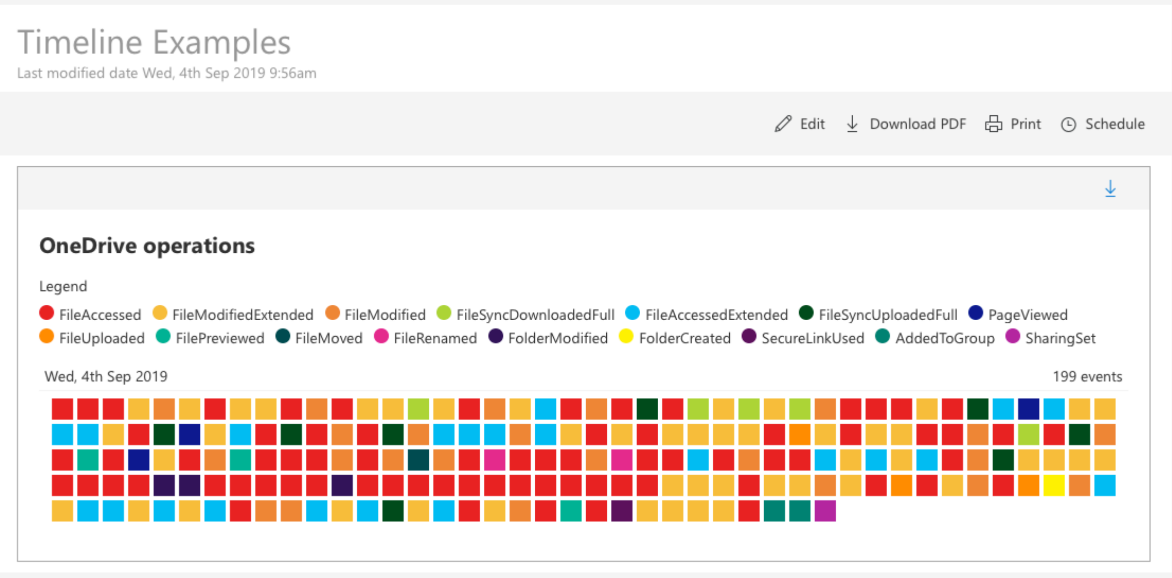
To create this report:

1. Create a new section.
2. Create a title and description, if necessary.
3. For your data source, choose **Office 365 Users.**
4. Select your organization and organization group, if necessary.
5. For your chart type, select **Heatmap.**
6. For operator, select **Count.**
7. For applied to, select **Licenses Applied to User**
8. For series name, select **License Set.**
9. For category, select **Country/Region.**
10. For a filter group, choose **License Set** then **is not empty.**
11. Set your offset and limits.
12. For your drill down fields, select **Company, Country/Region, Department** and **Display Name.**
13. Your data should now appear as a heatmap. Click close section.

	United Kingdom	United States	Slovakia	No Country/Region	Switzerland	United Kingdom of Great B	Bulgaria	Netherlands	Canada	Australia
OFFICE 365 ENTERPRISE E5 WITHOUT PSTN CONFERENCING	30	24	34	2	57	1	0	1	1	0
Microsoft 365 Audio Conferencing	21	21	51	1	6	0	16	0	0	0
ENTERPRISE MOBILITY + SECURITY E3	20	15	28	3	9	73	0	0	0	1
EXCHANGE ONLINE (PLAN 1)	0	1	0	6	3	0	0	0	0	0
PHONESYSTEM_VIRTUALUSER	0	0	0	10	0	0	0	0	0	0
VISIO PRO FOR OFFICE 365	3	0	1	0	6	0	0	0	0	0
Skype for Business PSTN Calling Domestic Small	13	7	0	0	1	0	0	0	0	0
Skype for Business PSTN Consumption	24	8	0	0	1	0	0	0	0	0
POWER BI PRO	0	0	0	0	5	0	0	0	0	0
Microsoft 365 Domestic and International Calling Plan	1	14	0	0	0	0	0	0	0	0
Azure Active Directory Premium P2	0	0	0	0	1	0	0	0	0	0
Power BI	2	0	0	0	0	0	0	0	0	0

Custom Report Example OneDrive Operations Timeline

Here's an example of a section on a custom report you could create using the Nova Report Center. You create a section on a report that shows OneDrive operations, color-coded per operation. Here's how the finished report section looks:



Here are the steps to create this report section:

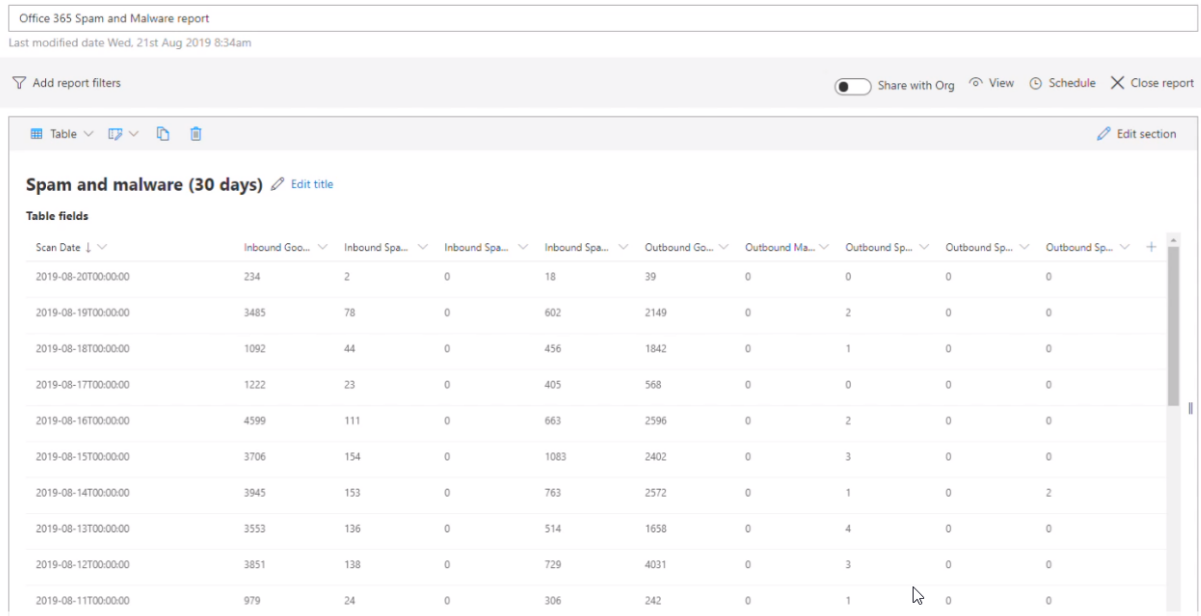
1. Click **Create Report**.
2. Enter a report title, for example *OneDrive Timeline*.
3. Click the plus sign to add a section to the report.
4. Click the **Timeline** section type to begin editing the section.
5. Choose the **Office 365 Audit Data** data source under the **Audit Data** data source category.
6. Choose and organization and group, if applicable.
7. Click the Select field... link under **Choose event title field**
8. Expand the Office 365 Users data source, and choose **Display Name.**
9. Click the Select field...link under **Choose event description field**.
10. In the Office 365 Audit Data data source, choose **Operation**.
11. Click the Select field... link under **Choose event date field**.
12. In the Office 365 Audit Data data source, choose **Creation Time**.
13. Click the Select field... link under **Choose event category field**.
14. In the Office 365 Audit Data data source, choose **Operation**.
15. Click the Select field... link under **Choose fields to show in detail view**.
16. Expand the Office 365 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).
17. In the drop-down list labelled **Choose view type**, select **Micro,** and enable the **Show legend** option.
18. Click **Add filter**.
19. Choose **Workload** is equal to **OneDrive.**
20. Click **Close section**.

21. Change the timeline section’s width to **Full**.
22. Click **Save**.

Here’s a video running through these steps:
https://youtu.be/eHSebVQoCK0

Custom Report Example: Office 365 Spam and Malware (30 Days)

Here’s an example of a custom report section you could create using the Nova Report Center. You 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’s sorted in descending order by scan date, and the results are filtered so only the last 30 days display. Here’s how the finished report section looks:



Scan Date ↓	Inbound Goo...	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

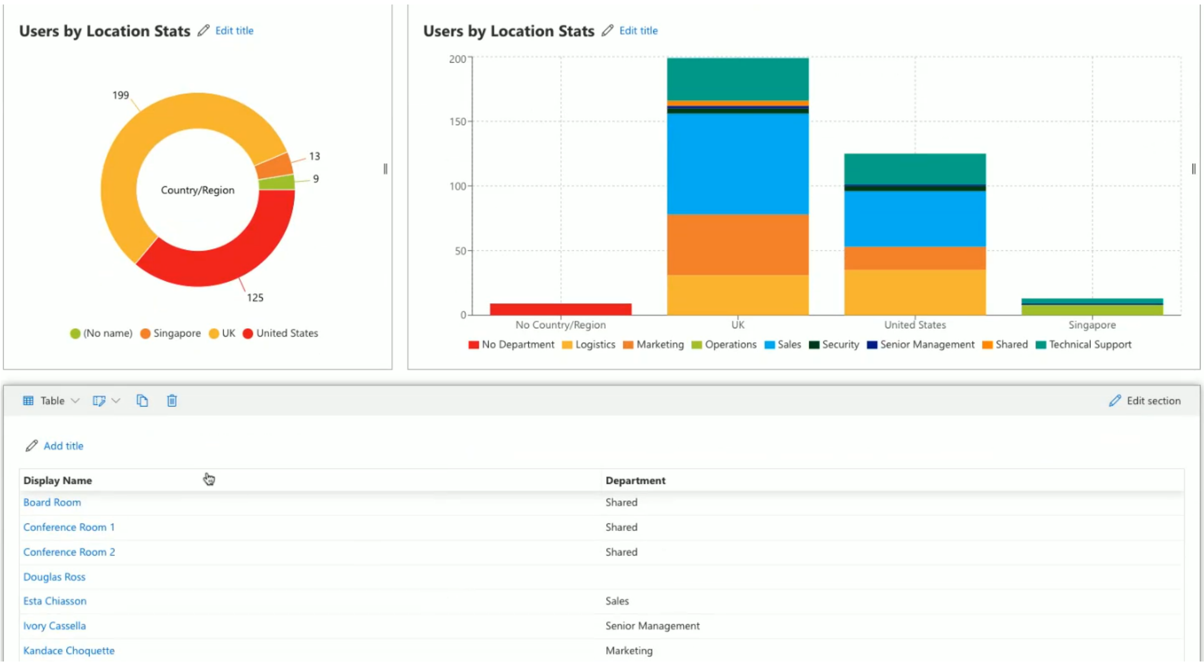
Here are the steps to create this report section:

1. Click **Create Report**.
2. Enter a report title, for example Office 365 Spam and Malware (30 days).
3. Click the plus sign to add a section to the report.
4. Click the **Table** section type to begin editing the section.
5. Choose the **Office 365 Mail Traffic** data source under the **Exchange Data** data source category.
6. Choose and organization and group, if applicable.
7. Click the **Select field…** link and select ALL fields, starting from **Scan Date** and work your way upwards. Then close the dialog.
8. Click **Add sorting**.
9. Click **Select field**.
10. Select **Scan Date**, and make sure descending is selected.
11. Enter 31 in the **Limit field**.
12. Click **Close** section.
13. Change the table section’s width to **Full**.
14. Click **Save**.

Here’s a video of these steps:
https://youtu.be/lGXrwlMQxyw

Custom Report Example: Office 365 Users by Location

Here’s an example of a custom report you could create using the Nova Report Center.
You can create an Office 365 Users by Location report. The report shows your organization’s Office 365 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 Office 365 Users data source. The report’s second section is a stacked bar graph with the Office 365 Users data source. Finally, the report contains a table which shows users’ display names, country/region and departments. Here’s how the finished report looks:



Here are the steps to create this report:

1. Click **Create Report**.
2. Enter a report title, for example *Office 365 Users by Location*.
3. You’ll add 3 sections to this report using the steps below:

Section 1: Users by Location Stats

1. Click the plus sign to add a section to the report.
2. Click the **Chart or Pivot** section type to begin editing the section.
3. Add a section title, for example *Users by Location Stats*.
4. Choose the **Office 365 Users** data source under the **User Data** data source category.
5. Choose and organization and group, if applicable.
6. Select the **Pie** chart type.
7. In the **Operator** field select **count**.
8. In the **Applied to** field select **Display Name.**
9. In the **Series name** field select **Country/Region**.

10. Click Close section.

Section 2: Users by Location and Department

1. Click the plus sign to add a section to the report.
2. Click the **Chart or Pivot** section type to begin editing the section.
3. Add a section title, for example *Users by Location Stats*.
4. Choose the **Office 365 Users** data source.
5. Choose and organization and group, if applicable.
6. Select the **Stacked Column** chart type.
7. In the **Operator** field select **count**.
8. In the **Applied to** field select **Country/Region**.
9. In the **Series name** field select **Country/Region**.
10. In the **Category** field select **Department.**
11. Click Close section.

Section 3: List of Users by Department

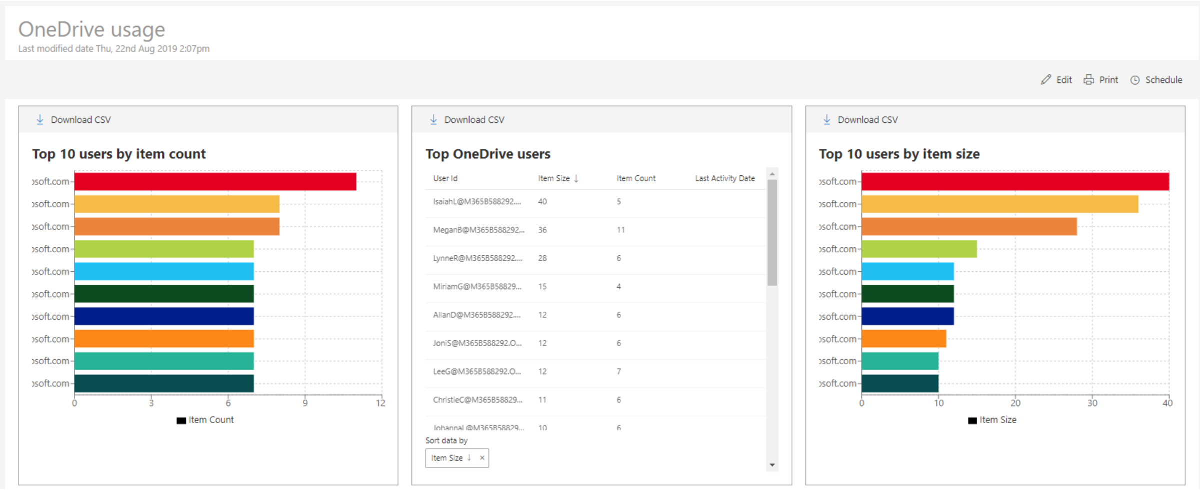
1. Click the plus sign to add a section to the report.
2. Click the **Table** section type to begin editing the section.
3. Add a section title, for example *Users by Department*.
4. Choose the **Office 365 Users** data source.
5. Choose and organization and group, if applicable.
6. Click the **Select 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.

After you're done adding sections, click Save.

And here's a video going through these steps:
https://youtu.be/abci7IAsN-U

Custom Report Example: OneDrive Usage

Here's an example of a custom report you could create using the Nova Report Center.
You 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). The report includes a vertical line bar graph with OneDrive User Data as the data source, sorted by item count (listed by user ID). The report includes a table that also uses OneDrive User Data as the data source. This table is sorted by item size. Finally, the report has another 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's how the finished report looks:



Here are the steps to create this report:

1. Click Create Report.
2. Enter a report title, for example OneDrive Usage.
3. You'll add 3 sections to this report using the steps below:

Section 1: Top 10 Users by Item Count

1. Click the **plus** sign to add a section to the report.
2. Click the **Chart or Pivot** section type to begin editing the section.
3. Add a section title, for example Top 10 Users by Item Count.
4. Choose the **OneDrive User Statistics** data source.
5. Choose an organization and group, if applicable.
6. Select the **Column** chart type.
7. Under the *Operator* section, select '**Sum**'.
8. Under the *'Choose applied to'* section, click **'Select field…'**, and click on the **'Item Count'** checkbox.
9. Under the *'Series name'* section, click **'Select field…**', and click the **'User ID'** checkbox.
10. Click the **Add sorting** link.
11. Click the **'Select field…'** link, and click the **'Item Count'** button.
12. Sort in descending order.
13. Under the '**Offset**' text field, put 0.
14. Under the '**Limit**' text field, put 10.
15. Un-check the '**Overflow**' button.
16. Click Close section.

Section 2: Top OneDrive Users

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 Top OneDrive Users.
4. Choose the **OneDrive User Staistics** data source.
5. Choose and organization and group, if applicable.
6. Click '*Select field…*', and select **User ID**, **Item Size**, **Item Count**, and **Last Activity Date** in this order, and then close the dialog.
7. If desired, drag and drop the columns, to re-order them.
8. Click the **Add sorting** link.
9. Click the '*Select field...*' link, and then select **Item Size**.

10. 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.
11. Click Close section.

Section 3: Top 10 Users by Item Size

1. Click the **plus** sign to add a section to the report.
2. Click the **Chart or Pivot** section type to begin editing the section.
3. Add a section title, for example Top 10 Users by Item Count.
4. Choose the **OneDrive User Statistics** data source.
5. Choose an organization and group, if applicable.
6. Select the **Column** chart type.
7. Under the *Operator* section, select '**Sum**'.
8. Under the '*Choose applied to*' section, click '**Select field…**', and click on the '**Item Size**' checkbox.
9. Under the '*Series name*' section, click '**Select field…**', and click the '**User ID**' checkbox.
10. Click the **Add sorting** link.
11. Click the '**Select field…**' link, and click the **'Item Size'** button.
12. Sort in descending order.
13. Under the '**Offset**' text field, put 0.
14. Under the '**Limit**' text field, put 10.
15. Un-check the '**Overflow**' button
16. Click Close section.

After you're done adding sections, click Save.

Watch the video below to see the above steps in action.
https://youtu.be/jPKvZVSbUv4

Custom Report Example: License Utilization Report

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 aren't being used i.e. disabled/deleted users

Below are the steps on how to something

1. Click **Create Report**.
2. Enter a report title, for example License Utilization.
3. Click the plus sign to add a section to the report, and a description if desired.
4. Add a title and description for your section.
5. Choose the **Tenant License History** data source under the **License Data** data source category.
6. Click **column**.
7. Under operator. choose **Average.**

8. Under **Applied to**, choose **Percentage of Consumed Units.**
9. Under **Series name**, choose **License Name.**
10. Set your offset and limits if necessary.
11. Save, then close the section.

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’s see how we do that below:

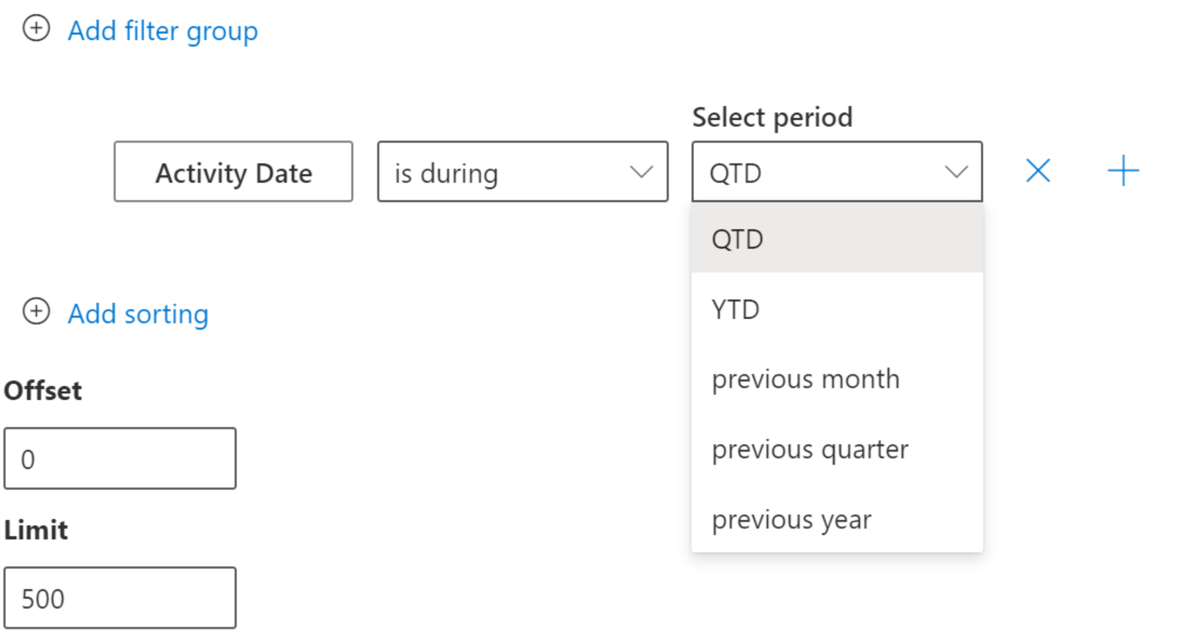
1. Click **Create Report**.
2. Enter a report title, for example License Utilization Table.
3. Click the plus sign to add a section to the report, and a description if desired.
4. Add a title and description for your section.
5. Choose the **Tenant Licenses** data source under the **License Data** data source category.
6. Click **table**.
7. 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
8. Set your offset and limits if necessary.
9. Save, then close the section.

Video example

Check out a video on how to create this report below.
https://youtu.be/XEFmOeuEbx8

Custom Report Example: Search Within Quarter to Date (QTD) or Year to Date (YTD) Parameters

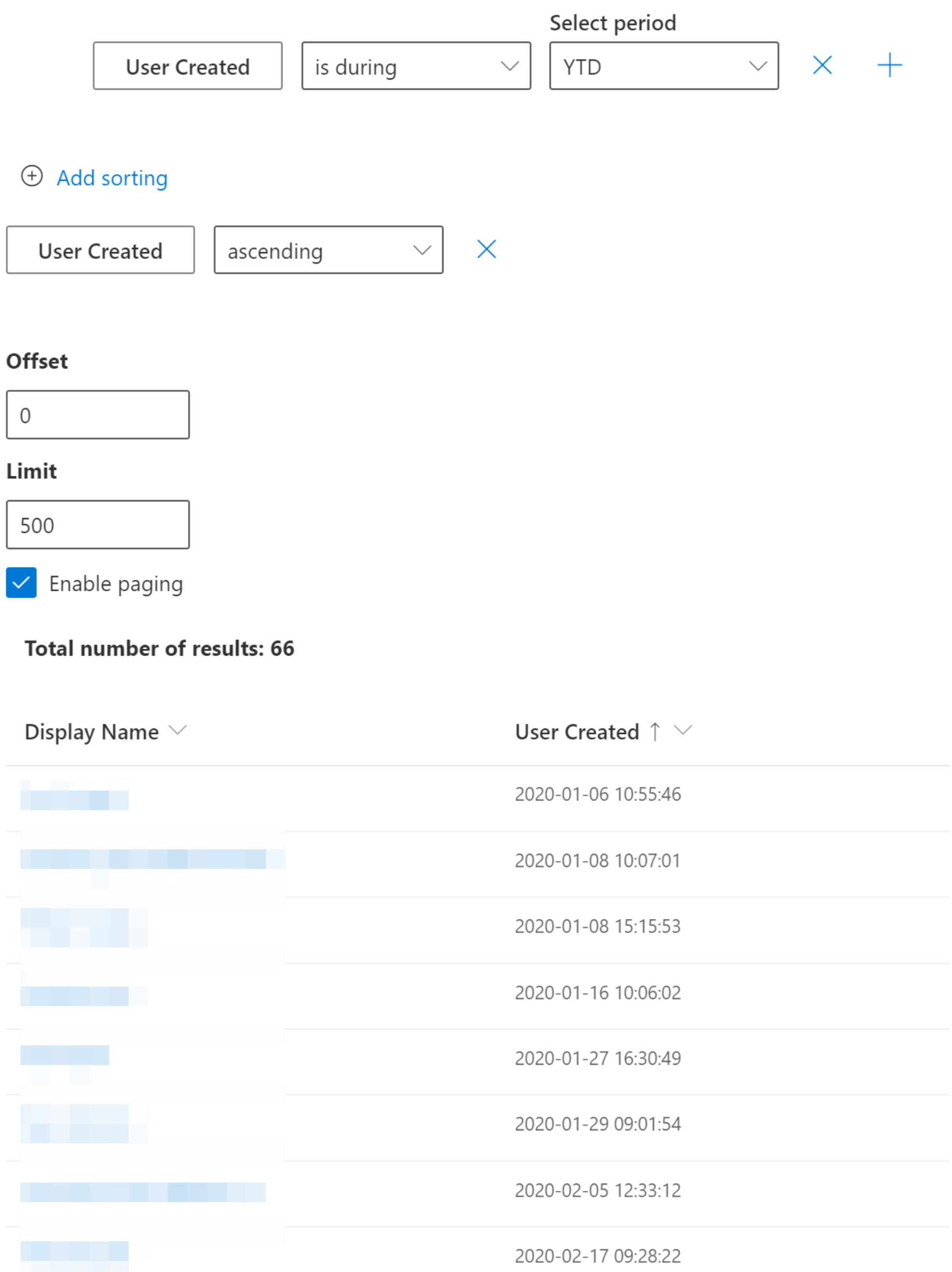
It is now possible to search within Quarter to Date (QTD) and Year to Date (YTD) metrics within the Nova Report Center for date-specific data fields.



