Quest®

Quadrotech Nova security backgrounder

General security and privacy

Our overall privacy policy is published on our website and sets out what data we collect and use for customer interactions with our website and support team.

Quadrotech Nova and GDPR

Quadrotech Nova complies with the European Union General Data Protection Regulation. As required by GDPR, we have Data Protection Acts (DPAs) in place with our suppliers, procedures to remove customer and partner data upon request and upon the termination of a business relationship, and collection minimization procedures to ensure we neither collect nor retain unnecessary or excessive information. Our standard data processing agreement is available to view. For specific inquiries about GDPR compliance, please contact privacy@quest.com.

Quadrotech Nova security and privacy

Why service accounts?

Quadrotech Nova is a complex multi-component SaaS application that has a variety of solutions available. Its functionality can be divided into two areas:

- It lets you see data about objects in Microsoft 365 tenants
- It lets you do things to objects in Microsoft 365 tenants

Service delegation is a key feature of Nova, meaning that users who do not have permissions *in Microsoft 365* can still see and do things that would normally require elevated permissions.

Multi-tenant access is another solution of Nova, meaning that a user who signs in to Nova using an account in tenant A may be able to see and complete actions in tenants B-Z that would normally require the user to have a privileged account in each of those tenants.

Nova uses *service accounts* to help provide both the 'see' and 'do' feature sets.

Service accounts and what they do

Microsoft offers two primary API sets for accessing Microsoft 365 services; PowerShell and Microsoft Graph. Graph API access is managed through the Azure AD enterprise applications deployed as part of Quadrotech Nova provisioning in a tenant. However, PowerShell access requires the Nova application to authenticate to the service using a named credential instead of the enterprise application registration. This is where a service account is required.

Nova supports four types of service accounts. Only the first type is required.

1. The Reporting service account is used to gather data from the target tenant using both PowerShell and Microsoft Graph. It is a read-only account and is required for all tenants. We recommend and have tested assigning the Global administrator role to this account.
2. The Delegation and Policy Control (DPC) service account is used to read *and* write data to the target tenant. This account requires the Global administrator role. This account is only required if the target tenant is provisioned for DPC.
3. The DPC on-premises agent (OPA) is used to read and modify objects in the on-premises Active Directory. When the OPA is used, it must be a member of the Domain Admins or Built-In Admins AD group in each domain in the forest under management and have the 'Logon as a service' account right. This account is only required if the target tenant is provisioned for DPC and the customer wants writeback services to on-premises objects.
4. Private monitoring beacons, if deployed, must be configured with Office 365 account credentials for the test mailboxes they will use. Each beacon will normally have a unique test account assigned to it. These accounts do not require elevated privileges. If private beacons are deployed in a tenant, these service accounts are required.

Encryption

Nova makes extensive use of data encryption for data in transit and at rest:

- Traffic from Nova users is encrypted using HTTPS in their web browser.
- API traffic between the Nova application and Microsoft's services is all encrypted. Graph traffic is natively encrypted as it's HTTP requests; other protocols, such as remote PowerShell, are tunneled over HTTPS.
- All Nova data is encrypted at rest.

Permissions

A list of Microsoft permissions for reporting can be found here. A list of Microsoft permissions for DPC can be found here. A list of AAD Graph, Microsoft Graph API and Office 365 Exchange Online permissions can be found here.

Service account credential storage

All service account credentials held by Nova for reporting are stored and encrypted, in two places:

- The Service Account password is encrypted before it leaves the client machine setting the password, whether that is via the User Interface or PowerShell script. It is therefore sent in an encrypted form to our backend servers. Only our job collection servers have the private key to decrypt this password.
- The encrypted service account password is then further protected by being stored in Azure Key Vaults, where only our 'job engines' (those services that collect data) have access to the key vault to obtain the data.

Service account credentials for private monitoring beacons are stored, locally encrypted, using the Windows system cryptography libraries and key material from the X.509 certificate issued by the Nova environment to that individual beacon.

Multi-factor authentication and conditional access

As of May 2021, Microsoft does not support the use of multi-factor authentication (MFA) for accounts used as service accounts in Office 365. This is not a Quadrotech Nova limitation; it's a restriction imposed by Microsoft. The default policies applied by the service will break the Nova service account access because they require MFA for accounts that hold the Global administrator role.

Microsoft's recommended solution is to enable conditional access white listing for IP addresses used to access M365 services using these service accounts. Note that the default conditional access policies available to all Office 365 customers do not support whitelisting; customers who do not currently have O365 licenses with support for the full set of conditional access features will need to purchase an Azure AD P1 or P2 license from Microsoft. Conditional Access policies also require manual creation.

The list of IP addresses used for the reporting service account is here. The IP addresses used for the DPC service account is here.

The DPC On Premises Agent and monitoring beacon service accounts are not subject to Microsoft's limitations and do not require whitelisting.

