Quest® Nova Delegation and Policy Control

Security Guide

Quest® Quest® Nova Security Guide
Updated January 2024

Contents

Introduction

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity and availability.

This document describes the security features of Quest Nova Delegation & Policy Control. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About Quest Nova Delegation & Policy Control

Quest Nova Delegation & Policy Control provides granular delegation and policy control for Office 365, enabling you to assign pre-defined roles and responsibilities to specific users, such as help desk operators, country-level administrators, or even end-users setting boundaries far more precise than native delegation. Quest Nova also includes policy-based automation for authorization, service configuration and license assignment.

Quest Nova Delegation & Policy Control is hosted in Microsoft Azure and delivers most of its functions via Microsoft Azure cloud services.

Hybrid accounts are managed via Quest Nova On-Premises Agent.

Architecture overview

The following scheme shows the key components of the Quest Nova Delegation & Policy Control configuration.
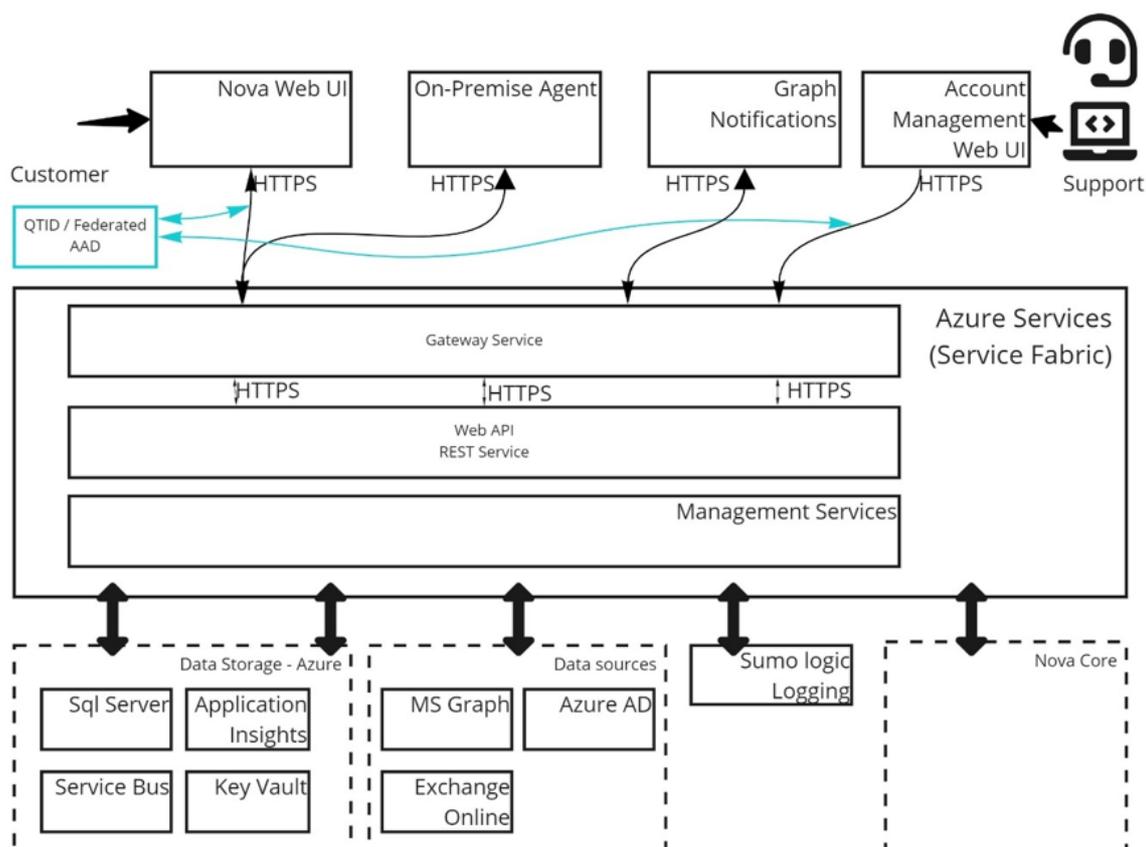
Figure 1: High-Level Architecture

Azure datecenter security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure and well protected datacenters in the world. They are subject to regular audits and certifications including Service Organization Controls (SOC) 1, SOC 2 and ISO/IEC 27001:2005.