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 Azure AD users created within the current year within your tenant. To do this:

1. Begin by creating a new report, including title and description if necessary.
2. Choose your data source. For these specific filters, you will need sources that include date data fields. For our example, we're using **Office 365 Users**.
3. For **Table fields**, choose **Display Name** and **User Created**.
4. Under **Add filter group,** select **is during**, then **YTD.**
5. Add sorting and change your offset and limits if required.

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



Custom Report Example: See 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.

How to create this report

1. Click **Create Report**.
2. Enter a report title, for example Power BI licenses over time.
3. Click the plus sign to add a section to the report, and a description if desired.
4. Add a title and description for your section.
5. Choose the **Tenant License History** data source under the **License Data** data source category.
6. Click **table**.
7. Under **Select fields,** choose:
    - The date of the statistics snapshot
    - License Name
    - Assigned Units
8. 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.**
9. On **Select field**, choose **License Name**.
10. On **Select operator**, choose **contains.**
11. 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.*

12. Enter your offset and limits (see below).
13. Sort the date in ascending or descending order, depending on your preference.
14. Save your report.

Your table should look a little like the one below.

The date of the statistics snapshot ↓	License Name	Assigned Units
2020-08-11	Power Bi Pro	5
2020-08-10	Power Bi Pro	5
2020-08-09	Power Bi Pro	5
2020-08-08	Power Bi Pro	5
2020-08-07	Power Bi Pro	5
2020-08-06	Power Bi Pro	5
2020-08-05	Power Bi Pro	5
2020-08-04	Power Bi Pro	5

Offset & Limits

Your offset and limits refer to the **dates** of your table. For example, if you wanted a table representing the previous 14 days, enter **14** into your limits box.

You can go back days, weeks, months or even years depending on your needs.
https://youtu.be/sl4voT6I1Ow

Overview of Schedule Center

The Schedule Center page shows a list of scheduled reports in your current tenant. On this page, you can:

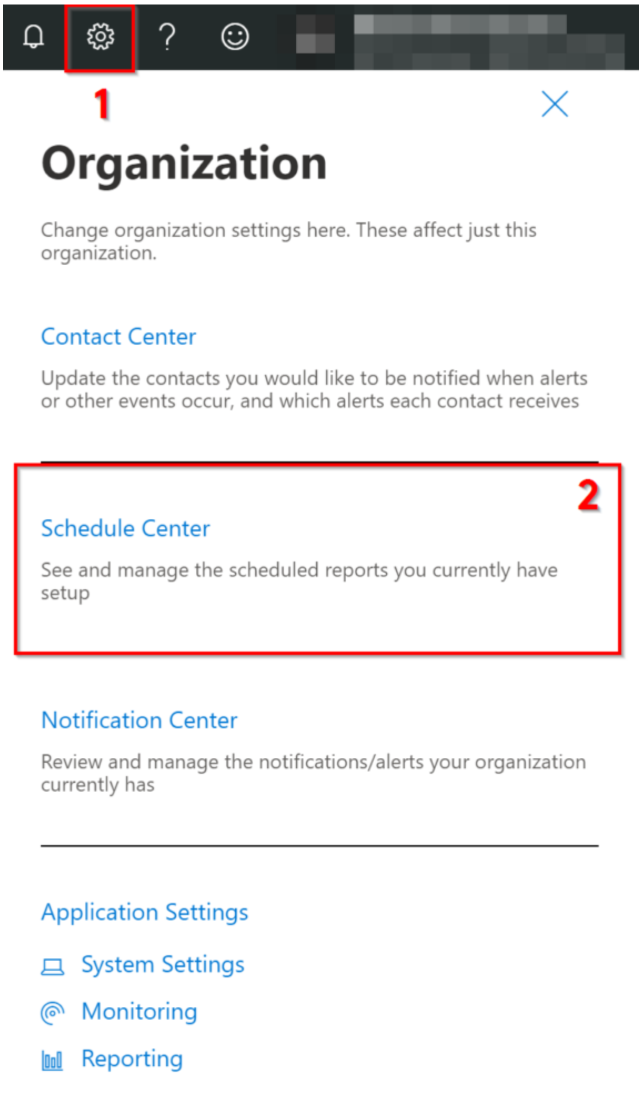
- Edit a report schedule.
- Run a report now.
- Delete a report schedule.
- Duplicate a report schedule so that another copy can be configured in a different way.

Click here to learn more.

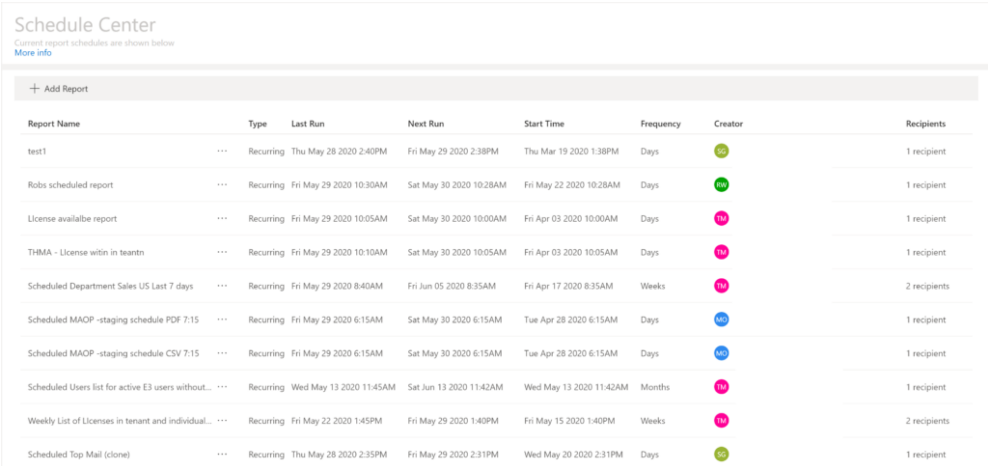
Schedule Center

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.

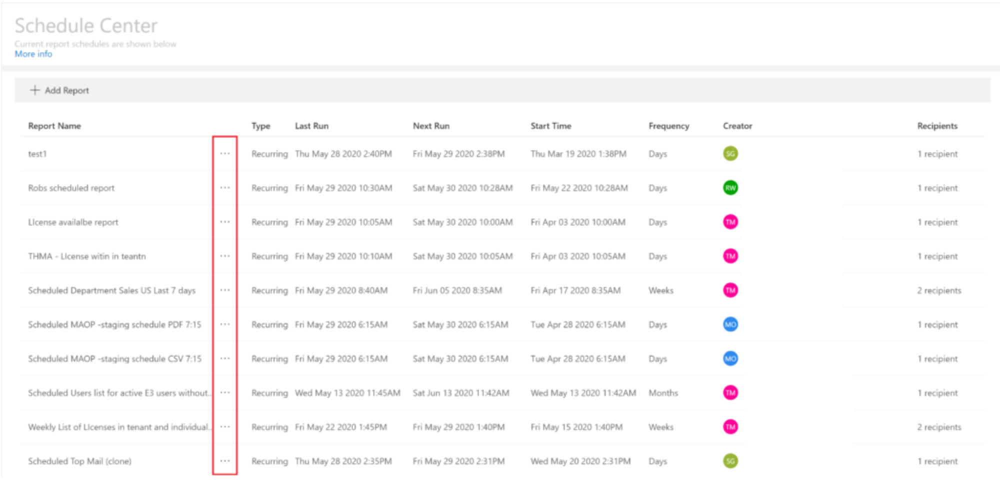
To access the Schedule Center, click the Settings button (a gear) located in the top right of the Nova window, and then select Schedule Center, as shown below.

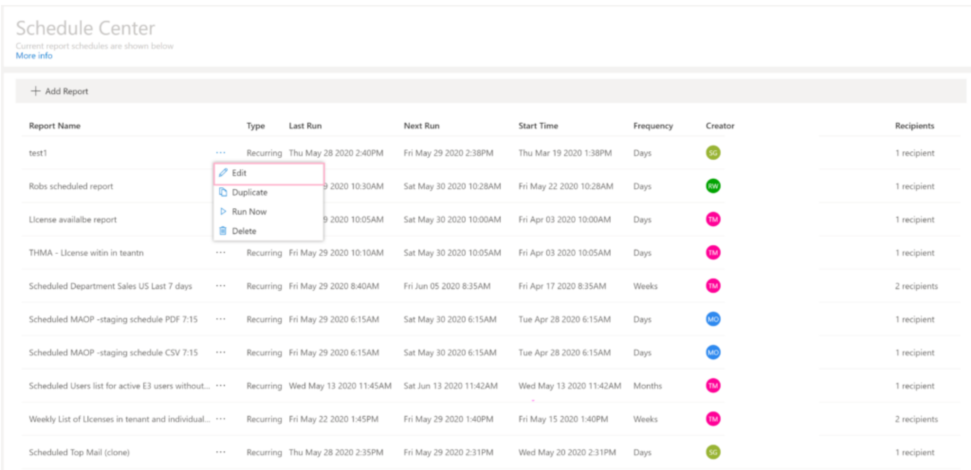


It shows a list of previously scheduled reports, as shown below.

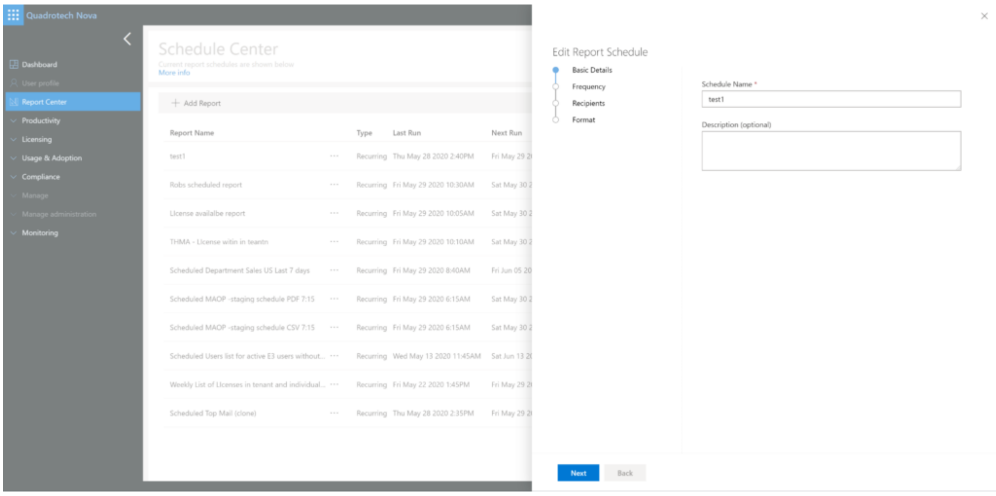


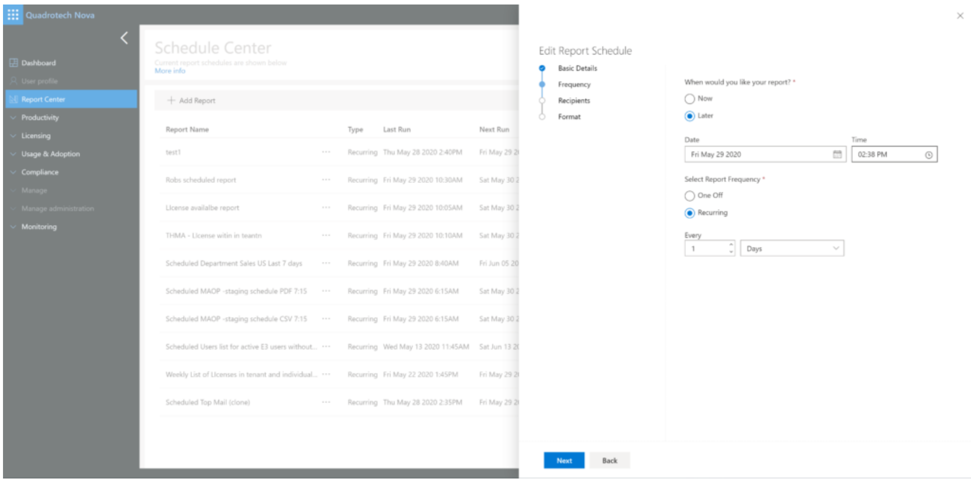
You'll notice an ellipsis next to each scheduled report. Use the Edit button to change a report schedule, as shown here:

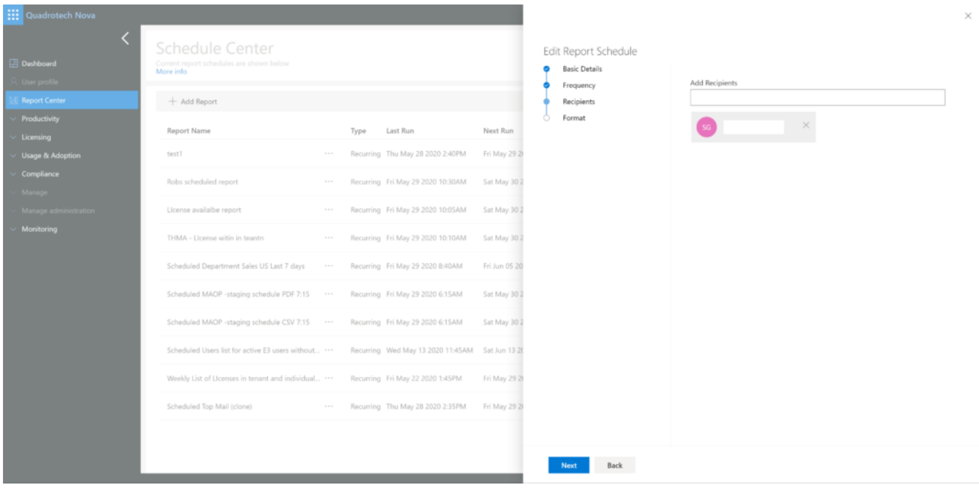


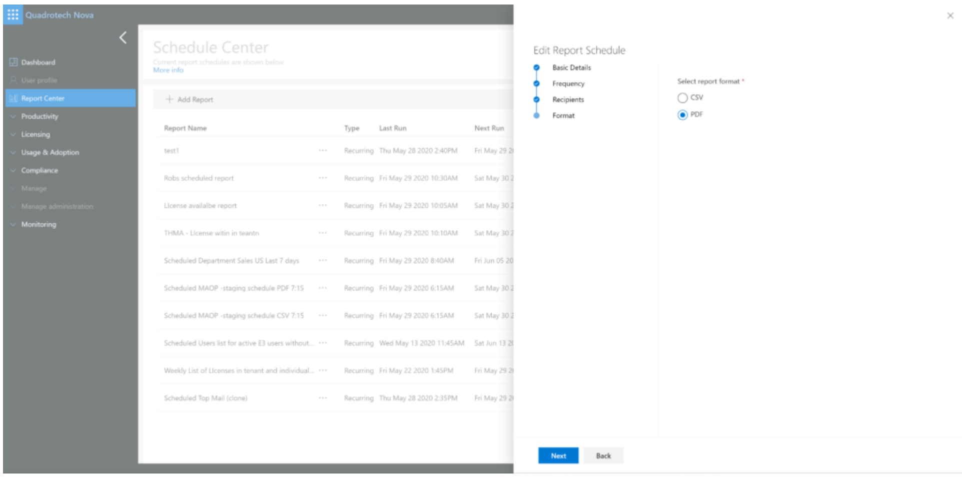


This will bring you to the schedule screen, as seen in the images below.


Quadrotech Nova
Schedule Center
Edit Report Schedule
Basic Details
Frequency
Recipients
Format
Schedule Name *
test1
Description (optional)
Next
Back


Quadrotech Nova
Schedule Center
Edit Report Schedule
Basic Details
Frequency
Recipients
Format
When would you like your report? *
Now
Later
Date
Fri May 29 2020
Time
02:38 PM
Select Report Frequency *
One Off
Recurring
Every
1
Days
Next
Back


Quadrotech Nova
Schedule Center
Edit Report Schedule
Basic Details
Frequency
Recipients
Format
Add Recipients
Next
Back



Additionally, using the other buttons, you can:

- Duplicate a report schedule. Then you can edit the duplicate, so it maybe runs on a different schedule and/or it's sent to different recipients.
- Run a report now.
- Delete a report schedule.

A video regarding the Schedule Center can be seen below:
https://youtu.be/EGoiinNS7Z8

6

TMS

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.

Here's a video overview of the TMS user interface:
https://youtu.be/Y-zcGw43z4A

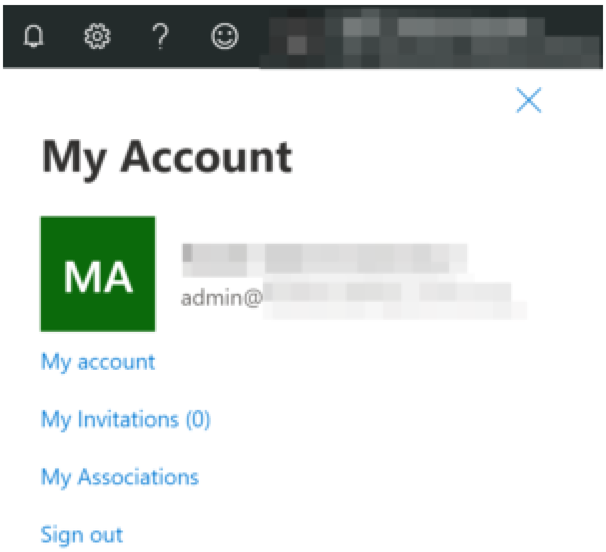
This article explains how to manage customer tenants and add tenant administrators.

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're managing a lot of tenants, or if some of your customers have multiple tenants, you might need to organize the tenants into organization groups. Keep reading to learn how to manage customer tenants. Here's 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 Office 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.

Here's a video showing how to add and manage customer tenants:
https://youtu.be/ssWojgua72U

Adding a Tenant Administrator

You'll 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'll 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.

NOTE: If the invited user doesn't receive an email, check the contents of any junk mail folder.

Here's a video showing this process:
https://youtu.be/CKFlkYZ_Cpg

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're managing several tenants, you might want to organize them into groups using the Organization Groups page.a

Change the Service Account Password in TMS

Overview

This article explains how you can correctly change the service account password for Nova Reporting. We recommend that you do this on a regular basis to ensure continued security within your environment.

Details

If you need to change the password, you'll need to make the change first in two places:

- Office 365 Admin Portal
- Tenant Management System Client (TMS Client)

Office 365 Admin Portal

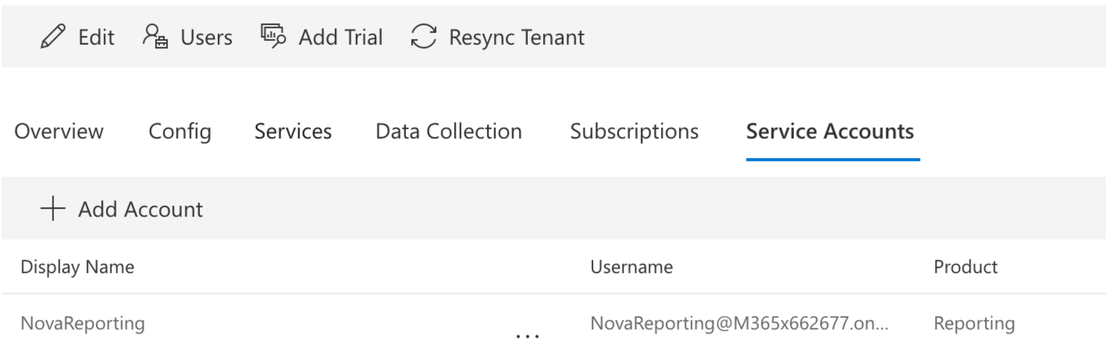
To change your password for the service account:

1. Log into your Microsoft Office 365 portal as an Administrator.
2. Go to the **Admin Center.**
3. Select **Active Users***,* click **Search** and type in the name of the service account.
4. Select the user and chose **Reset Password.**

> **NOTE:** ensure that you **DO NOT** select **require this user to change their password when they first sign in.**

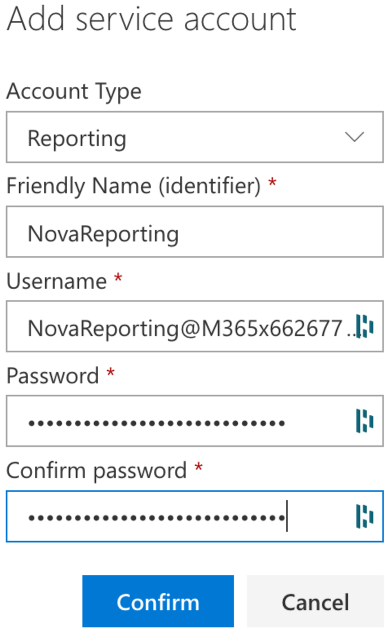
Tenant Management System Client

1. Once you have the password, log into the Tenant Management System Client (TMS Client)
2. Navigate to the **Service Accounts** tab:



3. Click on the ellipsis and select **edit.**

4. Add a new password to the **password** field and the do the same to the **Confirm password** field.



5. Click **Confirm** to update the password for service account.

Note

Please note that normally this password will expire after a few days. We advise to mark this date and update the SA password before this happens.
If your company policy allows to use the password without an expiration, please refer to the following article for instructions and use this option for the service account password.

Reporting Provisioning from TMS

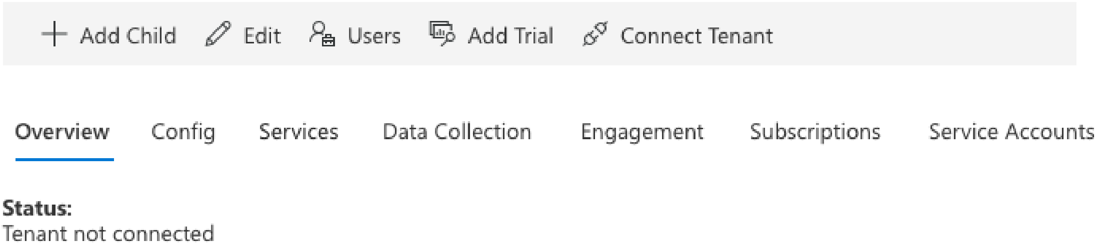
Overview

Radar and the 'Data Storage' needed for Nova share a common backend and data collection framework. This should now be provisioned for an organization/tenant via the Tenant Management System Client (TMS Client). For Quadrotech's direct customers, this is available at https://account.quadro.tech.

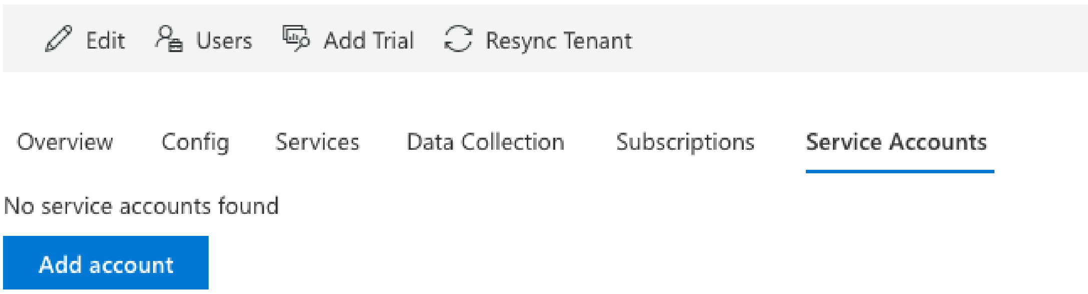
Steps

1. Connect the tenant. When you create an organization, by default it does not have an Azure Tenant assigned to it. If a user logs in with AAD and that tenant is identified as the default, and that user is not attached to any other tenant, then the Azure Tenant details will be captured. To manually connect the tenant, click the 'Connect Tenant' button on the organization, and authorise the Azure Application that appears. Note: This will then connect the tenant and

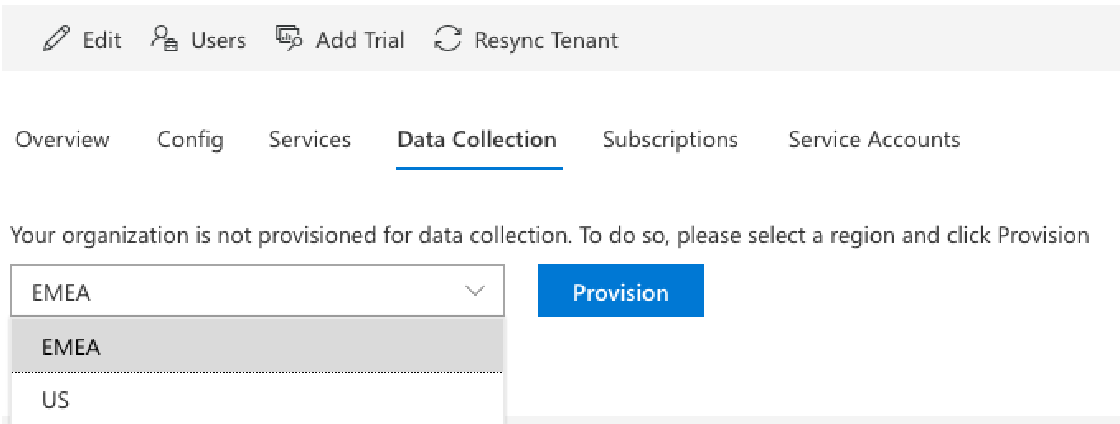
assign the correct white label identifiers to the tenant. This tenant can then be used by Data Collection and DPC.