Auditing for service account access

Every write action taken by a Quadrotech Nova DPC user is recorded in the Nova DPC audit log. This audit log is available through the Manage Administration > Audit Log command. Actions performed in the target tenant by a user's Nova DPC request will appear in the target tenant's Microsoft 365 audit log as having been performed by the DPC service account configured for that tenant. Audit entries for the reporting data collection service account are in the TMS client under the Data Collection tab.

In addition, every action taken inside the Nova Services Framework is audited by a special security middleware layer and retained in audit logs accessible to internal support staff.

What data is captured and stored by Nova?

Quadrotech Nova captures a wide range of data and metadata once a tenant is enrolled. This data includes information about user and administrator identities taken from Azure AD, information about user activity (such as signins, file sharing, and permission changes), information about usage of specific workloads (such as counts of email or Teams messages sent and received), information about system configuration changes, and data about where and how users interact with Office 365 services. Some of this information falls under the definition of personally identifiable information under the EU GDPR.

Nova does *not* capture, store, or process information about the contents of individual user mailboxes or files; it does not read or scan file or mailbox contents. However, metadata such as file names, names of Microsoft 365 Groups or Teams, or IP addresses will be collected and retained as a normal part of our operations.

All data gathered is collected using publicly documented Microsoft APIs, using either PowerShell (with the service accounts as described earlier) or the Nova Azure AD enterprise application.

All data in Nova except data retrieved from the Office 365 audit log is retained as long as the tenant subscription is active. Audit log data is retained for 7 days by default, or longer if the customer has purchased an Advanced Audit subscription.

All stored data in Nova is encrypted at rest using the default database encryption methods provided by AWS and Azure.

When a customer cancels a service, we remove all data and metadata related to that customer. Any customer wishing to have their data deleted may do so by contacting privacy@quest.com.

Where is the data stored?

All data collected for customers based in the EEA is maintained only in the EEA. Data collected for customers based in North America is generally retained in North America. Data collected for customers in the rest of the world will be retained in the EEA.

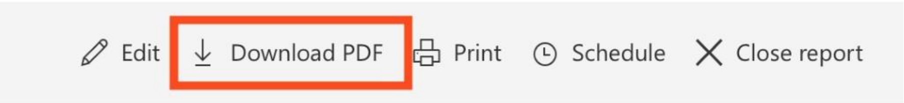
How is customer data separated?

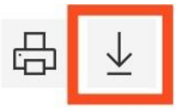
Quadrotech Nova reporting data is maintained in a shared set of databases, with each tenant's data marked with its tenant ID. The service account for each tenant reads data from Microsoft and that data is stored in the shared databases. All customer access to reporting data is mediated through the Nova data access layer, which is authenticated using accounts from the customer domain, so customers do not have access to any data other than their own. Customers can define their own logical rules (known as 'virtual business boundaries') to further restrict data access within a tenant; for example, creating a boundary that allows administrators based in Germany to only see reporting data about users who are also based in Germany while denying that same data to administrators in every other country.

Nova delegation and policy control (DPC) maintains a separate independent database instance for each tenant that has DPC configured. DPC provides authorization and configuration policies to allow each customer to apply the scope of data access rights they want to grant each Nova-enabled user or group.

How can data be exported from Nova?

In Quadrotech Nova, it is possible to download a report as a PDF file. It's also possible to export individual sections of a report to CSV file. A report can also be scheduled and at the designated time/date a PDF file will be generated of the report and emailed to the recipients specified in the schedule.





In both situations, the resulting file is downloaded and stores on a users' local machine in a folder that they choose. After this the data can be distributed at the users' discretion. Report downloading is not audited or tracked by Nova.

Nova does not support a generally available facility to export data in bulk.

Who has access to Nova?

Before any user can access any Quadrotech Nova functionality, the user must be invited to associate with a specific tenant and then assigned a Nova role in that tenant. For example, austin@contoso.com may be associated with the contoso.onmicrosoft.com tenant and given the IT Administrator role and associated with the fabrikam.onmicrosoft.com tenant with the System Administrator role. The Nova role controls what the user can do in the tenant.

Nova allows the customer to choose an identity management (IdM) system for authentication. Azure Active Directory is the default IdM. All decisions about whether a user's credentials are valid, and whether the user should be allowed to log in, rest with the IdM.

In order for a user to be able to see reporting data, they must have a specific role: either the IT Administrator, System Administrator, Report Reader, or Radar Classic role in a tenant. Radar Classic is only for backward compatibility. Users who do not have a reporting-enabled role *and* a valid association with the tenant cannot access reporting data for a tenant.

User access to DPC is controlled by the policies assigned to the user. A user with the IT Administrator or System Administrator role has full access to create and manage DPC policies and objects; users that have specific authorization policies assigned to them are constrained to the set of actions assigned to them by the policies that apply to their accounts.