Relevant references with additional information about the Windows Azure datacenter security can be found here:

- Microsoft Azure Trust Center: https://azure.microsoft.com/en-us/overview/trusted-cloud/

- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/trust-center/compliance/compliance-overview?service=Azure#Icons

- Microsoft's submission to the Cloud Security Alliance STAR registry: https://cloudsecurityalliance.org/star/registry/

- Whitepaper: Standard Response to Request for Information – Security and Privacy: http://www.microsoft.com/en-us/download/details.aspx?id=26647

- Microsoft Global Datacenters: Security & Compliance: https://www.microsoft.com/en-us/cloud-platform/global-datacenters

- Azure data security and encryption best practices: https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices

- Microsoft and FIPS:https://docs.microsoft.com/en-us/compliance/regulatory/offering-FIPS-140-2?view=o365-worldwide

Overview of data handled by Nova Delegation and Policy Control

Quest Nova Delegation & Policy Control manages the following type of customer data:

- Azure Active Directory and Office 365 tenant, users, groups, devices, drives and teams with their properties returned by Azure Active Directory Graph API including account name, email addresses, contact information, department, membership and other properties. Part of the information is stored in the product database.

- Exchange Online mailbox information and contacts with their properties returned by Exchange Online Management including email account name, email addresses, contact information and other information.

- On-Premises Active Directory organizational units, users, groups and contact with their properties. Part of this information is stored in product database.

- Application does not access, process or store content of drive or mailbox items.

- The application does not read end-user passwords of Azure AD or On-Premises objects.

- Application temporarily stores password required for operations like create Azure AD user, reset Azure AD user password, create on-premises user.

- The application stores administrative account name and password to access and modify mailbox information via Exchange Online Management.

- Management of on-premises objects is performed via integration with Quest Nova On-Premises Agent.

Admin Consent and Service Principals

Quest Nova Delegation & Policy Control requires access to the customer's Azure Active Directory and Office 365 tenancies. The customer grants that access using the Microsoft Admin Consent process, which will create a Service Principal in the customer's Azure Active Directory with consents required by Quest Nova Delegation & Policy Control. The Service Principal is created using Microsoft's OAuth shared secret based client credentials grant flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-client-creds-grant-flow. Customers can revoke Admin Consent at any time. See https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/delete-application-portal and https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.

Following is the base consent required by Quest Nova Delegation & Policy Control.

Quest Nova Delegation & Policy Control currently uses the Microsoft Exchange Online, SharePoint Management Shell, Azure Active Directory and MSOnline PowerShell API with support for the "limited permissions" model for Accounts, Email, SharePoint, Teams and OneDrive migrations, without needing global administrator permissions during migration. After the consent has been granted using the global administrator account, thereafter all operations will be driven by the token generated using app Service Principal.

The Admin Consent process of Quest Nova Delegation & Policy Control will create a Service Principal in the customer's Azure AD tenant with the following permissions.

Permissions requested
Review for your organization

Autopilot
App info

This application is not published by Microsoft or your organization.

This app would like to:

- Manage Exchange As Application
- Read all usage reports
- Manage apps that this app creates or owns
- Read calendars in all mailboxes
- Read and write calendars in all mailboxes
- Read contacts in all mailboxes
- Read and write contacts in all mailboxes
- Read and write devices
- Read Microsoft Intune device configuration and policies
- Read and write Microsoft Intune device configuration and policies
- Perform user-impacting remote actions on Microsoft Intune devices
- Read Microsoft Intune devices
- Read and write Microsoft Intune devices
- Read directory data
- Read and write directory data

- ⌄ Read and write domains
- ⌄ Read files in all site collections
- ⌄ Read and write files in all site collections
- ⌄ Read all groups
- ⌄ Read and write all groups
- ⌄ Read all user mailbox settings
- ⌄ Read and write all user mailbox settings
- ⌄ Read mail in all mailboxes
- ⌄ Read and write mail in all mailboxes
- ⌄ Send mail as any user
- ⌄ Read all hidden memberships
- ⌄ Read all OneNote notebooks
- ⌄ Read and write all OneNote notebooks
- ⌄ Read online meeting details
- ⌄ Read and create online meetings
- ⌄ Read all users' relevant people lists
- ⌄ Read all usage reports
- ⌄ Have full control of all site collections
- ⌄ Create, edit, and delete items and lists in all site collections
- ⌄ Read items in all site collections
- ⌄ Read and write items in all site collections
- ⌄ Invite guest users to the organization
- ⌄ Read all users' full profiles
- ⌄ Read and write all users' full profiles
- ⌄ Access the directory as the signed-in user

∨ Read directory data

∨ Read and write directory data

∨ Read and write all groups

∨ Read all groups

∨ Read all users' full profiles

∨ Read all users' basic profiles

∨ Sign in and read user profile

∨ Read hidden memberships

∨ Read and write domains

∨ Read all hidden memberships

∨ Manage apps that this app creates or owns

∨ Read and write all applications

∨ Read and write domains (deprecated)

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel   Accept

Location of customer data

When a customer signs up for Quest Nova, they select the region in which to run their Quest Nova organization. All computation is performed and all data is stored in the selected region. The currently supported regions are:

- East US
- West Europe (Netherlands)

Azure SQL Server databases are replicated three times in the same datacenter for resiliency against hardware failure. The data is replicated across different fault domains to increase availability. All replication datacenters reside within the geographic boundaries of the selected region.
See this Microsoft reference for more details: https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview.