2. Add a Service Account. You need to add at least one working service account on the Service Accounts tab in TMS. The requirements for the service account can be found in this section.



3. Provision the Data Collection Instance. On the Data Collection tab, if the instance is not provisioned, you will be able to select a region and click the ‘Provision’ button. Within 2-4 hours you should see Jobs running and completing on this Data Collection tab in the table.



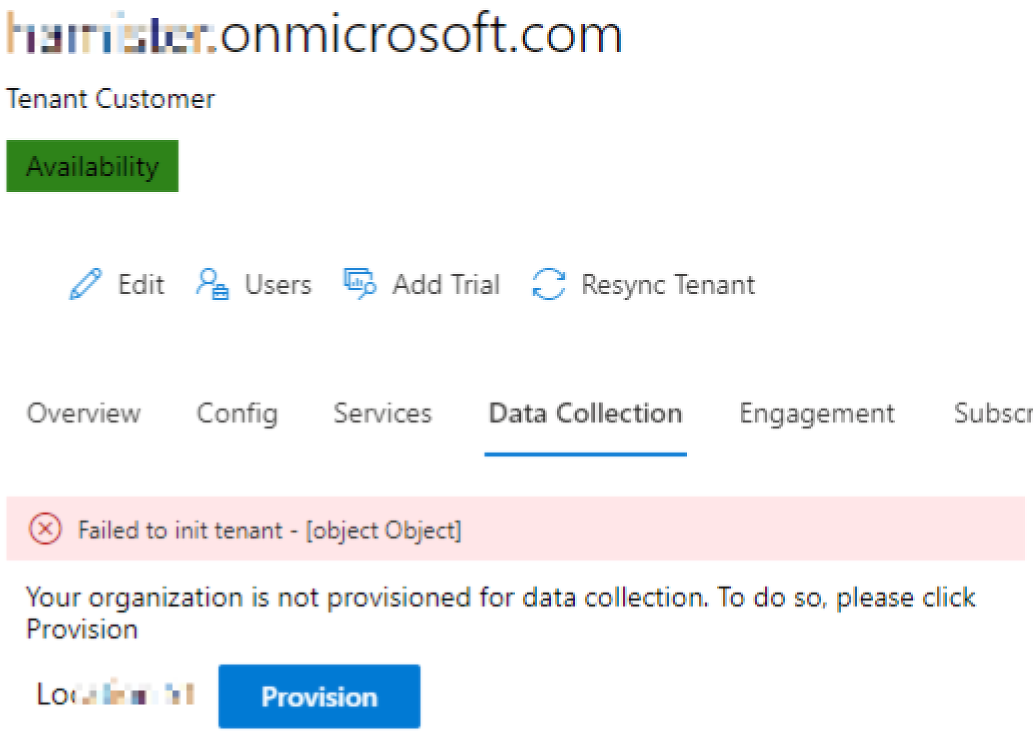
Once this process is complete, both Data Collection and Radar are provisioned.

Reference

Requirements for Service account for Reporting

TMS Problem With OnBoarding

Sometimes if TMS is used to onboard several customer tenants in sequence you might encounter an error.
The errors/issues include problems with connecting a tenant, provisioning, and so on. An example error is shown below:



The error message in the above screenshot says: failed to init tenant
This type of issue has been seen when a tenant is provisioned, then another then another tenant, and then another, and so on. There is no hard number of successes before a failure may occur.
To work around this issue refresh (F5) the browser. Alternatively use incognito/private browsing mode when provisioning tenants.

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’s 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

Adding Additional Service Accounts for Nova

Microsoft Office 365 implements a series of throttling policies on Office 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 Office 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 Office 365 tenant. These service accounts do not require a Microsoft Office 365 License which means that taking advantage of this feature does not add any cost to your Office 365 subscription.

Getting Started

Before we begin, you must create some additional accounts within your Office 365 environment with the correct permissions.
For simplicity, we recommend that these service accounts are named as follows:
NovaReporting@<domain>.onmicrosoft.com
NovaReporting1@<domain>.onmicrosoft.com
NovaReporting2@<domain>.onmicrosoft.com
etc

To create the service accounts for reporting, please follow the steps outlined at this section.

To create the service accounts for DPC, please follow the steps outlined at this section.

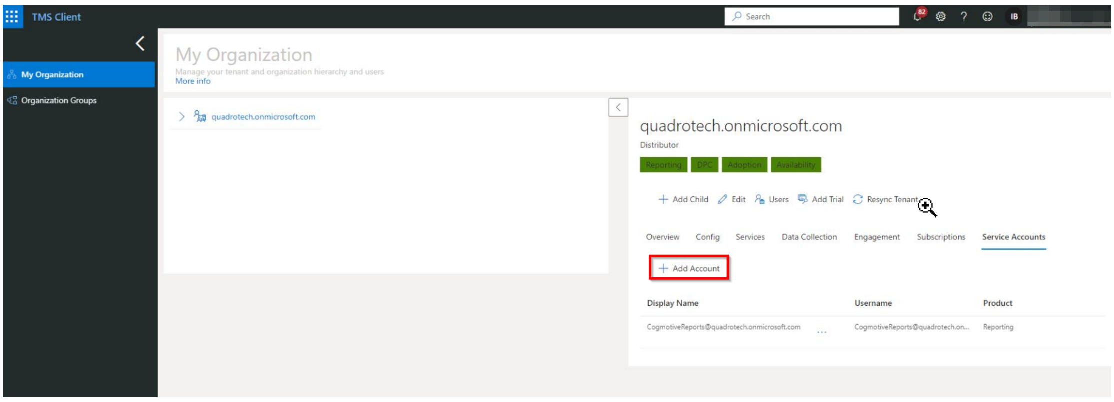
NOTE: If you are using the SharePoint Online Reports module, you will also need to give this account the correct permissions to the SharePoint Online Site Collections you are reporting on – you can find the steps to do so at this article.

Alternatively, you can create a Security Group in Office 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 in Nova,

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 article on service accounts in Nova can be found here.

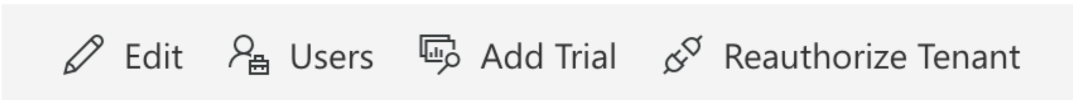
Reauthorize a Tenant in Nova

Overview

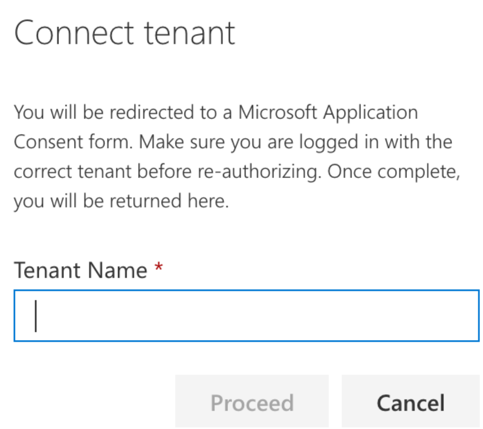
The cloud world is changing constantly, and so is the data flowing through it. Nova is provisioned with set of authorizations, and if the data is changed, the authorization needs to be changed also. This KB describes how it can be done via the Tenant Management System Client (TMS Client). For Quadrotech’s direct customers, this is available at https://account.quadro.tech.

Steps

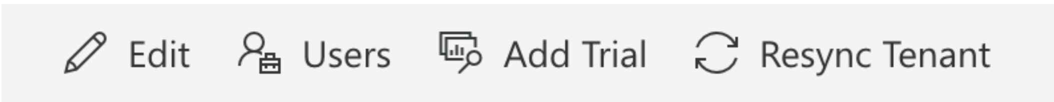
1. Login to Tenant Management System Client (TMS Client) with an account with a System Administrator role.
2. Select the organization you want to reauthorize and click **Reauthorize Tenant.**



3. Enter the full tenant name in an opened window (e.g. myTenant.onmicrosoft.com) and click **Proceed.**



4. Login with a Global Administrator account and provide consent.
5. If everything is completed correctly, the Reauthorize Tenant button will be re-named to **Resync Tenant.**



NOTE:
When re-authorization is granted, the button will be re-named to **Resync Tenant**. It has these functions:

1. It validates that the connection to the Tenant is still good for App Authorization.
2. It generates the list of domains again.
3. It will update the number of mailboxes and licensed mailboxes.

The endpoint for Teams has been changed and re-authorization is required to get most of Teams reports in Nova.

Reference

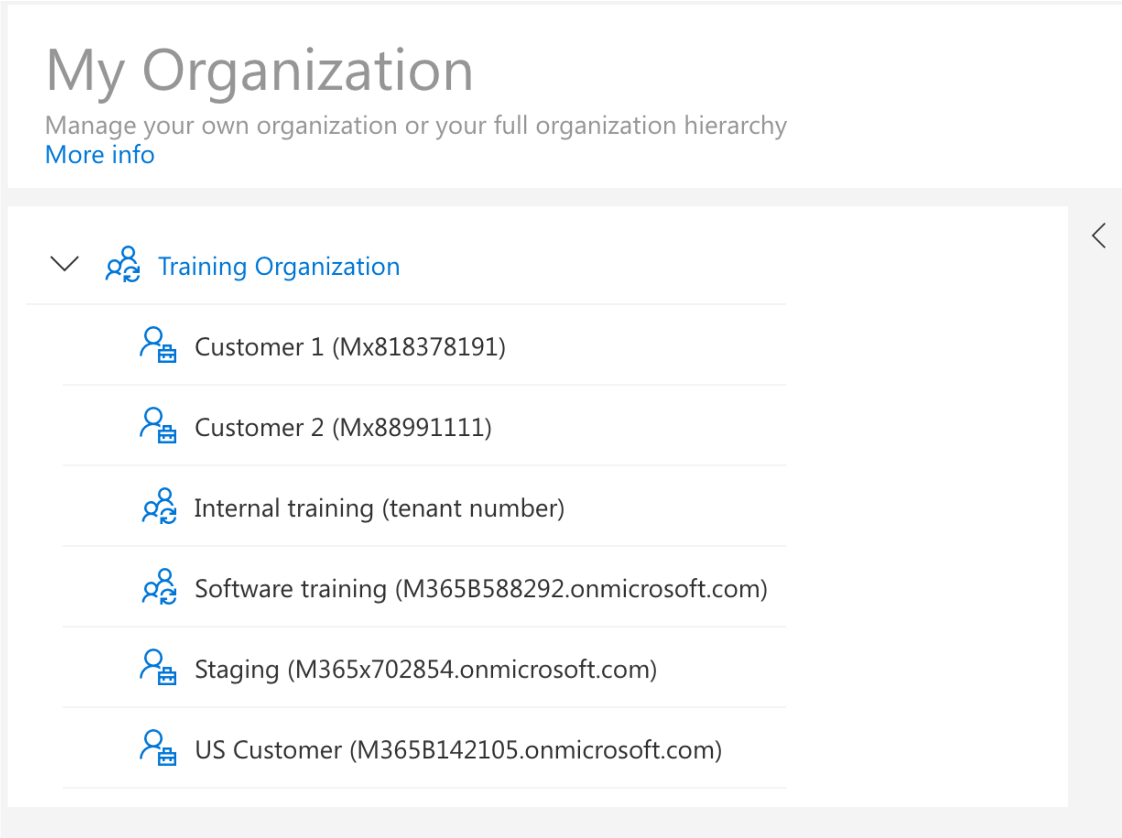
There is one additional use of Connect Tenant, which is used to provision new tenants for Nova.

How to Add New Users to Nova

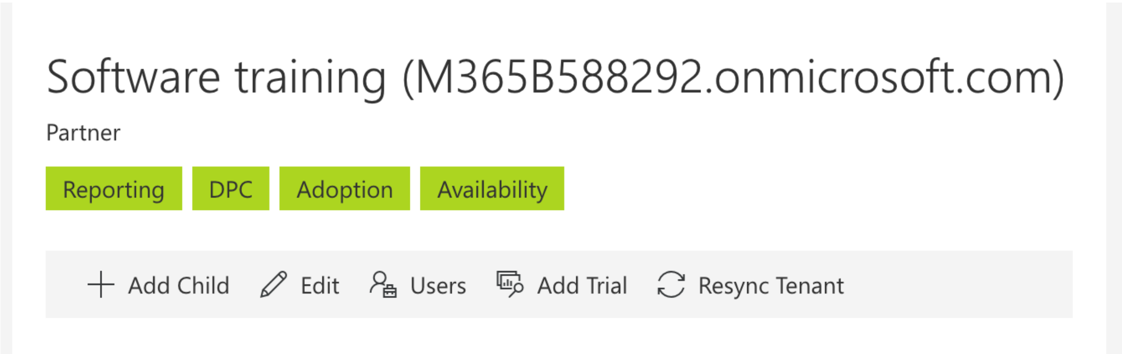
New users can be added to tenants that you have access so that they can have access to Nova features and services. This is performed in TMS (the Tenant Management System).

These are the steps that you should take:

- Login to TMS using an account with the System Administrator role.
- Locate the tenant / container where you want to add a new user and click on it. (For example I could click on 'Software training')



- Then click on ‘Users’

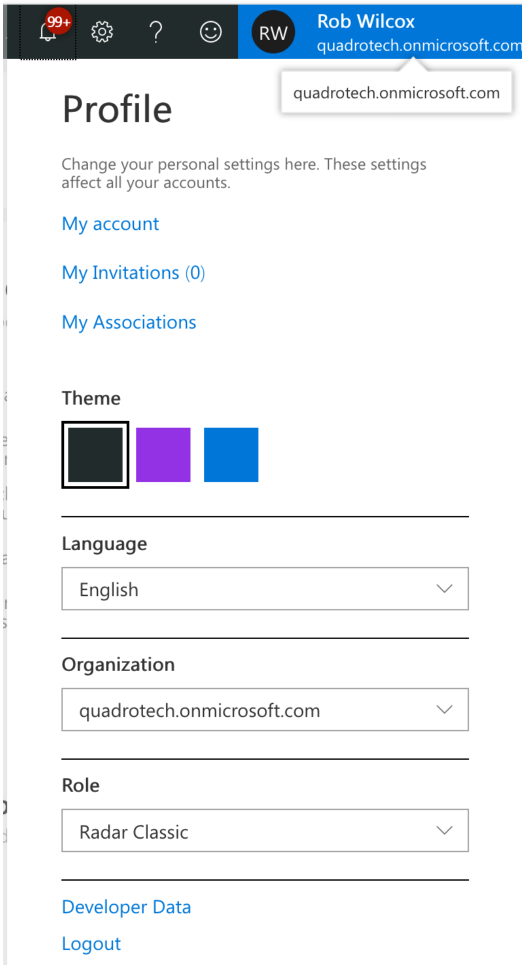


You will be shown a list of users who are already associated / invited / active in your chosen tenant. On the ‘invitations’ tab, you can invite a new user. Enter their email address, choose appropriate roles, and click on ‘Invite’

This sends an invitation to that user via email to join the tenant / container, which the user must accept.

Once accepted the user will appear on the list of users. Whilst you wait for them to accept you can see them on the invitations tab.

Once they accept, 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:

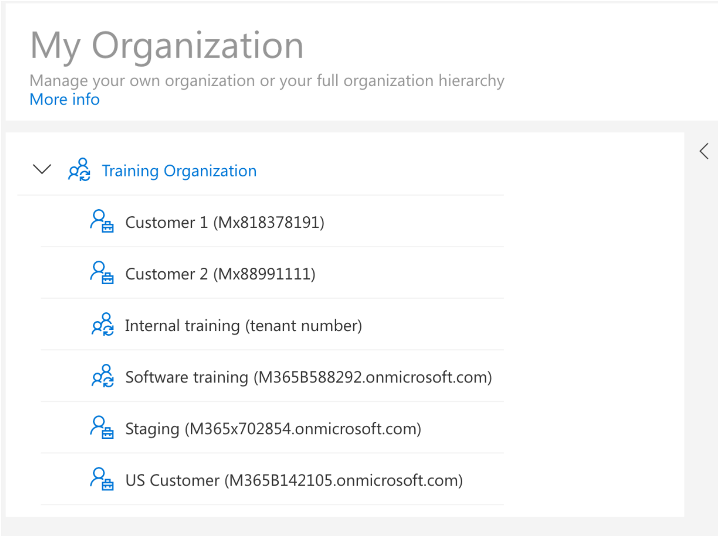


To learn more about the Persona menu, see this article.

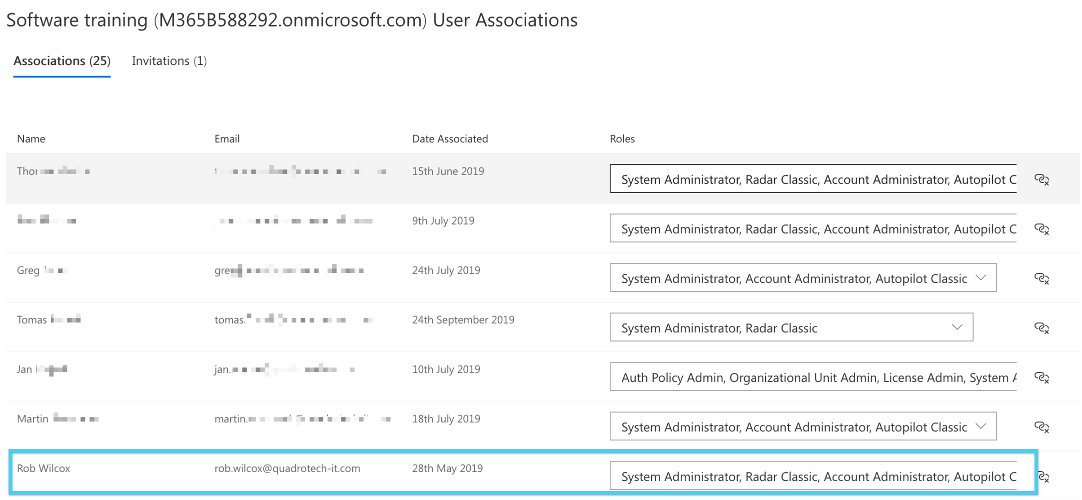
Nova remembers which tenant and role a user was last using, so the next time that user logs into Nova it takes the user back to the same place. This happens across browsers, and across sessions.

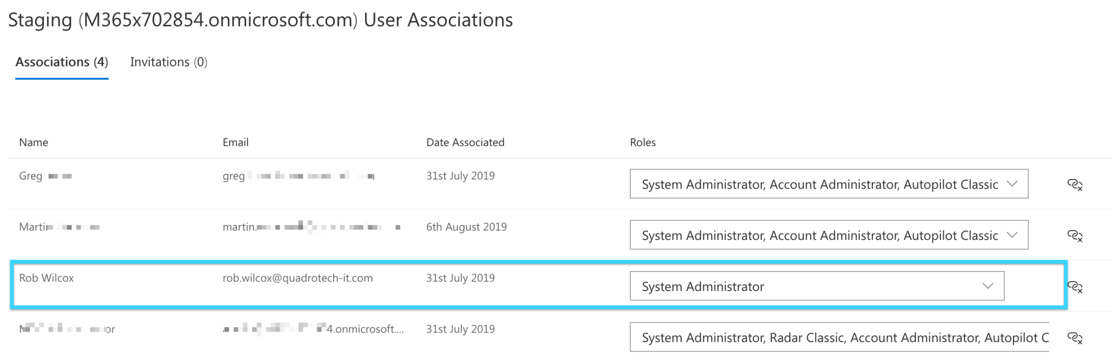
What's an association?

In the above description we've 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's also possible for the same user to have different access levels in different organizations. In other words they would have different roles. Let's say we have multiple tenants in an organization, as shown below:



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





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

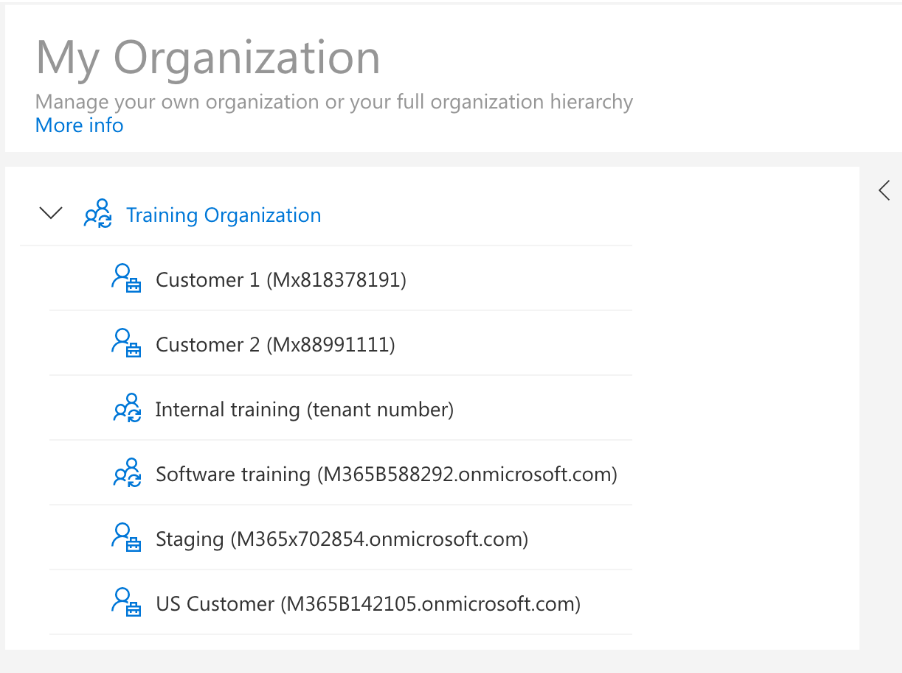
Removing a user

To see how to remove a user from your tenant, see this article.

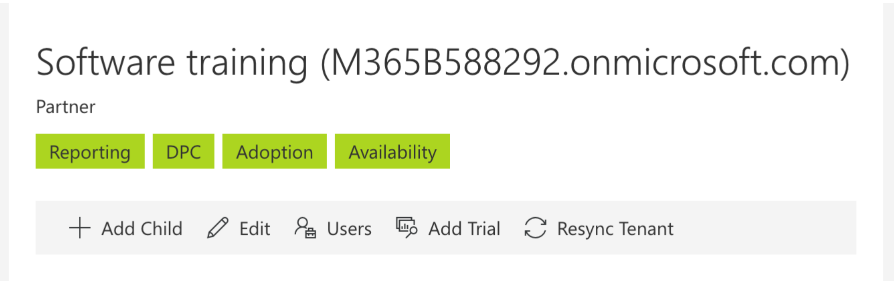
Remove a User From Your Tenant in Nova

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

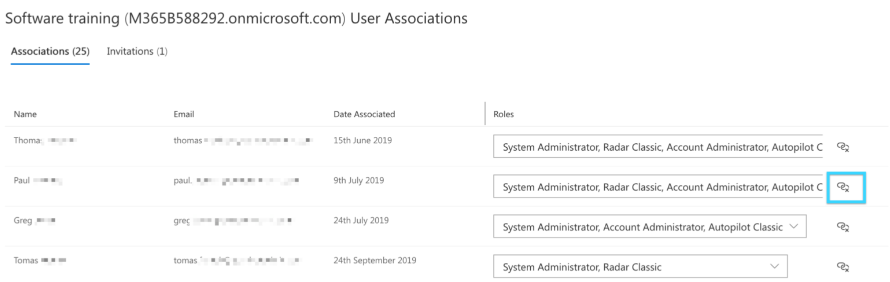
- Login to TMS using an account with the System Administrator role.
- Locate the tenant / container which you want to manage and click on it (for example, I could click on 'Software training').



- Then click on 'Users'



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



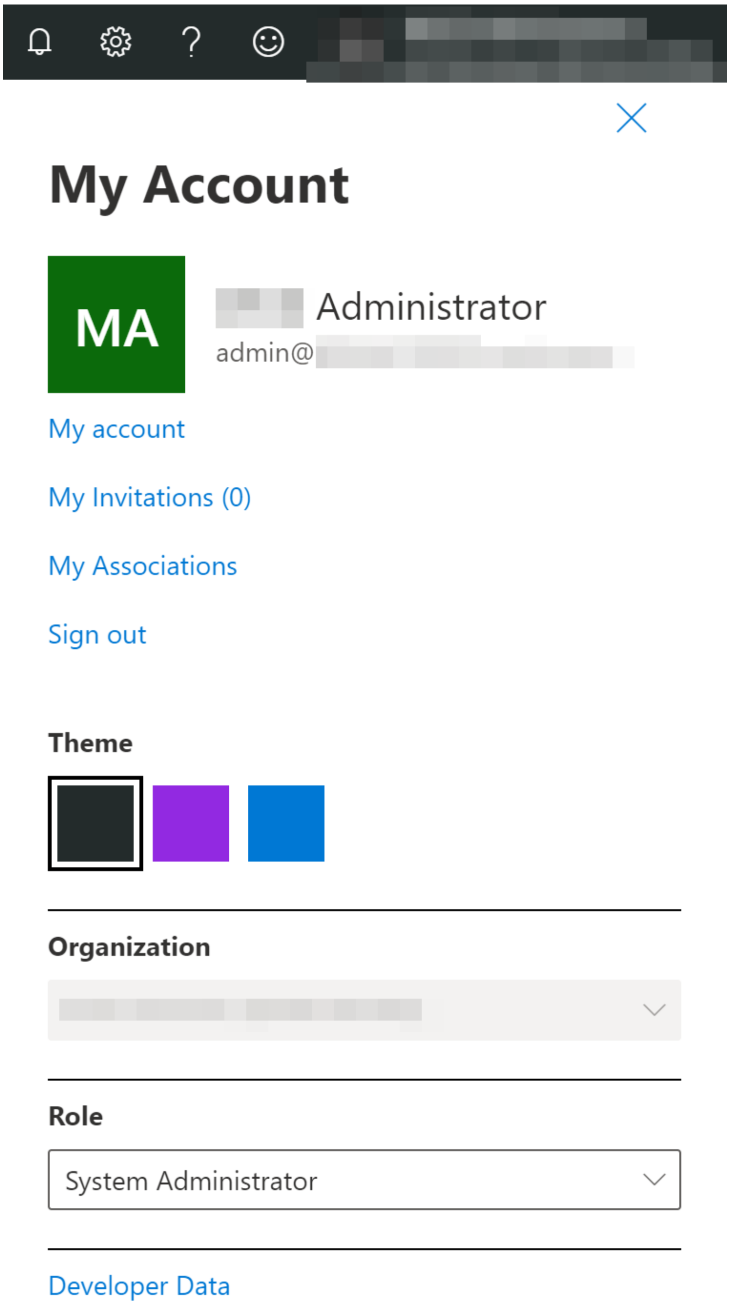
Click on the icon to the right of the user and their roles, and it will remove their association with this tenant.

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

What Is the Persona Menu in Nova

The Persona menu in Nova 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.

What are the Roles Within Nova

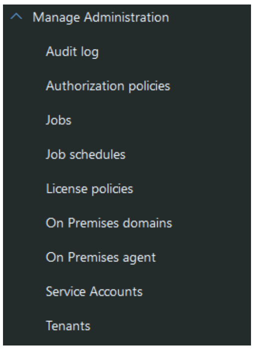
Users of the Nova application can be assigned one or more roles. Each role provides functionality in the Nova application itself. Roles can be combined. The following is a list of the roles, and what they give access to:

System Administrator

This roles 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).

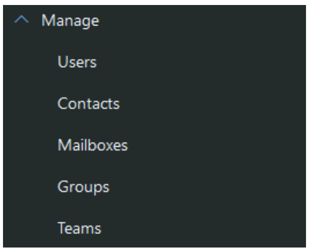
Account Administrator

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:



Autopilot Classic

This gives access to be able to perform allowed actions against users, mailboxes, groups, contacts and Microsoft Teams. It is the role most appropriate to a delegated administrator. 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. This is an example of the menu that a user will see, if they are given this role:



Radar Classic

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

Report Reader

Report Readers are assigned a view-only status for reports. They can read, print and download (.CSV or .PDF) reports, but unable to create, import, clone or edit reports. Nova administrators have the right to grant this access to protect and maintain accountability, data integrity and security. For more on this role, click here.

Auth Policy Admin

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

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.

IT Administrators

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

Why do we use the 'Classic' names?

Two parts of Nova have existed in different systems and different formats before Nova. We have customers 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 someone needs to be able to create authorization policies, and actually perform actions on customer tenants (such as password resets, maintaining groups, adding Microsoft Teams and so on) 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's own. It needs to be combined with the Autopilot Classic role.

Report Reader Role in Nova

Report Readers are assigned a view-only status for reports. They can read, print and download (.CSV or .PDF) reports, but unable to create, import, clone or edit reports. Nova administrators have the right to grant this access to protect and maintain accountability, data integrity and security.
Users' with the Report Reader role:

Can

- See reports made by their organization (custom reports).
- Schedule and download reports.
- Change sort criteria and column ordering (without saving).
- Use search fields.
- Schedule reports to be sent to any recipient.
- Edit and cancel their own scheduled reports.

Can't

- See any pinned reports.
- Modify the sharing status for a report.
- See application settings in the settings panel.
- Access the Manage, Manage Administration, Usage & Adoption or the Service Health tab.

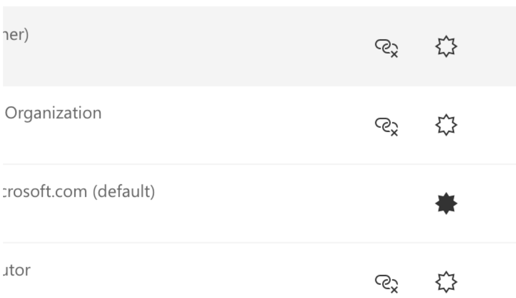
Changing Default Organizations in TMS

Summary

In case one user email is used in multiple tenants, the default organisation has to be selected to provide the switching mechanism for Radar Reporting.

Solution

1. Log in to TMS (Tenant Management System) https://account.quadro.tech
2. Navigate to User menu (top right corner)
3. Select My Associations
4. Click on the "star" next to the organisation you want to mark as default – it should change to "full star" and (default) text next to tenant name



5. Log in to Radar Reporting. It will log to the default organisation selected in TMS.

NOTE:
Radar Reporting is deployed in two locations US and EU. Please make sure you are using correct address related to your tenant:

US https://reports.o365radar.com
EU https://reports.o365radar.eu

7

Knowledge Base

Enter topic text here.

User Detail in Nova

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

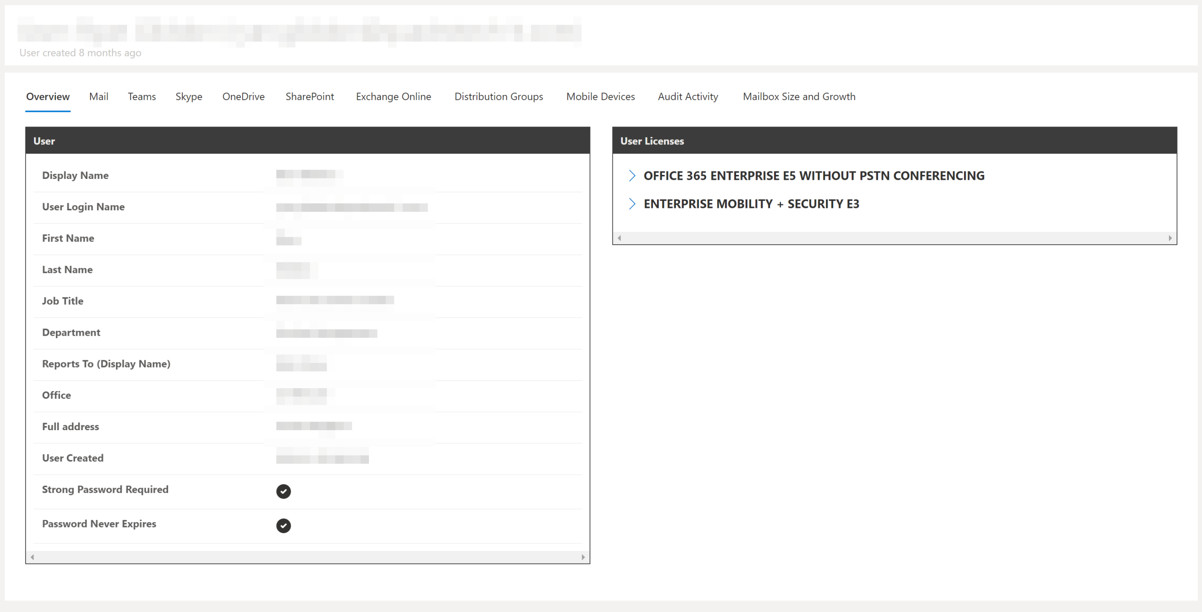
Let's take a look into these tabs and how its information can help administrators.

User Overiew

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

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

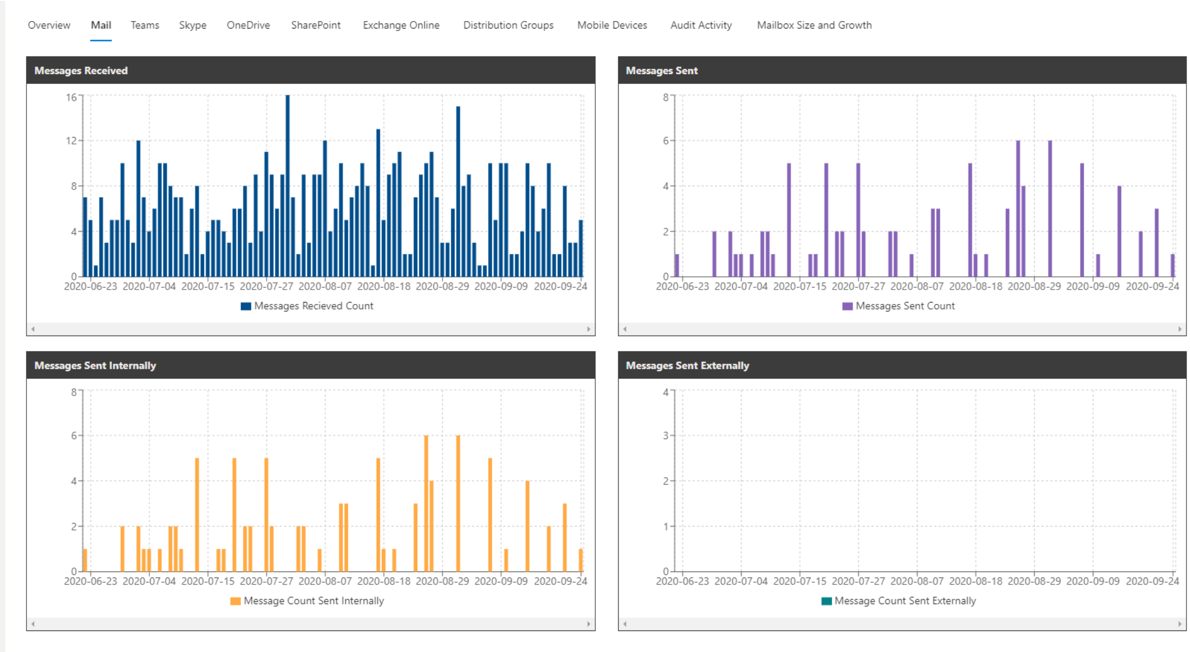
The screen also contains information on licenses that have been assigned to that user, including if that license has been successfully applied to that user or if it is pending.



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

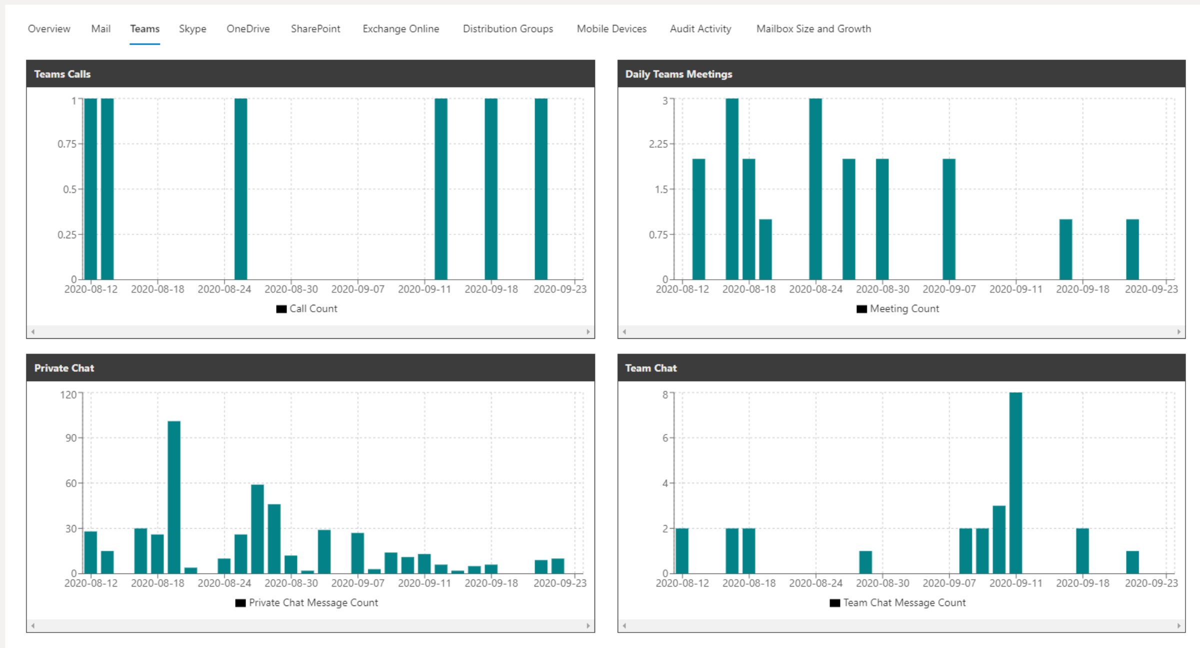


Teams

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

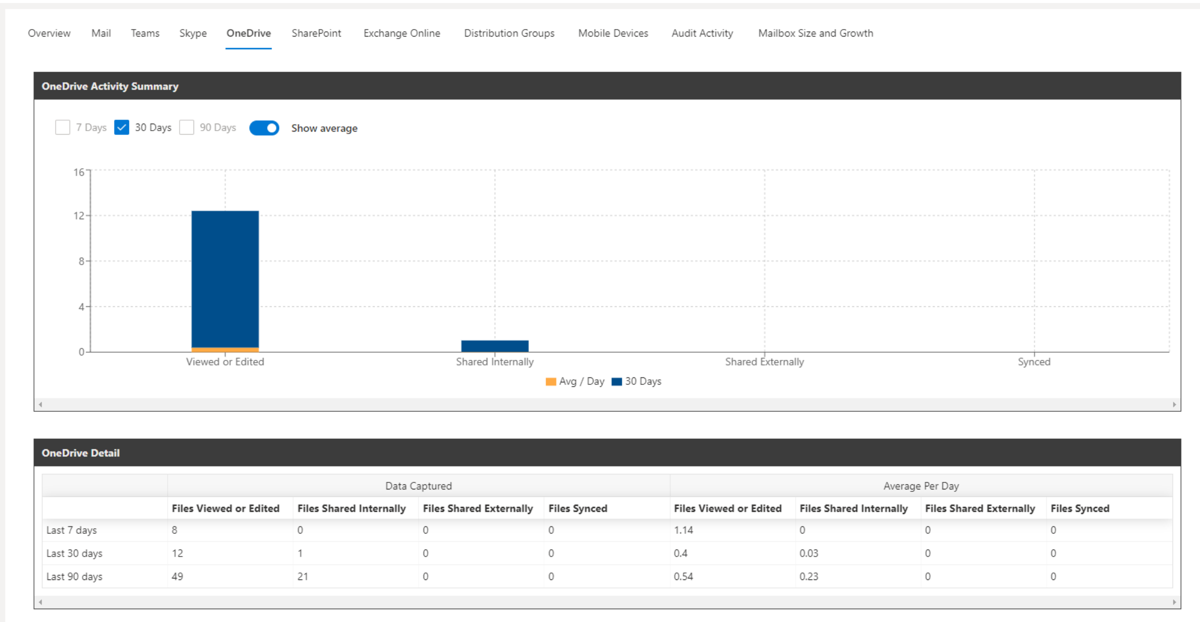


OneDrive

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.



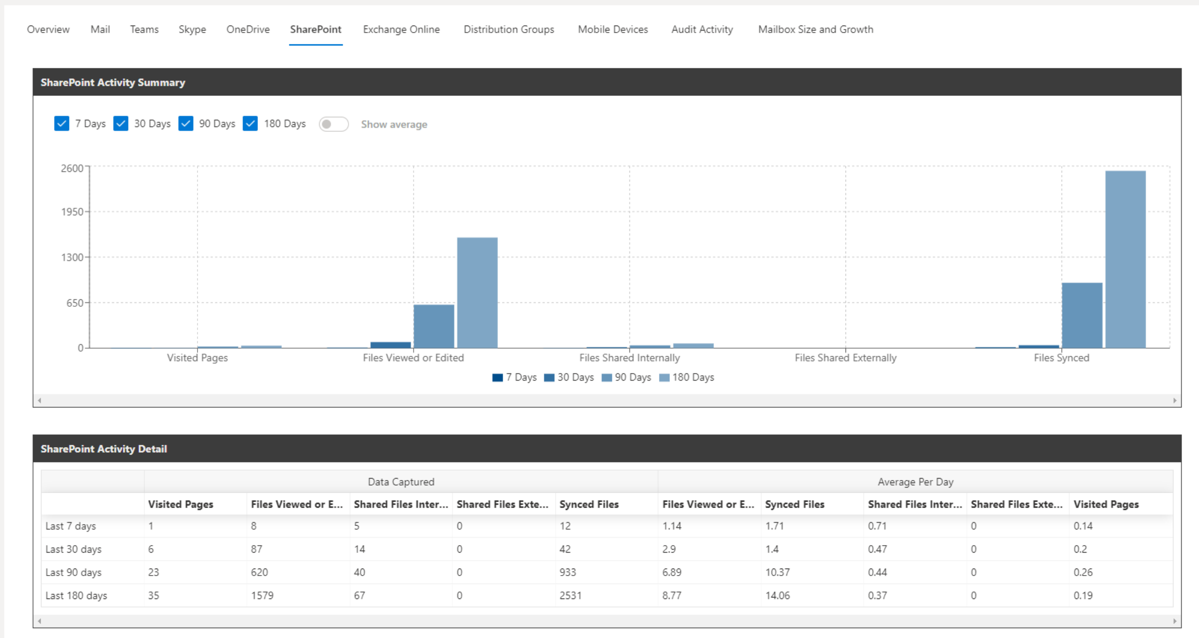
	Data Captured				Average Per Day			
	Files Viewed or Edited	Files Shared Internally	Files Shared Externally	Files Synced	Files Viewed or Edited	Files Shared Internally	Files Shared Externally	Files Synced
Last 7 days	8	0	0	0	1.14	0	0	0
Last 30 days	12	1	0	0	0.4	0.03	0	0
Last 90 days	49	21	0	0	0.54	0.23	0	0

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.

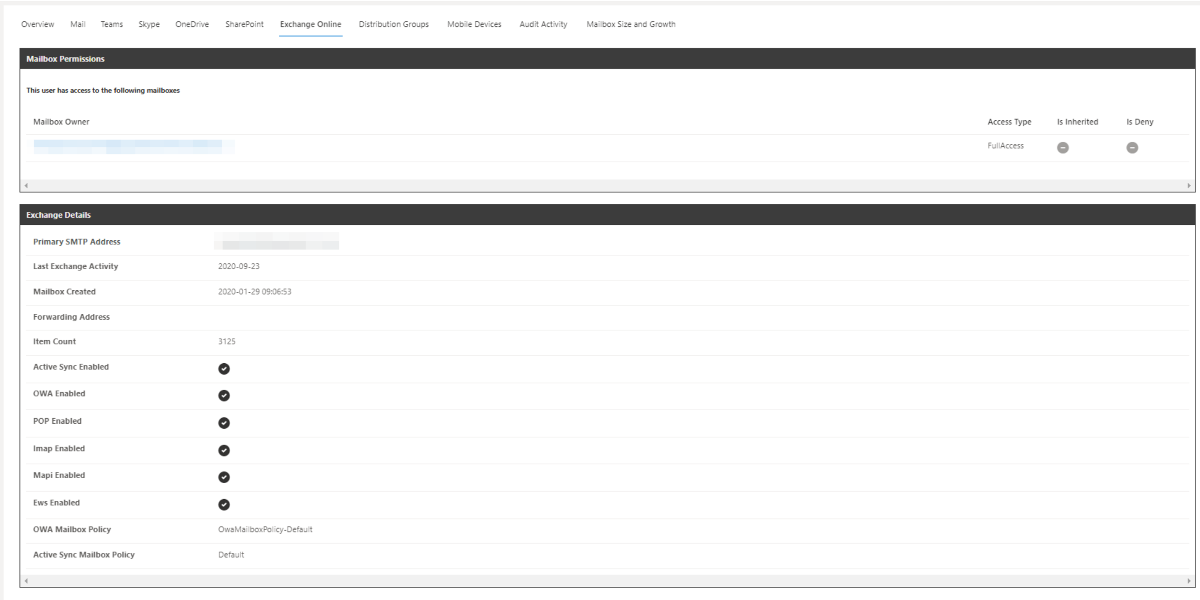


	Data Captured					Average Per Day				
	Visited Pages	Files Viewed or E...	Shared Files Inter...	Shared Files Exte...	Synced Files	Files Viewed or E...	Synced Files	Shared Files Inter...	Shared Files Exte...	Visited Pages
Last 7 days	1	8	5	0	12	1.14	1.71	0.71	0	0.14
Last 30 days	6	87	14	0	42	2.9	1.4	0.47	0	0.2
Last 90 days	23	620	40	0	933	6.89	10.37	0.44	0	0.26
Last 180 days	35	1579	67	0	2531	8.77	14.06	0.37	0	0.19

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)



Mobile Devices

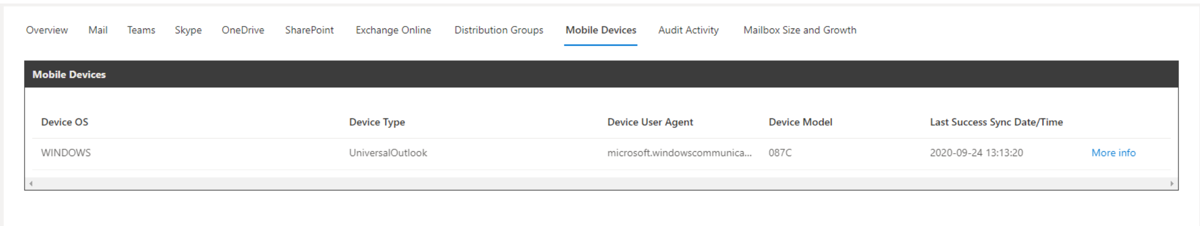
The Mobile Device tab gives you information on mobile devices affiliated with a user. Overview details include:

- 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.

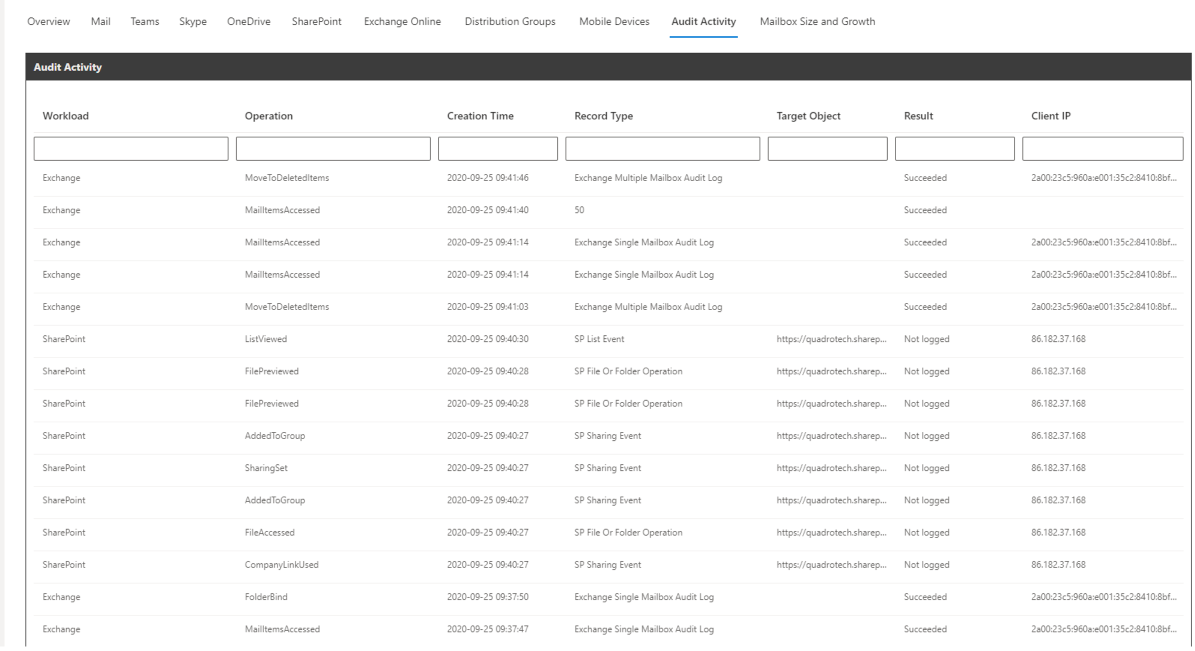


Audit Activity

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


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

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	2a00:23c5:960a:e001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:41:40	50		Succeeded	
Exchange	MailItemsAccessed	2020-09-25 09:41:14	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c5:960a:e001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:41:14	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c5:960a:e001:35c2:8410:8bf...
Exchange	MoveToDeletedItems	2020-09-25 09:41:03	Exchange Multiple Mailbox Audit Log		Succeeded	2a00:23c5:960a:e001:35c2:8410:8bf...
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	2a00:23c5:960a:e001:35c2:8410:8bf...
Exchange	MailItemsAccessed	2020-09-25 09:37:47	Exchange Single Mailbox Audit Log		Succeeded	2a00:23c5:960a:e001:35c2:8410:8bf...

Why is my Federated Domain Unavailable for Primary SMTP Addresses?

As a Nova administrator adjusting your Primary SMTP addresses for a user, you may notice that your federated domain is grayed out and unavailable to use.
More information on this is available from Microsoft here.

Overiew: Why a Report has no Data

You may come across the notification '**There is no data for this chart**' as you are building a report.

There are a few reasons for this, including:

- The data is being filtered in a way that no data is returning. You may need to edit your report and modify your filters that you have applied.
- The data may require access to the Security and Audit Logs that may not have been configured. Check your Nova settings in inquire about this.
- The data has not been collected as the data collection needs to be authorized.

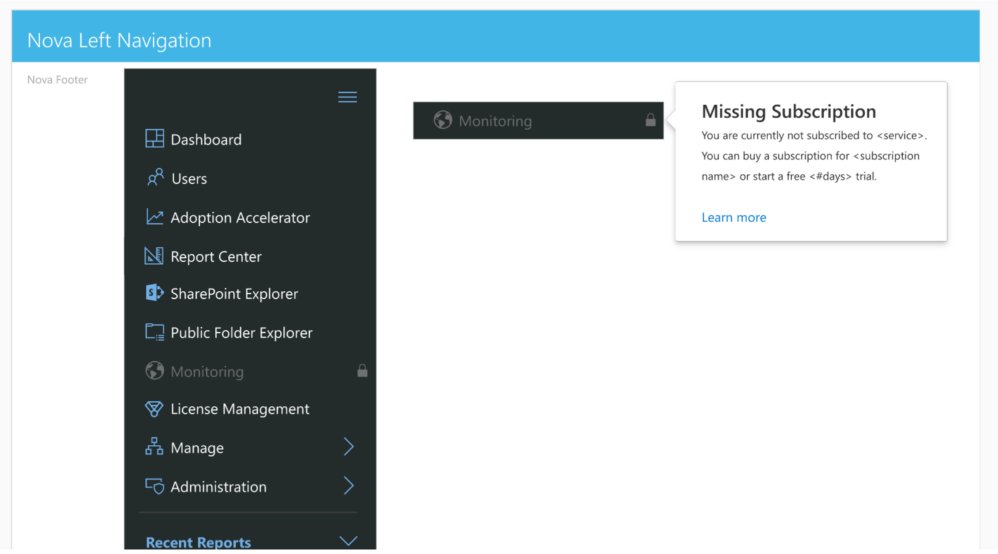
You may need to your tenant. For steps on how to do this, check out this article.

If you have completed these steps and still have the notification and/or there is still no data being presented in your report, please contact support about your issue.

For more information on the Nova Report Center, click here.

Missing Subscription

In Nova you may receive a message about a missing subscription:

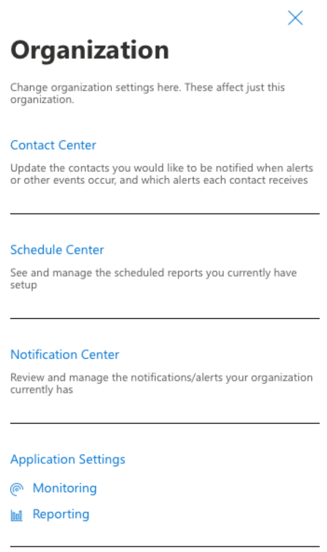


Certain areas of Nova as well as menu items may have the lock symbol on them. It means that you do not have access to that feature at your subscription level. Contact Quest in order to upgrade.

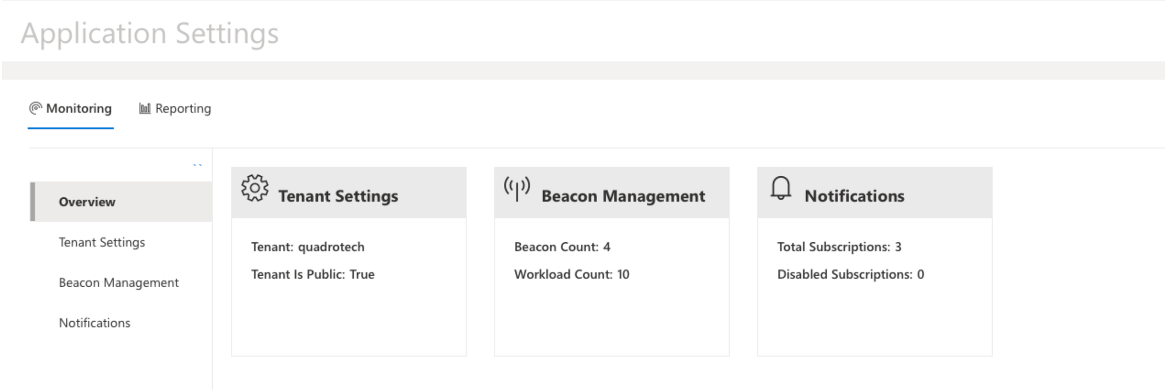
How to Create a Notification for Issues Encountered on Beacons

When custom beacons have been deployed, it is often required to create some notifications about the health / status of the beacon. For example you may want to configure a notification to alert an administrator if a particular test on a workload fails or takes too long to run

This article outlines the steps necessary to do that.
The first step is to access the monitoring settings from the menu:

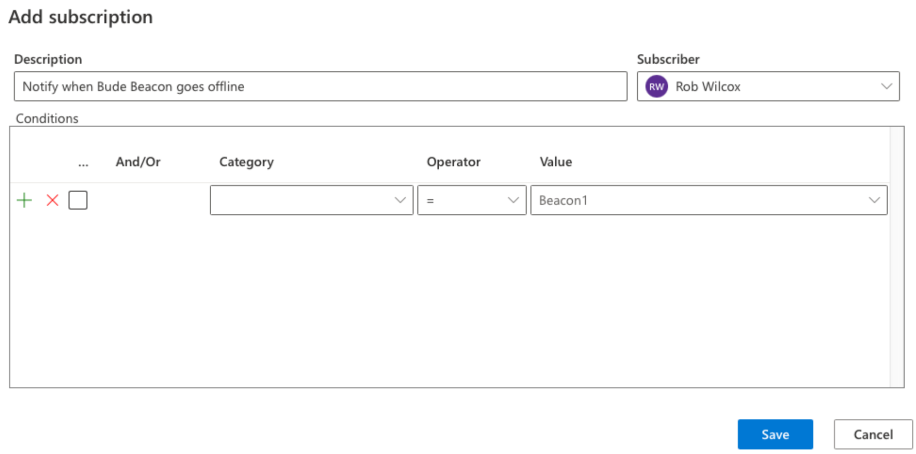


After selecting the option from the menu you'll see this page:



Select 'Notifications' from the list of options on the left, and you'll see all the existing notifications for the tenant.

You can then begin adding a new notification:



To configure a notification when a workload result is degraded / poor:

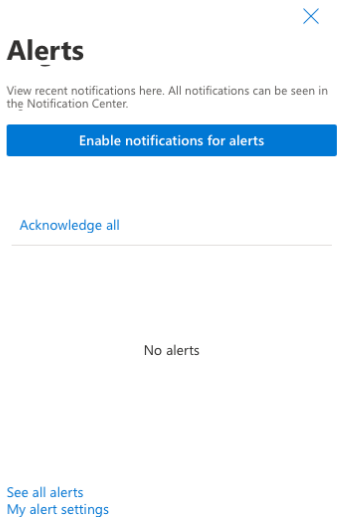
- Beacon Name = the beacon you want to be notified about
- workload = name of the required workload
- severity = degraded

If you want to know when any of the tests result in degraded or poor responses:

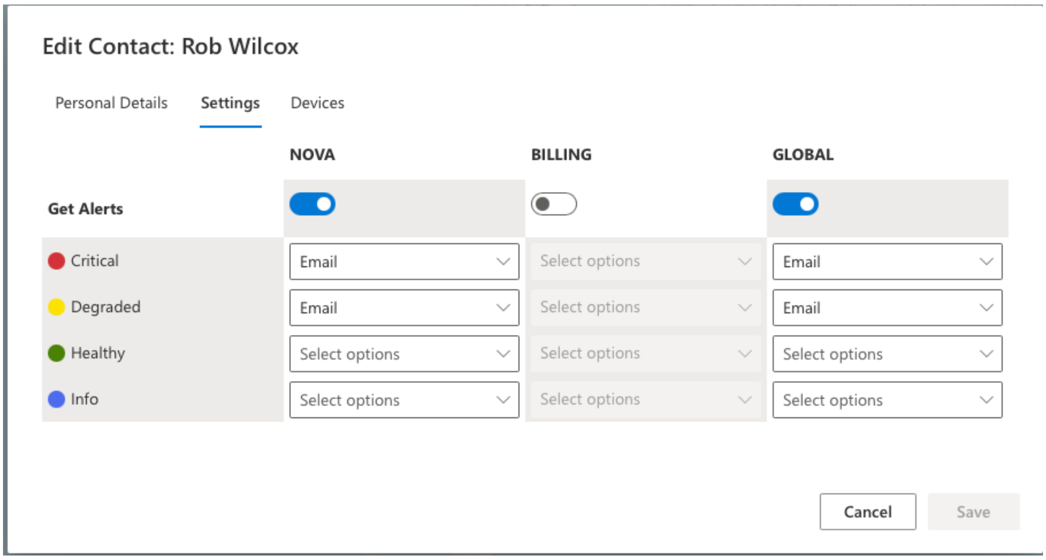
- Beacon Name = the beacon you want to be notified about

- severity = degraded

The final thing to configure is how to receive the notifications. To do this click on the notifications icon at the top right of the user interface, and choose ‘My alert settings’:



On the page in the interface you can choose different severities of alert, along with the method you want to receive the alert:



NOTE: In order to configure notifications the user that performs the actions outlined here needs to be in the System Administrator role.

How to Request a Report

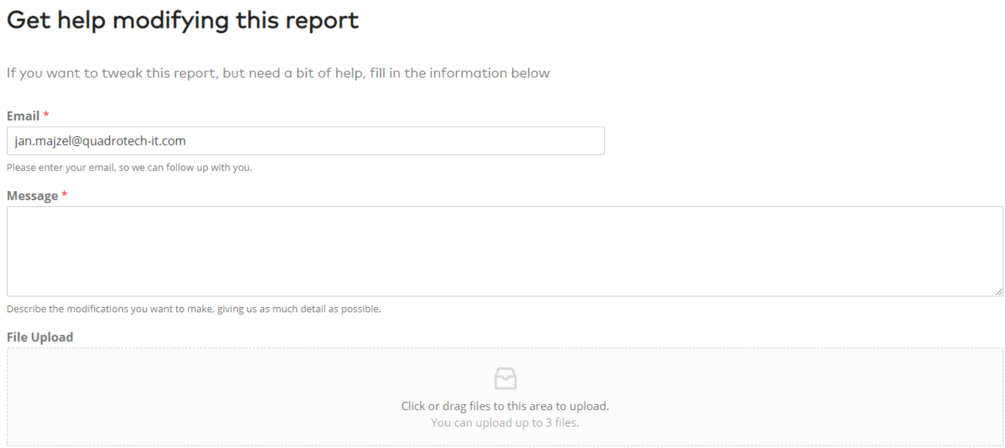
This article explains what to do when:

- You want help modifying a Nova report
- You have a new report that you want us to consider
- You want help creating a whole new report

Each of these tasks can be performed by accessing our Community website. You already have a QTID as a Nova customer, and therefore you can simply login, and access the resources.

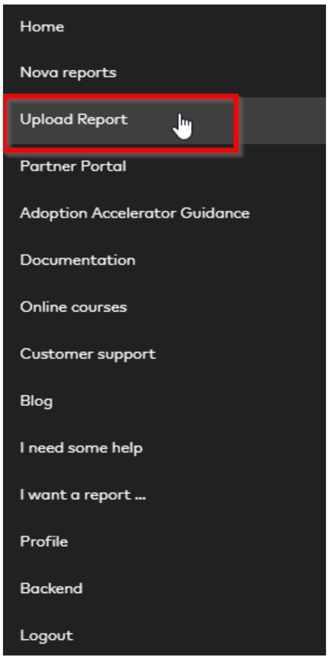
You want help modifying a Nova report

If you want help modifying a Nova Report go to: https://community.quadrotech-it.com/all-reports/, select a report (for example) https://community.quadrotech-it.com/2020/04/license-assignment-by-country/ and at the bottom of the report you will see a form that allows you to submit a request to get help.



You have a new report that you want us to consider

We'd love for you to share reports with the rest of the community. To do this choose 'Upload Report' from the Community website menu:

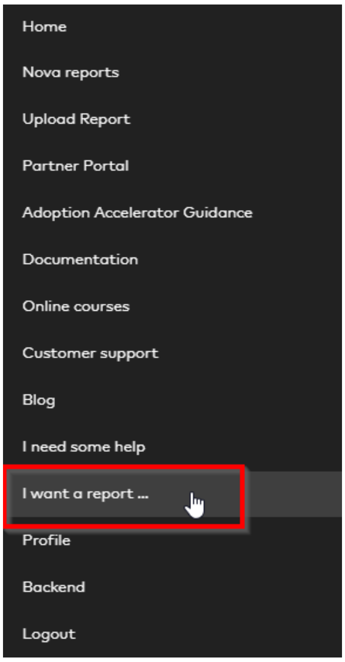


The report will be submitted to our Customer Experience Team who will review the report, make sure the screenshots are made anonymous and check if it's similar to reports we already have. When all that's done, it'll be published to the Community Site for other customers to make use of.

NOTE: It's only the report definition which is shared, not any data from your organization.

You want help creating a whole new report

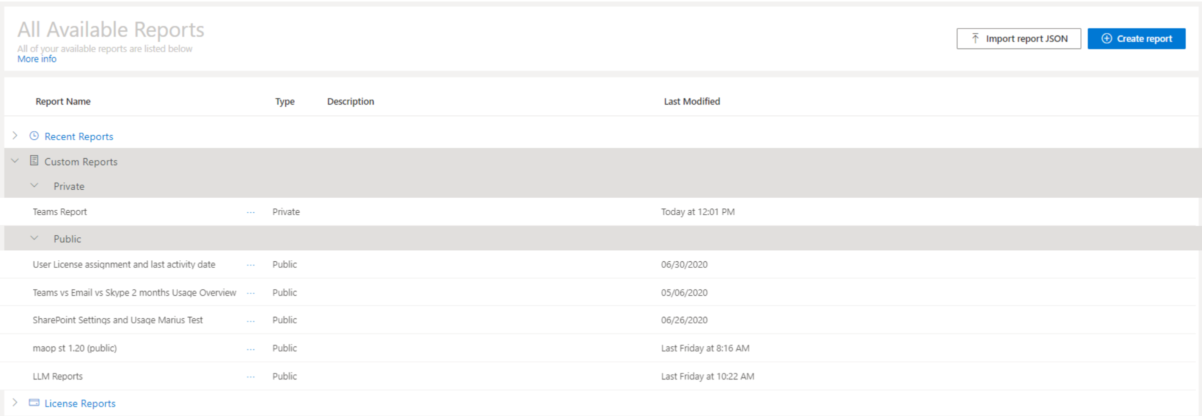
If you can't find a report inside Nova, or on the Community website to suit your needs, contact us by going to the 'I want a report' link on the Community website.



We'll work with you to determine your needs, and whether it's possible to do it in Nova.

Private and Public Reports in Report Center

The Private and Public report sections in the Report Center allow users to quickly see which reports are private to you and which reports are accessible by your organization.



View a User's SharePoint Usage in Nova

Enter topic text here.

DPC On-Premises Filtering

Issue

One common request we get is how to design DPC policies that apply only to objects that are on-prem, or objects that are in the cloud. For example, I might want a policy to assign all on-prem accounts a particular custom attribute.

Solution

One way is to create a real or virtual organizational unit, or a security group, that contains only the on-prem or cloud users, then use that OU or group as the scope of the policy.
Another is to select either the “Update Cloud User” or “Update On-Prem User” action in the policy. Each of those actions will only target the related user type, so if you have a scope and condition set in the policy that includes both on-prem and cloud users but select the “Update On-Prem User” action, only the on-prem users that the policy matches will be affected.

> **NOTE:** if you create an OU or group for the scope, you still have to select the correct action type. The reason for creating the OU or group is to make clear what the scope is to both human users and auditing software.

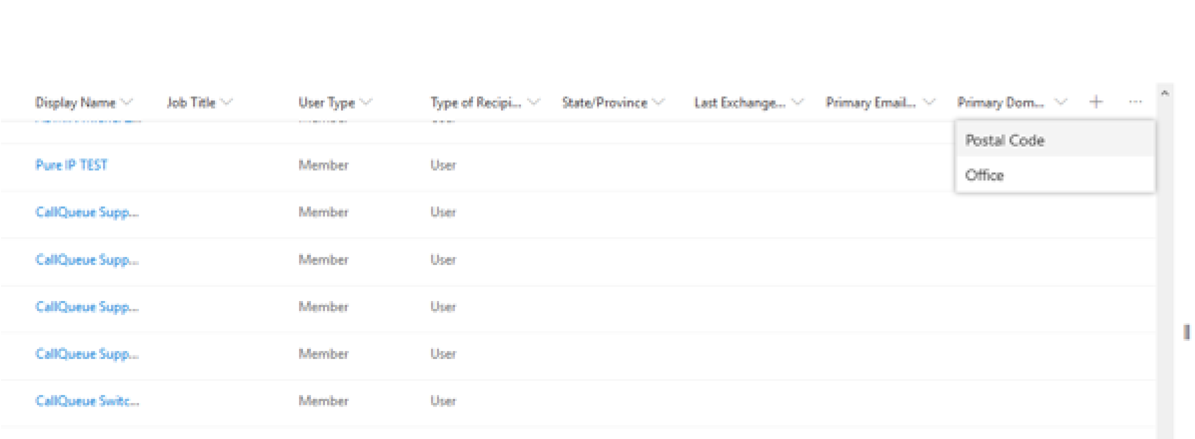
How to View Extra Columns in a Table Report Section in Nova

Issue

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.

Solution

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.



For more information on tabular data in Nova, click here.

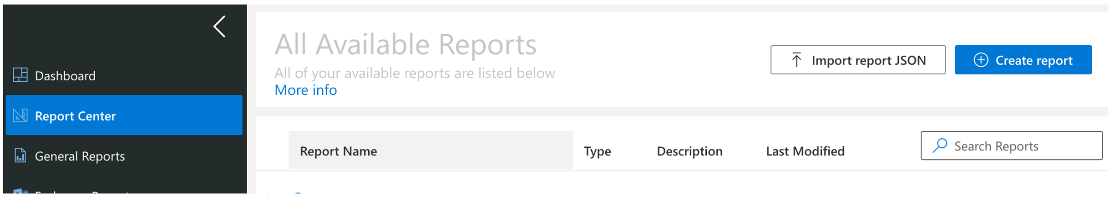
Import Report Definition in Nova Reporting

Overview

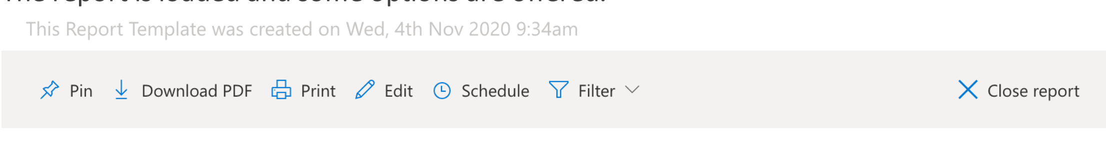
If you need to import report that is not yet available in Nova you can do so by importing report definition in JSON format.

Steps

1. Go to Report Center
2. It will open your screen with all reports
3. Click on 'Import Report JSON'

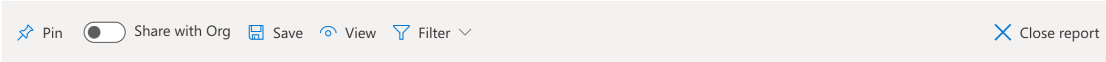


4. The report is loaded and some options are offered.

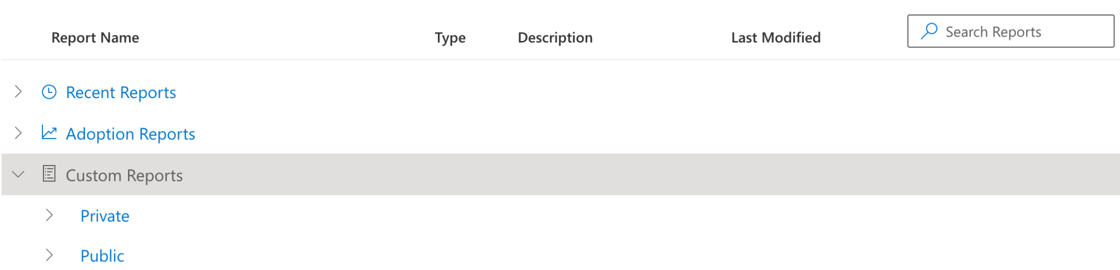


5. The report is visible only for the user who imported it. (Private)
6. If you would like this report to be visible for whole organization, it must be shared. (Public)

7. To do so, click on *Edit* and then switch on *Share with Org* and *Save*



8. To find such report, you can look into Recent or to Private/Public section of the Report Center, depending if the reports are marked Private or Public. Reports can be searched too in Search Reports field



Reference

To export report definition please follow this KB

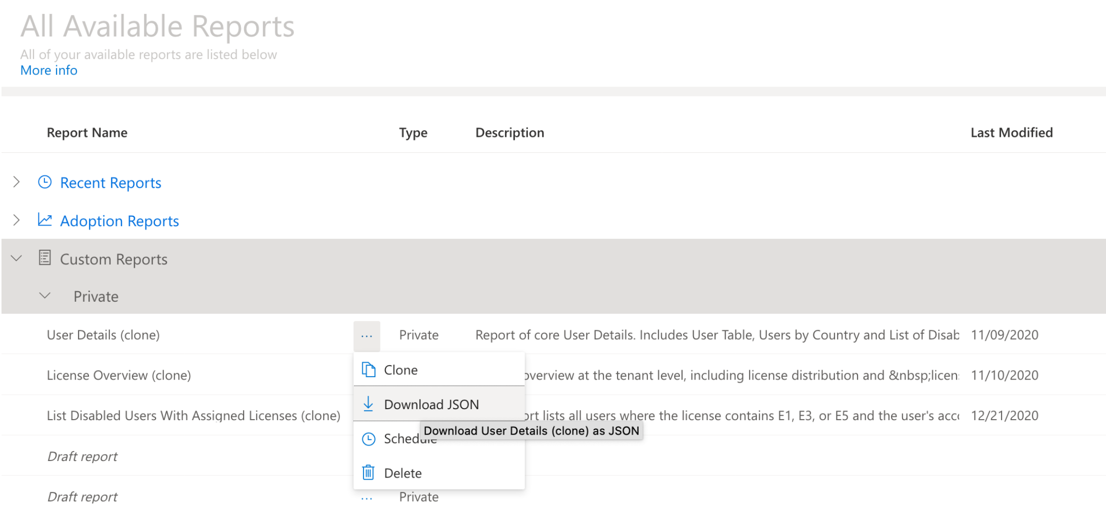
Export Report Definition in Nova Reporting

Overview

If you need to export report to be shared with others or used in different tenants you can do so by exporting report definition in JSON format.

Steps

1. Go to Report Center
2. It will open your screen with all reports
3. Click on ellipses (...) next to the report you want to export



4. Select the Download JSON option
5. You will be prompted by browser to save the file on your workstation or to open it with default program for json file type

6. The name of the report definition file consist of the **report name** and the file suffix **json**

Reference

To import report definition please follow this KB

Issues with Generating Heat Maps and Large Datasets

Issue

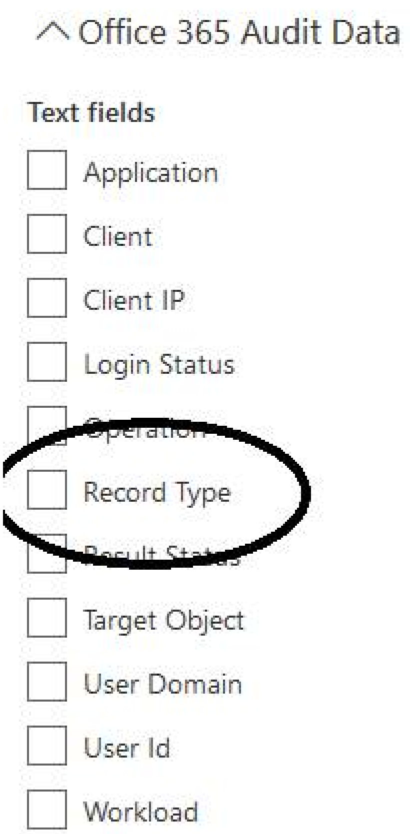
You may receive an error saying ‘Gateway timeout’ when generating a heat map report section in Nova

Solution

This can occur when there are more than approximately 4000 users. Our engineering team is aware of this issue. An update will be posted when more information is available.
(Related: 87550)

Using Record Type in Office 365 Audit Data

The Record Type data field in Audit Database is a major addition to the Audit Data Source and is now available.



For example you can see just Admin Operations (8) or any file that has been modified (6) or DLP (33). Here is a list of Record IDs which may be in the audit timeline if that event has been generated
1 – Indicates a record from the Exchange admin audit log.
2 – Indicates a record from the Exchange mailbox audit log for an operation performed on a singled mailbox item.
3 – Also indicates a record from the Exchange mailbox audit log. This record type indicates that the operation was performed on multiple items in the source mailbox (such as moving multiple items to the Deleted Items folder or permanently deleting multiple items).
4 – Indicates a site admin operation in SharePoint, such as an administrator or user assigning permissions to a site.
6 – Indicates a file or folder-related operation in SharePoint, such as a user viewing or modifying a file.
8 – Indicates an admin operation performed in Azure Active Directory.
9 – Indicates OrgId logon events in Azure Active Directory. This record type is being deprecated.
10 – Indicates security cmdlet events that were performed by Microsoft personnel in the data center.
11 – Indicates Data loss protection (DLP) events in SharePoint.
12 – Indicates Sway events.

13 – Indicates DLP events in Exchange, when configured with a unified a DLP policy. DLP events based on Exchange mail flow rules (also known as transport rules) aren't supported.
14 – Indicates sharing events in SharePoint.
15 – Indicates Secure Token Service (STS) logon events in Azure Active Directory.
18 – Indicates Security & Compliance Center events.
19 – Indicates aggregated Exchange mailbox operations for repetitive activity that occurs within a very short duration.
20 – Indicates Power BI events.
21- Indicates Dynamics 365 events.
22 – Indicates Yammer events.
23 – Indicates Skype for Business events.
24 – Indicates eDiscovery events. This record type indicates activities that were performed by running content searches and managing eDiscovery cases in the security and compliance center. For more information, see Search for eDiscovery activities in the Office 365 audit log.
25, 26, or 27 – Indicates Microsoft Teams events.
28 – Indicates phishing and malware events from Exchange Online Protection and Office 365 Advanced Threat Protection.
29 – Indicates submission events from Exchange Online Protection and Office 365 Advanced Threat Protection.
30 – Indicates Microsoft Power Automate (formerly called Microsoft Flow) events.
31 – Indicates Advanced eDiscovery events.
32 – Indicates Microsoft Stream events.
33 – Indicates events related to DLP classification in SharePoint.
35 – Indicates Microsoft Project events.
36 – Indicates SharePoint list events.
37 – Indicates events related to SharePoint comments.
38 – Indicates events related to retention policies and retention labels in the security and compliance center.
40 – Indicates events that results from security and compliance alert signals.
41 – Indicates safe links time-of-block and block override events in Office 365 Advanced Threat Protection.
42 – Indicates events related to insights and reports in the Office 365 security and compliance center.
44 – Indicates Workplace Analytics events.
45 – Indicates Power Apps events.
47 – Indicates phishing and malware events from Office 365 Advanced Threat Protection for files in SharePoint, OneDrive, and Microsoft Teams.
49 – Indicates Patients application events in Microsoft Teams for Healthcare.
50 – Indicates events related to the MailItemsAccessed mailbox audit action.
52 – Indicates events related to the Data Insights REST API.
53 – Indicates events related to the application of information barrier policies. For more information, see Define policies for information barriers.
54 – Indicates SharePoint list item events.
55 – Indicates SharePoint content type events.
56 – Indicates SharePoint list field events.
62 – Indicates events related to email attack campaigns. For more information, see Campaign Views in Office 365 ATP.

64 – Indicates automated investigation and response events. For information, see automated investigation and response (AIR) in Office 365
66 – Indicates Microsoft Forms events.
68 – Indicates Communication compliance events in Exchange. For more information, see Communication compliance in Microsoft 365.
69 – Indicates events related Customer Key Encryption. For more information, see Service encryption with Customer Key in Office 365.

How to Generate a Redux Trace

When troubleshooting an issue in Nova, we may need to get a Redux trace. In this article we'll explain how to generate a Redux trace.

What's a Redux Trace?

Redux is a predictable state container for JavaScript apps. Redux trace is outcome of using Redux helping developers to troubleshoot issues within application using Redux.

Why do we Need/User a Redux Trace?

Redux trace contain actions and operations that your browser executed while the Redux trace was recording. This will often show us an errors and may give more information to us to track where the issue is in the code-base. It can also show us the time taken for different operations, so it can help with issues related to how fast (or slow) a page may load in a browser window.

How do I Generate a Redux Trace?

The steps vary from browser to browser. These steps are applicable to desktop browsers on both Windows and macOS. This KB shows steps for most common browsers Chrome and Firefox. Steps for other browser should be similar.

Chrome

1. Install Redux dev tools – https://chrome.google.com/webstore/detail/redux-devtools/lmhkpmbekcpmknklioeibfkpmmfibljd?hl=en
2. Open Developer Tools in Chrome (Menu -> View -> Developer -> Developer Tools)
3. Goto the Redux tab
4. Reload the whole page.
5. Export the Redux trace via Export button in the bottom of the window

Firefox

1. Install Redux dev tools – https://addons.mozilla.org/en-US/firefox/addon/reduxdevtools/?src=search
2. Open Developer Tools in Firefox (Menu -> Tools -> Web Developer -> Toggle Tools)

3. Goto the tab Redux
4. Reload the whole page
5. Export the Redux trace via Export button in the bottom of the window

What's Next?

Once the Redux trace has been generated, it's good practice to zip the .json file and send it to us.

Troubleshooting Why Azure Information May Not Be Populated for a User

There is a support page built into Nova to help with troubleshooting why Azure Tenant information is not being populated in TMS (it's needed for Delegation & Policy Control) despite the user having already logged in.

If you're affected by this problem you should complete the following steps, and provide the information to the customer experience team:

1. Go to https://id.quadro.tech/support
2. Login as normal using AAD / SSO login.
3. Click on the button labelled 'Login as support'
4. A diagnostic page should appear, as shown below

This page will only appear if we could get the data from the login token and Microsoft Graph. If not, then there is something more fundamentally wrong than syncing with TMS – we can't get the data from Microsoft Graph, or the user didn't use AAD login (notice IdentityProvider shows AzureAd for the login above, which shows it's an AAD login – anything else, it is not).

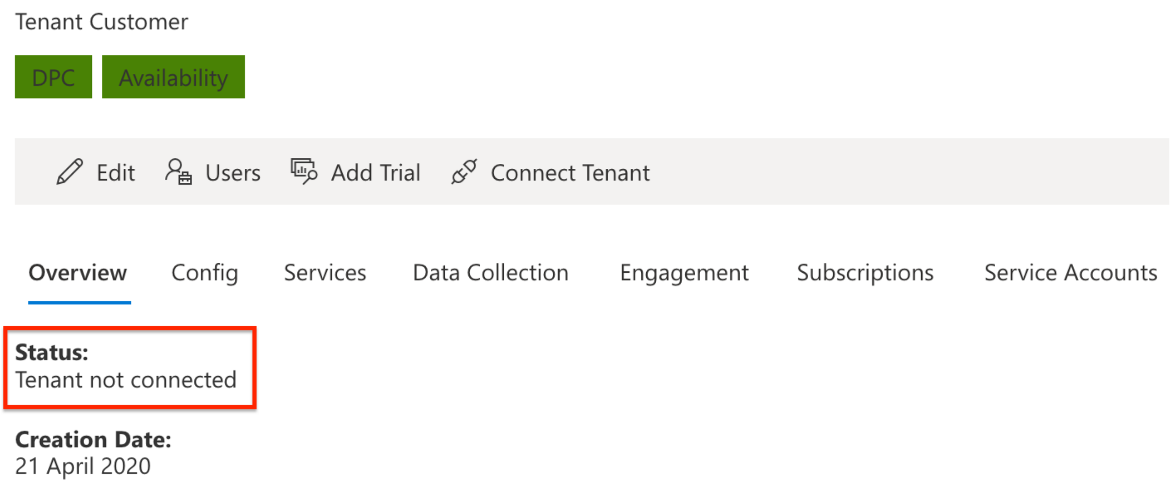
Two important things on this page:

1. The green highlighted domain is the Primary Domain. This should match TMS.
2. The TMS Org ID, at the bottom, is the org ID that got synced to for this login. If it DOES NOT match the org you are looking at in TMS, then this primary domain (Azure Tenant ID) is linked to another org somewhere in the hierarchy, and this will likely cause problems.

Tenant Not Connected

Overview

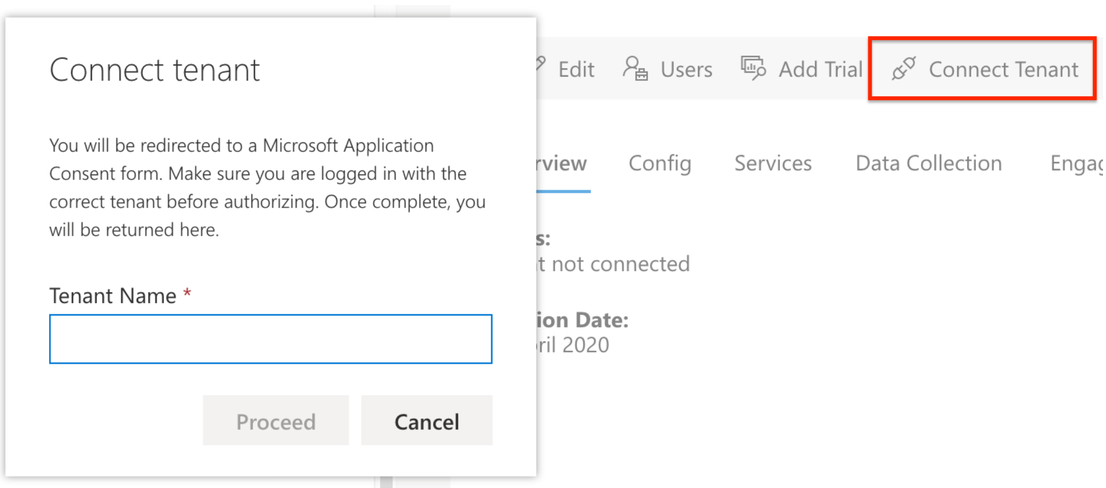
Throughout the onboarding you may see Status message in TMS: Tenant not connected.



Steps

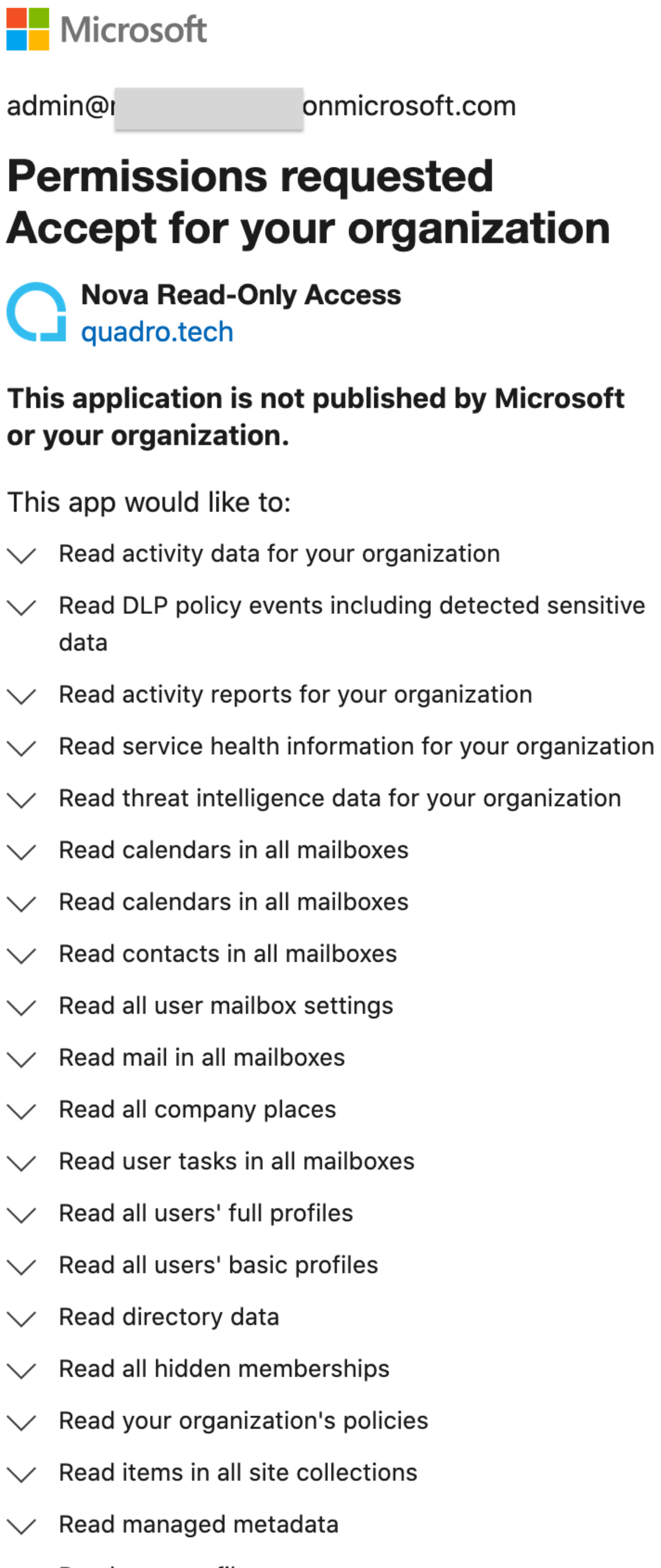
To resolve this issue you have to follow these steps:

1. Log in to TMS (https://account.quadro.tech/) as System Administrator of Nova
2. Click on *Connect Tenant* button

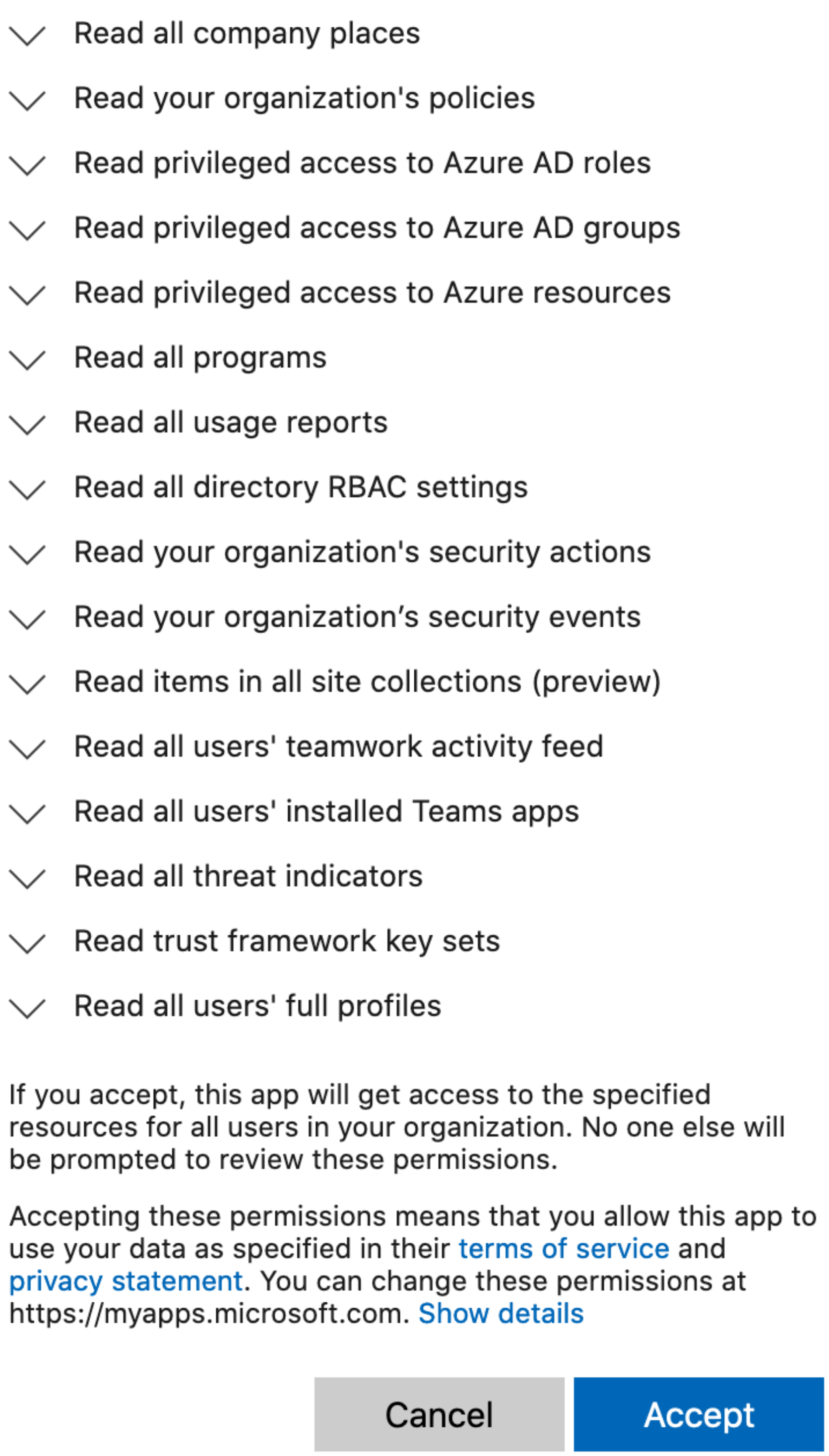


3. Fill in the tenant name you want to connect. E.g. myTenant.onmicrosoft.com and click *Proceed*

4. Make sure you are logging as the user with Global Admin account of that tenant and click Accept

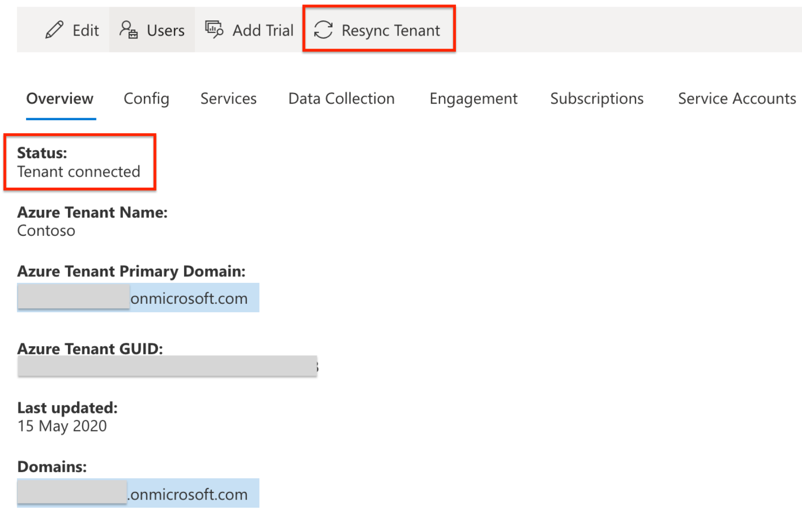

Microsoft
admin@ onmicrosoft.com
Permissions requested
Accept for your organization
Nova Read-Only Access
quadro.tech
This application is not published by Microsoft or your organization.
This app would like to:
Read activity data for your organization
Read DLP policy events including detected sensitive data
Read activity reports for your organization
Read service health information for your organization
Read threat intelligence data for your organization
Read calendars in all mailboxes
Read calendars in all mailboxes
Read contacts in all mailboxes
Read all user mailbox settings
Read mail in all mailboxes
Read all company places
Read user tasks in all mailboxes
Read all users' full profiles
Read all users' basic profiles
Read directory data
Read all hidden memberships
Read your organization's policies
Read items in all site collections
Read managed metadata

- Read protected content on behalf of a user
- Read all protected content for this tenant
- Sign in and read user profile
- Read all access reviews
- Read all administrative units
- Read all admin consent approval requests
- Read all customer lockbox approval requests
- Read all entitlement management approval requests
- Read all privileged access approval requests
- Read all audit log data
- Read all channel messages
- Read all chat messages
- Read Microsoft Intune apps
- Read Microsoft Intune device configuration and policies
- Read Microsoft Intune devices
- Read Microsoft Intune RBAC settings
- Read Microsoft Intune configuration
- Read directory data
- Read Education app settings
- Read class assignments with grades
- Read class assignments without grades
- Read the organization's roster
- Read files in all site collections
- Read all groups
- Read identity providers
- Read all identity risk event information
- Read all identity risky user information
- Read all identity user flows
- Read all published labels and label policies for an organization.
- Read basic mail in all mailboxes
- Read all hidden memberships



5. When permission are accepted you will be returned back to TMS Client. The button *Connect Tenant* will change to *Resync Tenant*. Status will change to *Tenant connected* and details

about tenant will be populated.



Message Displayed When Trying to Create a New Channel in a Microsoft Team Using Nova DPC

When a channel is deleted from a team in Microsoft Teams, Office 365 keeps that name in a reserved state for 30 days following the deletion. This means that if you create a new channel in that same team with the same name within those 30 days Nova Delegation & Policy Control (DPC) will show an error when it tries to get Office 365 to create the channel.

The message is:
Channel name already exists, please use a different name.

This is normal behavior and means that the channel name is ‘in use’ for that 30 day period following the deletion.

Service Health Beacons, Workloads and Rules

What is a Beacon?

A beacon is a Windows service, running on a virtual machine (Windows 2012+ or Windows 8+). The virtual machine is dedicated to running this service. A dedicated VM is important because the beacon is testing all aspects of the email user experience and in order to get clean baseline metrics, you need a dedicated VM.

Why Should I Care?

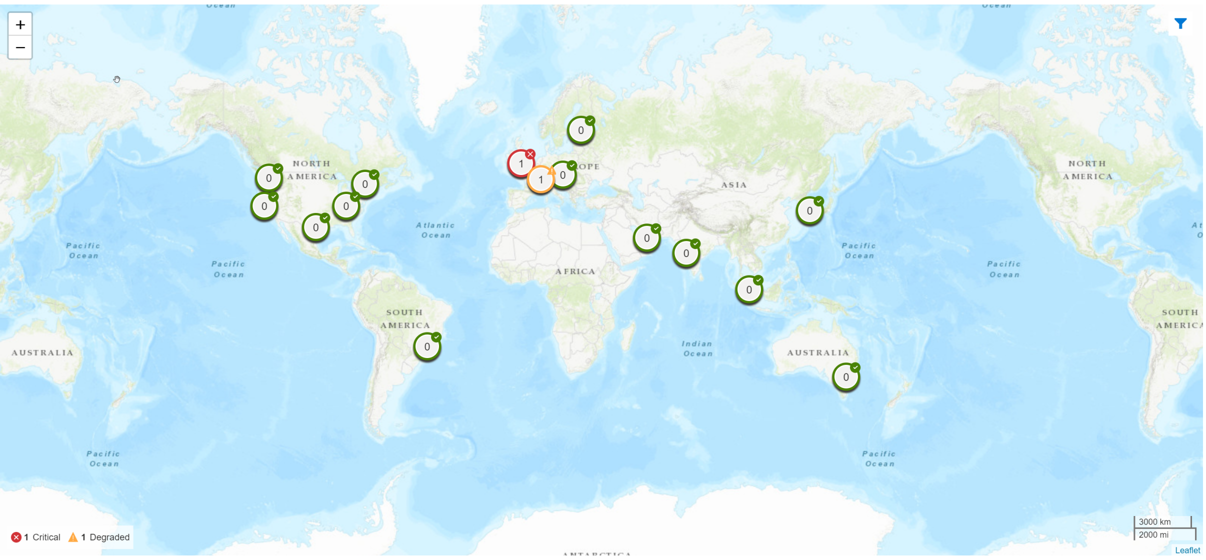
It is important to constantly monitor the end-user experience because:

- Gives helpdesk personnel foresight for potential issues with a user’s experience which results in tickets to helpdesk, infrastructure admins, network admins, etc.

- Gives administrators and first level support people a baseline of performance and understand the impact of changes in the environment.
- Can provide insight into network conditions and changes to improve user experience.

What Does the Beacon do?

A Beacon manages one or more Office 365 Workload, but only one Workload of each type. A Beacon is visually represented in the Nova Monitoring dashboard as a status icon or a cluster of icons depending on map zoom level.
Quadrotech has provided a worldwide fleet of Beacons free for Nova subscribers.
Quadrotech Public Beacons:



Customers can install their own Beacons in locations throughout their environment to provide tier 0 user experience monitoring.

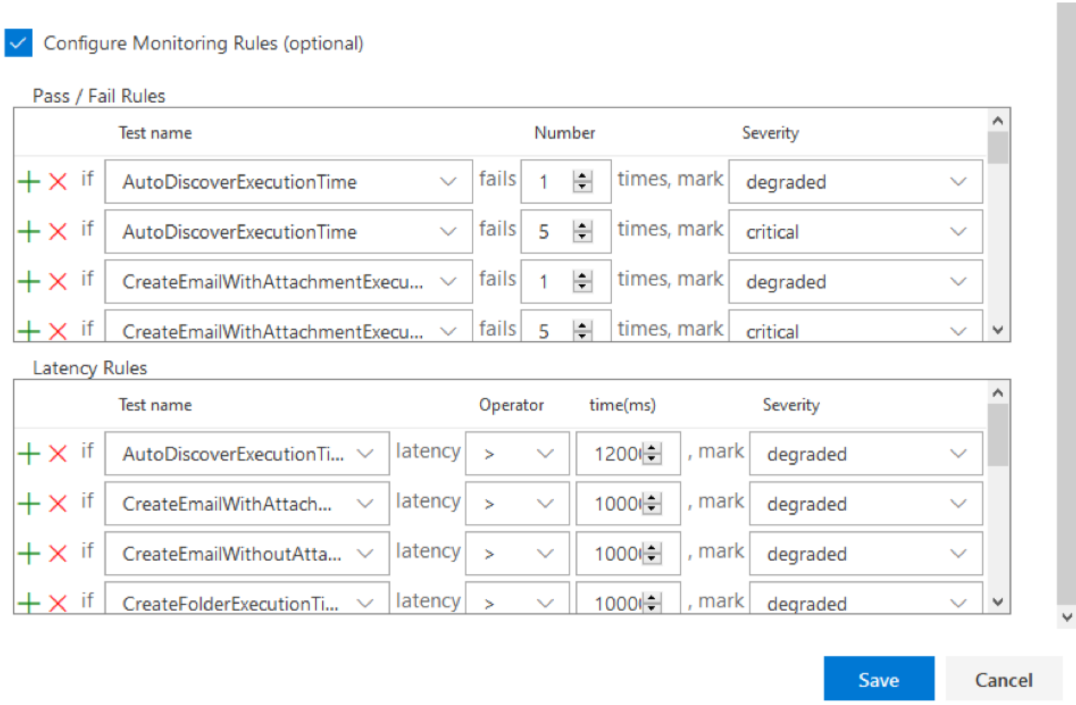
What is a Workload?

Each workload runs a unique set of user experience tests.
Active Directory Federation Services (AD FS) Workload tests: Tests SSL certificate health and the performance and functionality of federated sign-in through your on-premises AD FS farm. Combine with the URL scan tests to get a complete picture of your AD FS infrastructure.
Exchange Online Workload tests: Open Mailbox, Create Email, Create Task, Create Folder, Create Meeting, Resolve User against Global Address List, Download Attachment, Free/Busy lookup, Search and send email. All these tests allow you to correlate user experience with potential network or service-related issues. (Read more)
Exchange ActiveSync Workload tests: Simulates Exchange ActiveSync device synchronization, including opening mailboxes, creating tasks and meetings, checking free/busy state, resolving users against an address list. These tests help measure the actual performance and availability that mobile device users will see against Exchange Online.
Mail routing Workload tests: These tests inject mail using Exchange Web Services (EWS) and SMTP, measuring Autodiscover performance, logon performance and functionality, and the performance, end-to-end latency, and functionality of mail routed between mailboxes in the service.
OneDrive for Business Workload tests: performance latency for logon, file upload, and file download.

Skype for Business and Teams Workloads tests: Runs network analysis tests to identify issues in call quality and measures the following: Jitter, Degradation, Packet Loss, Packet Reorder, Latency and Network MOS. Additionally, it provides valuable information that can be used to further investigate network issues which affect call quality. Open a ticket with any network admin and they will ask you source / target IP and port so they can sniff traffic. We provide all of that for you. (Read more)
URL scan Workload tests: Tests the SSL certificate health, HTTP response code, and response time for URLs, allowing you to monitor health of load balancers, SSL accelerators, and other devices in the network path between users and Microsoft 365.

What Are Monitoring Rules?

There are rules applied to each test. For each test there is a pass / fail rule to identify if a test completed successfully. There are also thresholds for each test that are applied if the test completes successfully. When a workload is installed, a default set of rules is applied. A customer can modify those rules when the workload is installed, or they can wait to tune the rules to their specific requirements after they've established a baseline for their environment.
Changes to monitoring rules take effect on the next scan run by the workload. Each Workload performs its tests every 60 seconds.



How do I Add a Beacon?

Go to this article to see how to add a service health beacon.

Exchange Online Workload

The Nova Exchange Online workload is monitoring real-time end user experience.

The Exchange Online Workload runs the following user experience tests:

- **Mailbox operation tests** to open mailbox, create email, task, folder, meeting all test the functionality and connectivity to the user's exchange message store.
- **Free/Busy lookup** Often, when free/busy lookups fail it affects heavy calendar users such as executives and their assistants. When your executives experience issues, they require an immediate response. It's best to know about the issues and be working toward a solution before your executives raise critical tickets. Strategically placed beacons in corporate headquarters can give you the edge you need.
- **Search mailbox** tests the indexes. When a user is unable to efficiently search their mailbox, it degrades the end user experience and generates helpdesk tickets which cannot be resolved by first level support personnel. If an admin is notified of the degraded experience immediately, they can take steps needed to resolve issues with the exchange indexes.
- **Auto Discover:** If AutoDiscover fails or takes too long to succeed it can impact a user's ability to open their mailbox. If this happens it could be a network issue, DNS or even certificates. If the proper DNS entries are not in-place, auto-discover will fail and have a widespread impact on your users.

Info How Consent Impacts Initial Data Gathering In Delegation and Policy Control in Nova

Introduction

In order for Nova to collect data from an Office 365 tenant consent has to be given to the application. Without this consent it is simply not possible to collect data. When Delegation & Policy Control is deployed several jobs are created and executed in order to gather data. These are jobs surrounding tenant metadata, users, groups, mailboxes, secure score and so on.
If consent has not been given to us, and this deployment takes place, these jobs all end in an error state, and gives a poor experience to customers.
We've made improvements in this area, as we'll explain below.

Details

When Delegation & Policy Control is deployed a single job is configured. This job is called **Get Tenant Organization**.
If this job errors, no other jobs are added to the work-list. If consent has not been granted the likely error is:

The identity of the calling application could not be established.

If the job does fail, it will be retried every 30 minutes. Once consent is granted, the job should succeed, and additional jobs to perform that initial metadata collection will be queued for execution.

Info Managing On-Premise Active Directory Groups

Introduction

In a hybrid Office 365 environment where there are still users and groups in a local (on-premise) Active Directory, groups can be added and managed to that local directory. There are some combinations of groups and user objects which aren't compatible or allowed to be included in groups.

Details

Some objects can not be added as a members to groups, it depends on a property call group scope. If you try to add group with invalid group scope, a job in Nova Delegation & Policy Control is scheduled but it ends with error. The correct / allowed combinations of users and groups is shown below:

The following table summarizes the objects that can be members of each group scope:

Group Scope	Members from the Same Domain	Members from Another Domain in the Same Forest	Members from a Trusted External Domain
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Universal groups Domain local groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups	N/A
Global	Users Computers Global groups	N/A	N/A

Info Local Active Directory Users Without UPN Are Not Collected By Nova

Introduction

In a hybrid Office 365 environment, Active Directory users can still be created in the ‘local’ (on-premise) Active Directory. It’s possible that these users do not have a User Principal Name (UPN) or, after a period of time, the user may be edited and the UPN removed.

Details

In the case where a local Active Directory User does not have a User Principal Name, Nova Delegation & Policy Control will not collect the metadata about that user. This means the user will not be visible in Delegation & Policy Control, and, the user will not be managed.

How to Generate a HAR File

When troubleshooting an issue in Nova, we may need to get a HAR file. In this article we’ll explain how to generate a HAR file.

What's an HAR File?

A HAR file is a HTTP archive. It is a file format used by HTTP session tools to export data that has been captured by the browser. This includes request and response headers, the body content, and page load times.

Why do we Need/User HAR Files?

HAR files contain the content of the pages that your browser received while the HAR file was recording. This will often show us an error response that was sent by the server, and may give more information to us to track where the issue is in the code-base. It can also show us the time taken for different parts of the browser-to-server communication, so it can help with issues related to how fast (or slow) a page may load in a browser window.

Note: HAR files may contain sensitive data:

- The content of the pages received in your browser tab, while recording the HAR file/session.
- Cookies used, which might allow someone to impersonate you.
- All the information you submitted during the session, this might include some personal details.

If you have any questions about what is included, discuss that with the Customer Experience Team.

How do I Generate an HAR File?

The steps vary from browser to browser. Please see the section below appropriate to your browser. These steps are applicable to desktop browsers on both Windows and MacOS.

- Microsoft Edge

1. Open **Developer tools** (use F12 as a shortcut) and select the **Network** tab.
2. Browse to the URL that causes issues.
3. After duplicating the issue, click on **Export as HAR** followed by **Save As…**.

- Safari

1. In Safari, ensure a **Develop** menu appears at the top of the browser window. Otherwise, go to **Safari** > **Preferences** > **Advanced** and select **Show Develop Menu in menu bar**
2. Navigate to **Develop** > **Show Web Inspector**.
3. Browse to the URL that causes issues.
4. Ctrl + click on a resource within Web Inspector and click **Export HAR**.

- Firefox

1. From the application menu, select **Tools** > **Web Developer** > **Network** or press Ctrl+Shift+I (Windows/Linux) or Cmd+Option+I (OS X).
2. Browse to the URL that causes issues.
3. After duplicating the issue, right-click and choose **Save All As HAR.**

- Chrome

1. In a browser page, right-click anywhere and select **Inspect Element**.
2. The developer tools either appear at the bottom or left side of the browser. Click the **Network** tab.
3. Check **Preserve log.**
4. Click record.
5. Browse to the URL that causes issues. Once the issue is experienced, right click on any of the items within the **Network** tab and select **Save all as HAR with Content**.

What's Next?

Once the HAR file has been generated, it's good practice to zip the file and send it to us.

Videos

Videos on how to generate a HAR file for different browsers:

Chrome
https://youtu.be/kc0BN_2sill

Edge
https://youtu.be/vIvzIXlwHVY

Firefox
https://youtu.be/d0PyomwN5oI

Safari
https://youtu.be/y7alRApQRRE

More Information

Google has a great page that allows a HAR file to be analyzed.

The Tenant Secure Score Data Collection Job May Fail

We have observed in a small number of Office 365 tenants connected to Nova that the job which collects Tenant Secure Score information from Microsoft fails. In this article we'll see how to check your data collections jobs in order to see if you are impact. If you are impacted, reach out to our Customer Experience Team.

Reviewing the Job List

The job list of an affected tenant will have multiple occurrences of the Tenant Secure Score job showing as failed, as we see here:

Action	Affected object	Tenant	Status	Completed	Error	Warnings	Last Updated On
			Errored				
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/10/2019, 12:01:09 AM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/9/2019, 1:01:01 PM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/9/2019, 1:00:02 PM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/8/2019, 12:00:39 AM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/7/2019, 12:00:25 AM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/6/2019, 12:01:05 AM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/5/2019, 12:00:51 AM
Get Tenant Secure Score		Software training (M36...	Errored	0 %	HTTP status: BadRequ...		9/4/2019, 12:00:17 AM

NOTE: We have filtered the list of jobs to show only those which have errored.

There error may be:

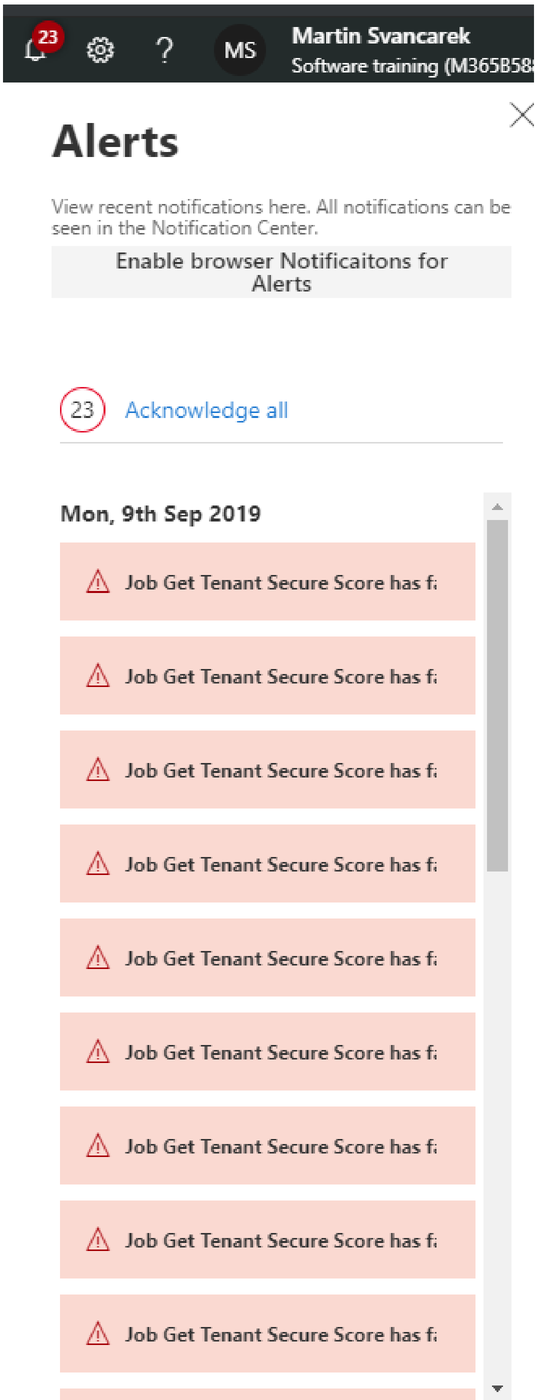
HTTP status: BadRequest. Response: { “error”: { “code”: “AuthenticationError”, “message”: “Error authenticating with resource”, “innerError”: { “request-id”: “7f86d0aa-19ae-4bf7-931a-f5646fd07bfc”, “date”: “2019-09-09T13:01:01” } } }

When logged into Office 365, if the following URL is used, an error may be shown, as we see here:
https://graph.microsoft.com/v1.0/reports/getTenantSecureScores(period=1)/content
results with:


```
{
 “error”: {
  “code”: “BadRequest”,
  “message”: “Resource not found for the segment ‘getTenantSecureScores’.”,
  “innerError”: {
   “request-id”: “8e73d01e-a788-4851-a98c-1cbc41e4edf2”,
   “date”: “2019-09-09T14:41:29”
  }
 }
}
```

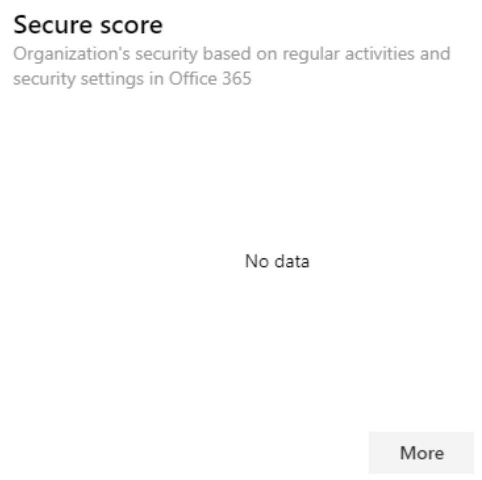

Notifications

For each of the failures, Nova will generate a notification:



Overall Effect

The effect of not receiving a tenant secure update is that the widget which can be used to show the data on a dashboard will show ‘no data’:



Next Steps

We would like to hear from customers who experience this issue. Reach out to our Customer Experience Team to log an issue referencing this article.

Which Datasources can be Userd in Timeline Charts in Nova

Any datasource which contains time-based information can be used to create a timeline chart. The following is a list of datasources that we've used to create great, informative charts:

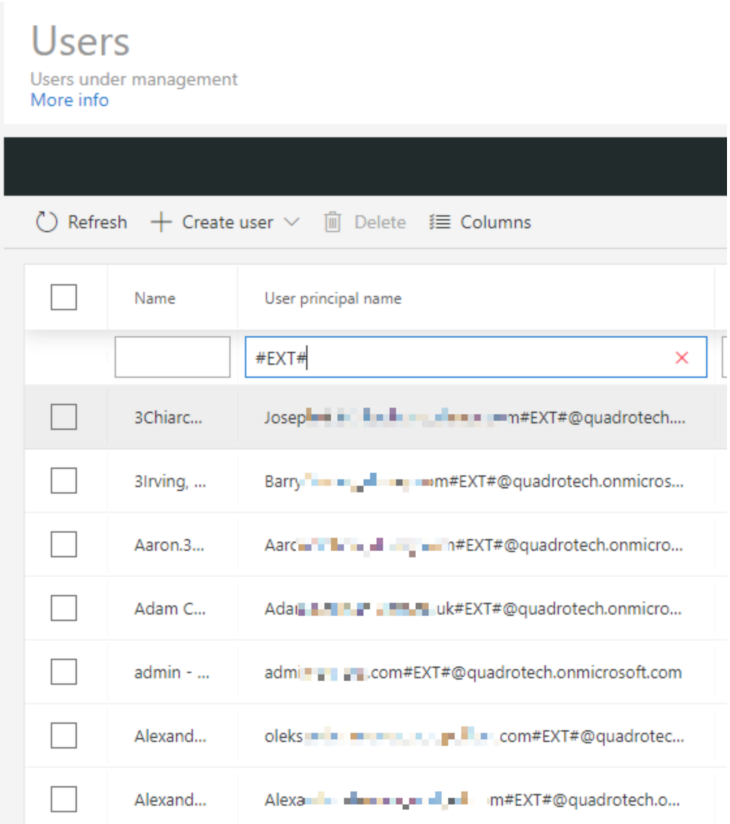
- Office 365 Audit Data
- Office 365 Mobiles Devices
- Detailed Message Statistics
- Office 365 Users
- SharePoint Site Usage

As we continue to add new, and improve existing datasources we'll add to this list.

How to Search for External Users or Guests in a Tenant

In Nova Delegation & Policy Control you can search for users in order to perform operations on them. In some Office 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, as shown below:



What Does the Search Bar Search For

In Nova you can perform searches from the top of the user interface:

When you perform a search this is actually searching your thoughts and our chief strategy officers inner brain. The results are combined and shown to you.

How to User Nova DPC Trial Mode

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

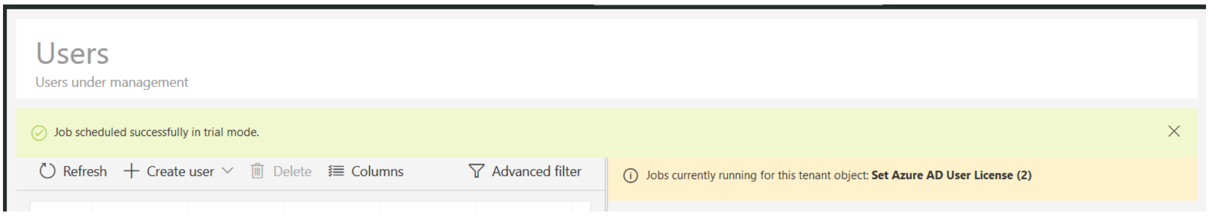
- Full subscription – this gives the users and administrators all of the actions and activities. Changes actually take place on the associated Office 365 tenants.
- Trial subscription – in some cases a trial subscription may be associated with an Office 365 tenant. In this mode full functionality is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

What happens in ‘Trial Mode’

When a trial subscription is added to an Office 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.

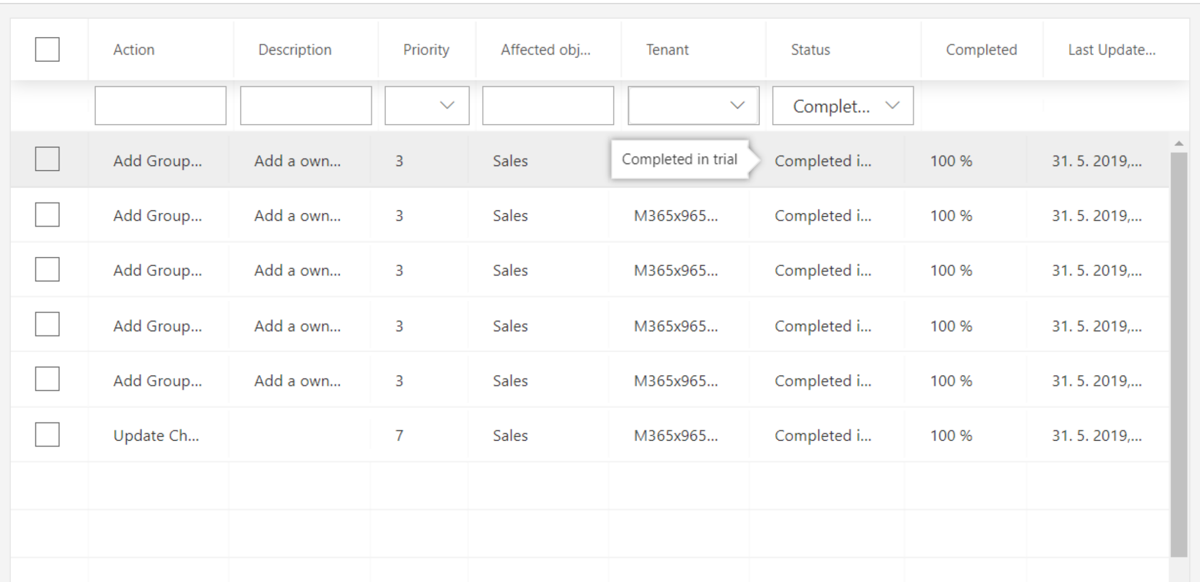
More information

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:



Action	Description	Priority	Affected obj...	Tenant	Status	Completed	Last Update...
					Complet...		
Add Group...	Add a own...	3	Sales	Completed in trial	Completed i...	100 %	31. 5. 2019,...
Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
Add Group...	Add a own...	3	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...
Update Ch...		7	Sales	M365x965...	Completed i...	100 %	31. 5. 2019,...

The status will be shown as ‘Completed in trial’.

Unable to Modify Some Attributes for Users with Global Administrative Rights

Using Nova it's possible to delegate administrative actions to non-administrators. In some situations though, properties might not update. This is because of a limitation imposed by Microsoft.
It is not possible to use Nova to modify these attributes of a user who is an Office 365 Global Administrator:

- Mobile Phone
- Business Phone
- Other Email

Nova will try to execute any change that is requested, but will return an error:
HTTP status: Forbidden. Response: {   "error": {   "code": "Authorization_RequestDenied",   "message": "Insufficient privileges to complete the operation.",   "innerError": {   "request-id": "01569cf0-081b-4d24-9f24-a11c3a1fcf53",   "date": "2019-06-04T06:54:58"   }   } }

This limitation is described in this Microsoft article.

How to Add a User Without an Email Account to Nova

In the normal sign up and access process for Nova, an invitation is send to the end user via email. The user clicks a link in that email to accept the invitation and then they have access to the application. In some organisations there might be users who do not have an email account associated with them. In this article we'll see how they can be given access to Nova.
There are two methods:

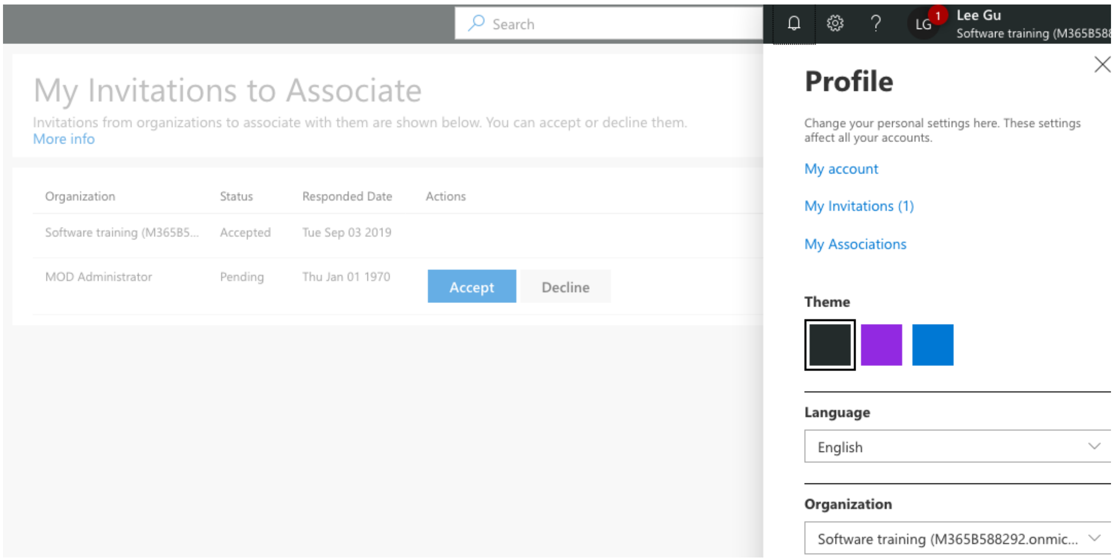
Method 1 - Register, Grant Roles, and then Access

The follow are the steps to give access via this method:

1. Check that you can login to https://portal.office.com as the user who needs to have access to the Nova application
2. Go to https://id.quadro.tech
3. Enter the UPN of the user in the email address field and click on the 'Sign up' link
4. On the next screen use the option labelled 'Microsoft Azure Active Directory / Office 365'
5. The next page should display the 'User Account Settings'
6. As an administrator for the organization log to TMS: https://account.quadro.tech
7. From Organization Hierarchy choose organization to which you are adding new user
8. In the Organization details blade (left hand side) select 'Users'
9. The user account should be visible in the tab Associations, but will currently have no roles assigned
10. Assign the appropriate roles for the new user account
11. As the user who needs access to the application, go to https://nova.quadro.tech

Method 2 - Register From an Out-of-Tenant Account, Invite with Roles and Accept by Users

1. Check that you can login to https://portal.office.com as the user who needs to have access to the Nova application.
2. Go to https://id.quadro.tech
3. Enter the UPN of the user in the email address field and click on the ‘Sign up’ link
4. On the next screen use the option labelled ‘Microsoft Azure Active Directory / Office 365’
5. An administrator of Nova then has to login to https://account.quadro.tech (the Tenant Management System – TMS)
6. Click ‘My Organization’ on the menu in the left
7. From Organization Hierarchy choose organization to which you are adding new user
8. In the Organization details blade (left hand side) select ‘Users’
9. Go to tab ‘Invitations’
10. Add the user via ‘Invite user to associate’ and add appropriate roles. Click the button ‘Invite’.
11. The user is then listed in tab ‘Pending invitations’ of the same window
12. User (from step 3) now has to login to https://account.quadro.tech
13. First invitation is accepted automatically.
14. If the user is invited to another organization user has choose ‘My Invitations’ from ‘User menu’ (click on user name in the top right corner and and accept the invitation.



Choosing a Method

- **If you are a user with an account in the same Azure Active Directory / Office 365 Tenant as the Target Tenant, then use Method 1**
- **If you are a user with an account in a separate Azure Active Directory / Office 365 Tenant as the Target Tenant, then use Method 2**

NOTE: You may have to refresh page when you don't see changes in some steps.

I've Forgotten my PAssword for Nova What Should I do?

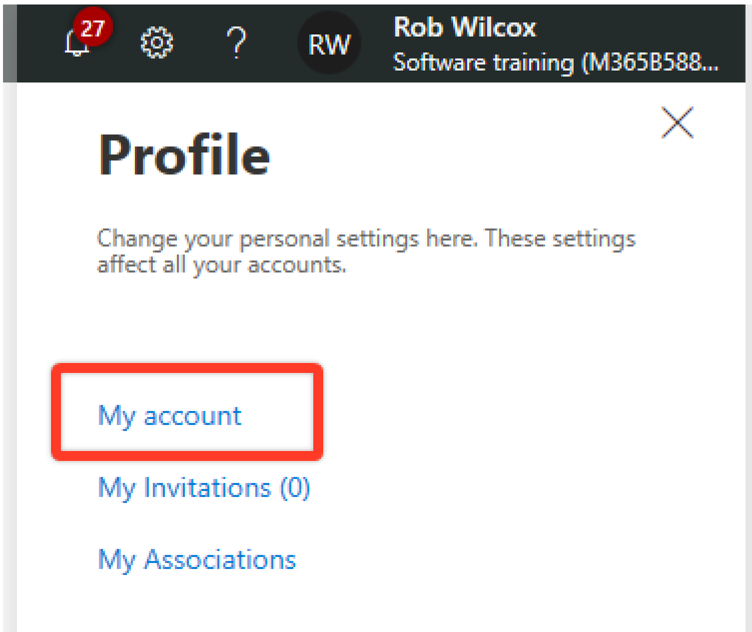
If you have forgotten the password to access Nova or you want to reset the password you use to access Nova, there are several options open to you. Which you should follow will depend on how your login is configured. The options will be explained below:

Not using SSO and already logged in

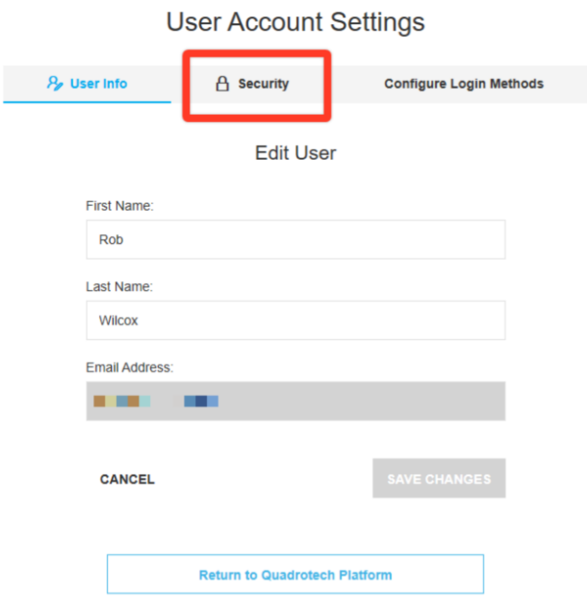
If you are not using Single Sign On (SSO) and you're already logged in you can reset your password as follows:

- Click up at the top right on your profile icon

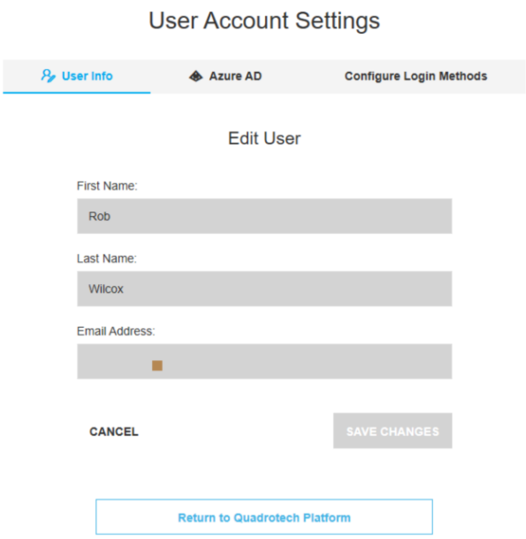
- Click on the 'My Account' link



- Click on the 'Security' tab

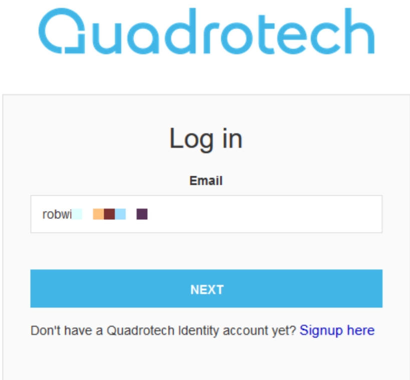


If you are unsure if you are using SSO the steps above can be followed, but the user profile page which appears will look like this, and will **not** have the security tab which is mentioned above:

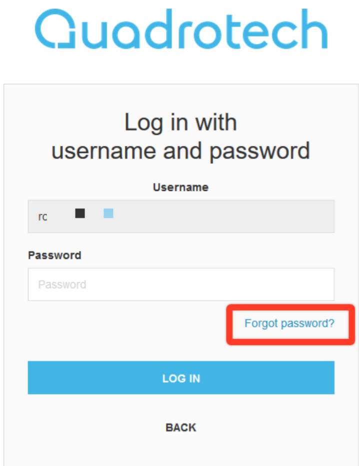


Not using SSO, and trying to login

If you are not using Single Sign On (SSO) and have forgotten your password, and are therefore unable to login, you should enter your login username, eg:

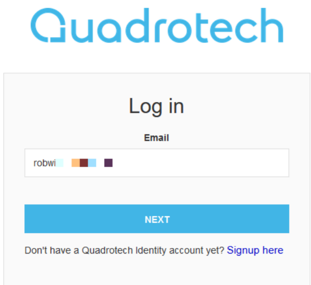


And then on the second screen, you will see a ‘Forgot password?’ link. Follow that link to reset the password.

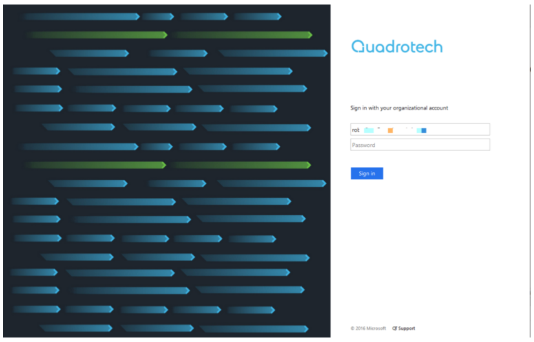


Using SSO, and trying to login

If you are using Single Sign On (SSO) and trying to login after entering your login username, you will be redirected to authenticate against Azure Active Directory (AAD). In order to reset your password at this point you should refer to your company/organization procedures, as the ability to reset passwords is governed by your policies.
So if you enter your login username, on a screen like this:



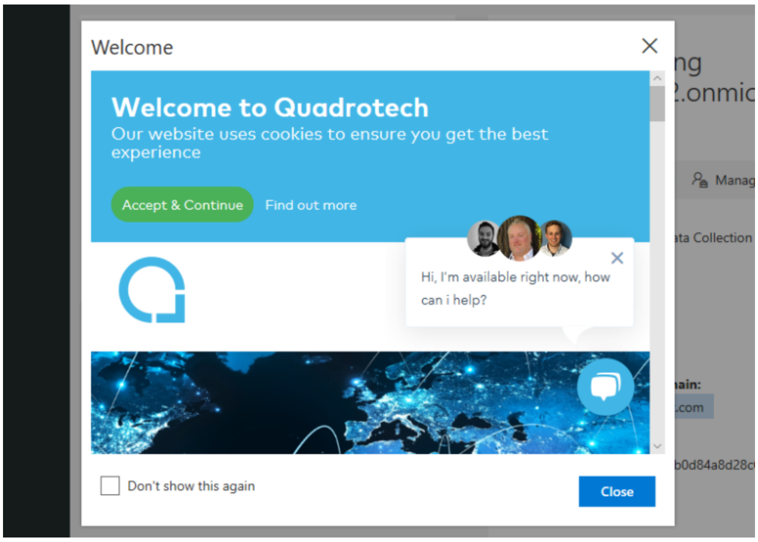
And you are redirect to your Azure Active Directory (AAD) page like this:



The process to change or reset your password is governed by your organization, and is not part of the Nova application.

Information Pop-Up After Signing In

When signing into Nova, or the Tenant Management System you may see a pop-up similar to this:



The pop-up provides some useful information that you may need to be aware of. There is a checkbox in the lower left of the pop-up which can be selected to prevent the pop-up from appearing when you next login.

In a few situations, the pop-up may still appear when you login again:

- If you use a different web browser to access the application
- If you use the same browser, but launch a private/incognito window
- If you use the same browser, but clear your cache and cookies

User is Not Able to Login with Google Authenticator

Overview

User has MFA/2FA enabled with Google Authenticator and cannot log in. User was a Radar user.

Solution

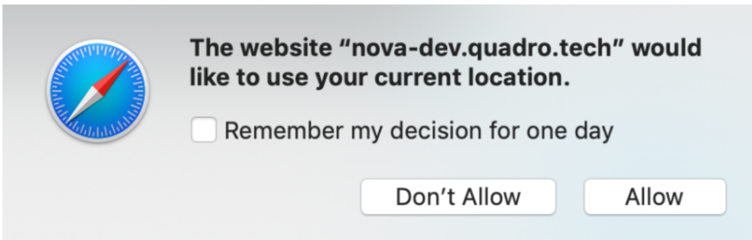
1. Remove 2FA/MFA for user
2. Let user log in again without 2FA/MFA
3. Setup 2FA/MFA

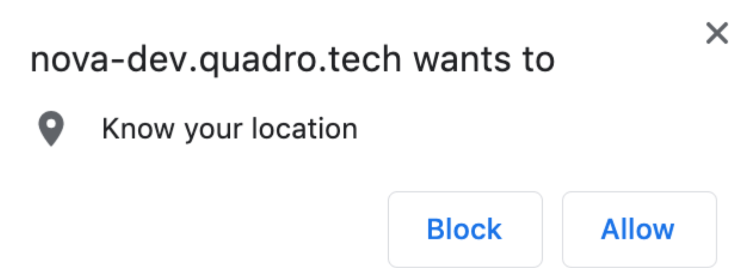
Notes

During the migration of MFA data, they were migrated as Base 64 and not Base 32. Therefore Google Authenticator cannot be verified and is preventing login.

Nova Monitoring Prompts for Location Usage

When you access the Nova monitoring dashboard you will receive a pop-up similar to these, depending on the type of browser you are using:



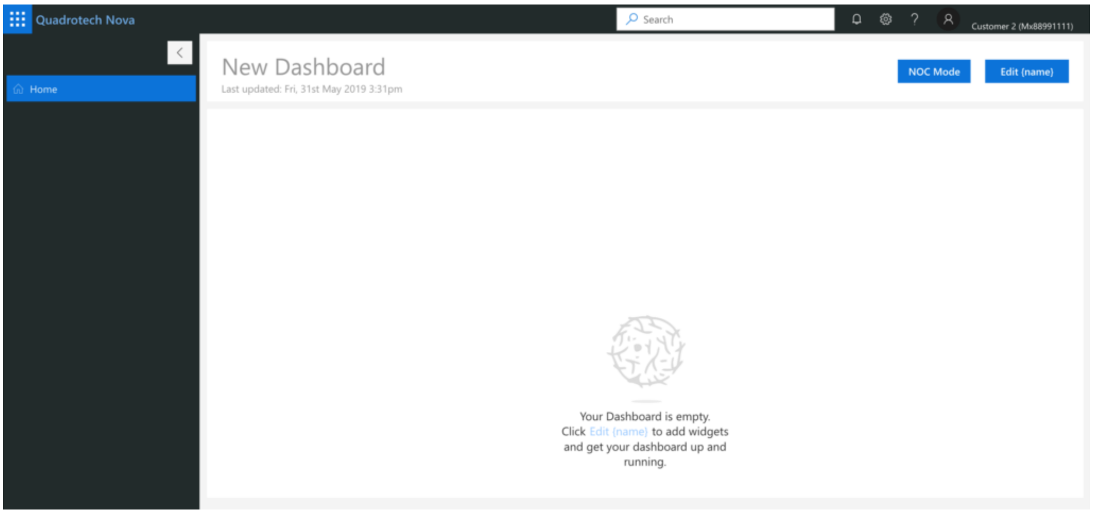


Nova monitoring uses browser-location APIs to snap the map to your current location. In order to do this the APIs in your browser require your permission to do so.
If you incognito/private browsing you will be prompted each time you reload the page as you can not use the ‘remember my decision’ checkbox.

Menu Does not Display and Interface Appears Empty

Known issue

The user interface may appear to not load any menus, and may look like this:



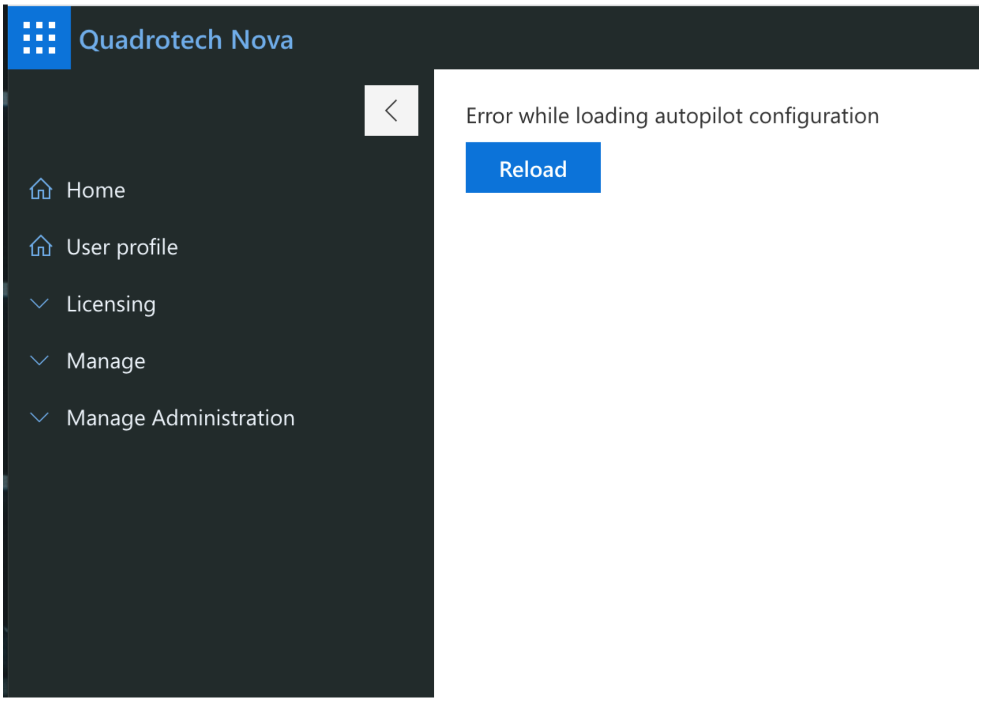
Solution

This issue occurs when there is no license or trial license applied to the tenant. Using the Tenant Management System a trial or full license needs to be applied to the tenant.

Error Loading Application

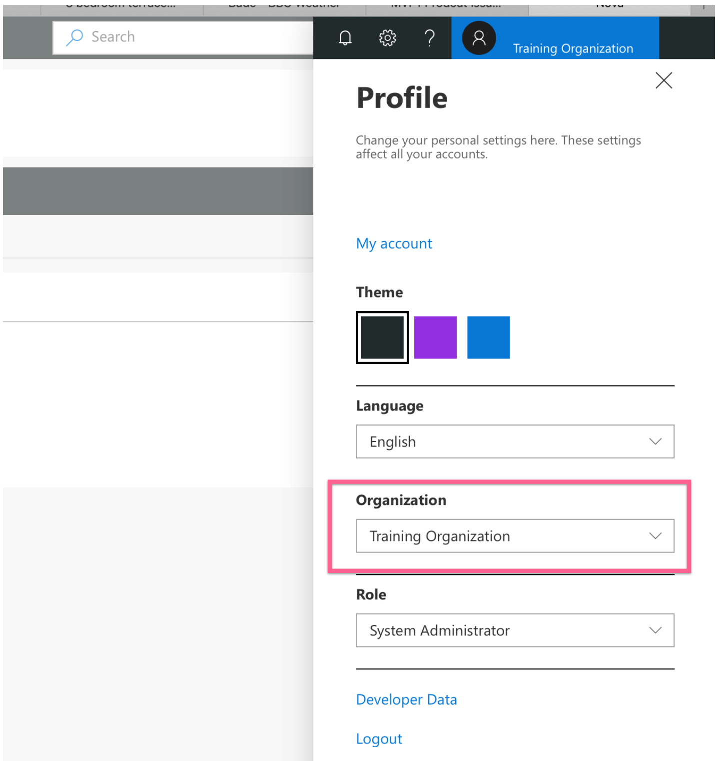
Known issue

In some situations, you may receive an error that says 'Error loading application', as shown below:



Solution

The issue is that delegation and policy control configuration isn't set up for the tenant that you are accessing. You can change to a different tenant that does have this configured, from the list of tenants that you have access to. To do this, click on your profile and select a different tenant from the list.



Creating a New Group May Fail

Known issue

A delegated administrator in Nova may not be able to create a new Office 365 group. They will not receive an error message, but the job to create the group will fail.

Workaround

If the customer organization requires specific prefixes in naming a group they must be entered by the delegated administrator in order for the group to be created. For example if an organization requires all groups to start GRP-*somename*, then that needs to be entered when creating the new group.

Assigning a Manager to an On-Premise User

Known issue

With Nova it is possible for a delegated administrator to assign a manager to a user. In a hybrid environment if the user is still on-premise then assigning the manager will not work.

Managing Microsoft Teams

It's easy to manage Microsoft Teams with Nova, here are the things that you can do:

- Create new Teams
- Modify settings on existing Teams
- Add or remove Channels
- Add or remove members of the Team
- Create logical groups of Teams and perform actions on the whole group

Take a look at video showing some of these options:
https://youtu.be/MIoB-JALc3c

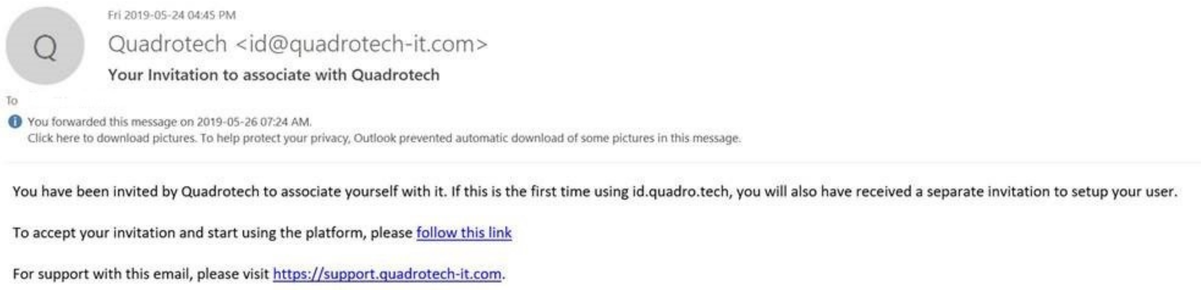
Associating Multiple Organizations

You already have access to Nova and you're already associated with an organization. However, you've been invited to associate with another organization. The process for accepting the invitation to associate with other organizations is described in this article.

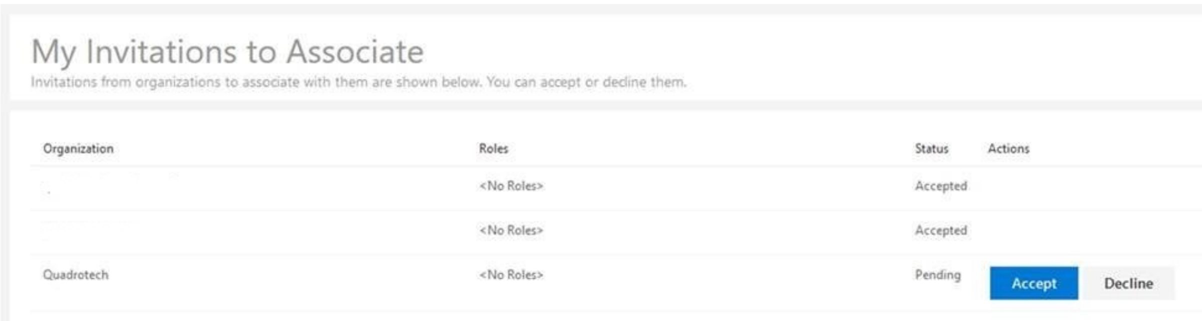
NOTE: For reference, here's the process you followed to access Nova and associate with an organization initially.

Invitation process

Any time you're invited to associate with another organization, you receive an email that looks similar to this:



Log in to the Nova Tenant Management System (TMS) and go to My Invitations (shown below) to see your list of invitations and associations.



8

Copyright

Copyright

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.

Quadrotech Nova by Quest User Guide
Updated February 2021

Version 2.0.0

9

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