Privacy and protection of customer data

The most sensitive customer data processed by Quest Nova Delegation and Policy Control is the Azure Active Directory tenant metadata. Other data are stored in SQL.

Each customer has his own database. The database stores the customer's sensitive data including Azure Active Directory and Office 365 users, groups, contacts and their associated properties. All customer's Azure SQL databases are protected and encrypted by Azure SQL Database Feature Transparent Data Encryption.

More information about Azure SQL Database Transparent Data Encryption: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-azure-sql

More information about Azure queues, tables, and blobs:

- https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blobs-introduction

- https://docs.microsoft.com/en-us/azure/security/security-storage-overview

- https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Separation of customer data

Quest Nova Delegation & Policy control is architected to prevent data commingling by separating customer data to customer exclusive resources. Customer data are differentiated by using unique customer alias, which is assigned during provisioning process. This alias is used to tie together customer specific service URLs, Azure Key Vault and Azure SQL Database resources.

Customer data is further separated as customer related services are isolated from any other OS process by the
Microsoft Service Fabric exclusive process model. See https://docs.microsoft.com/en-us/azure/service-fabric/service-fabric-hosting-model#exclusive-process-model for more information.

Network communications

The following scheme shows the communication configuration between key components of Quest Nova Delegation and Policy Control.
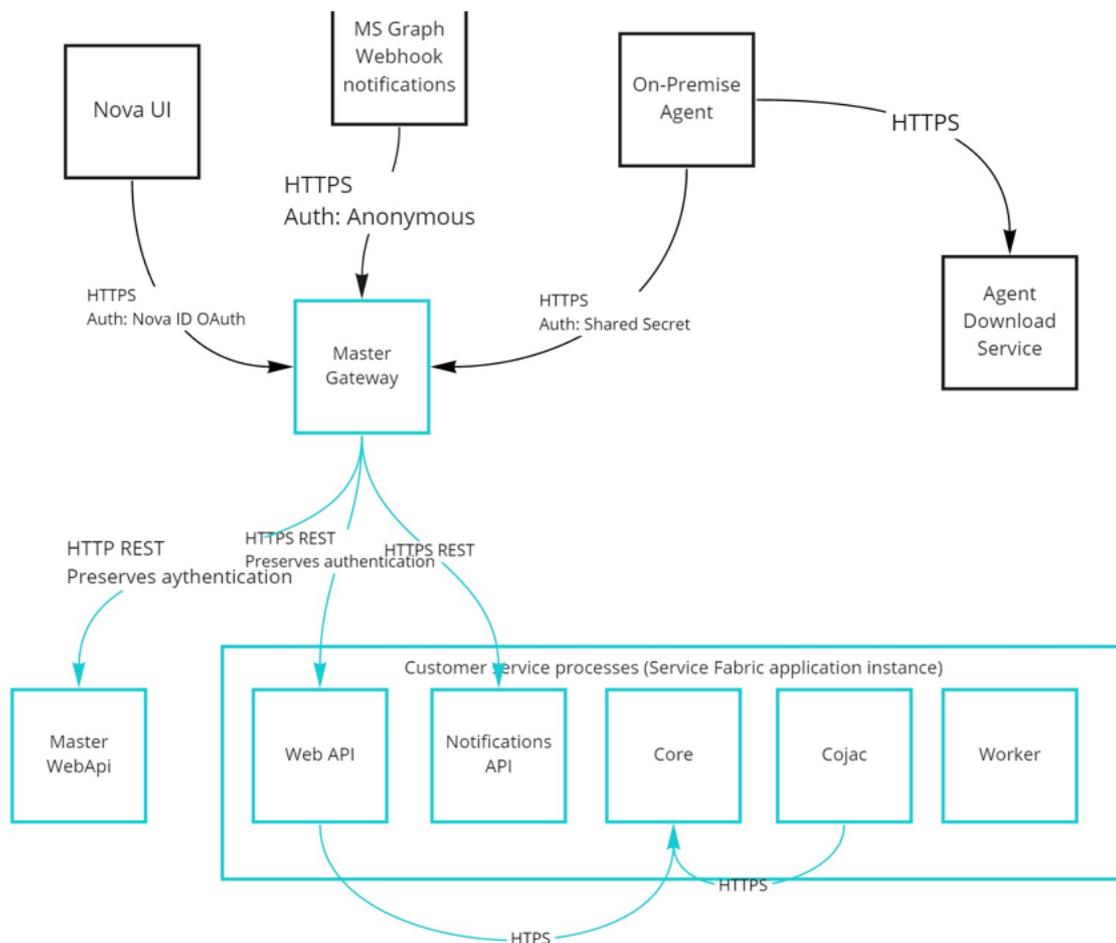
Figure 2: Component Communication Architecture - External
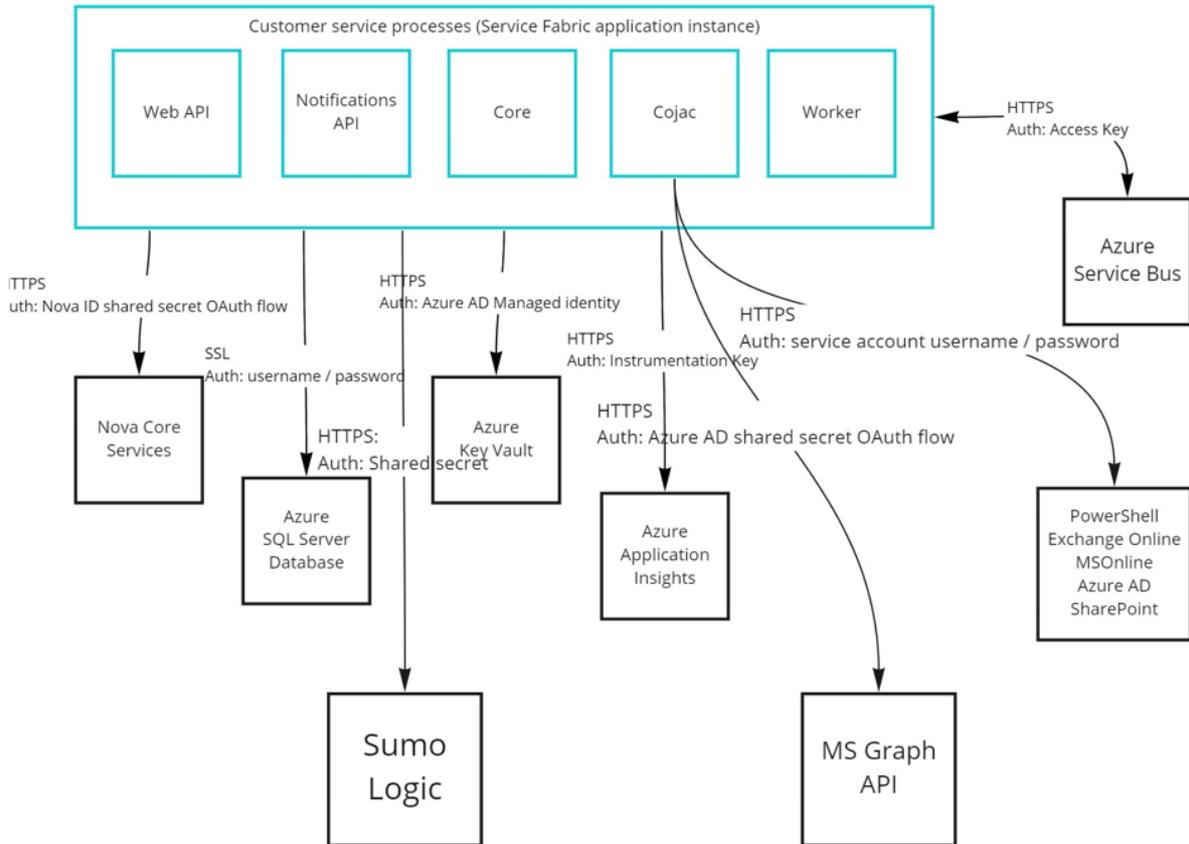
Figure 3: Component Communication Architecture - Internal

The network communication is secured with HTTPS and is not visible to the external public internet.

Inter-service communication uses OAuth authentication using a Quest Azure AD service account with the rights to access the services. No backend services of Quest Nova Delegation and Policy Control can be used by end-users.

Quest Nova Delegation and Policy Control Services accepts the following network communication from outside Azure:

- Access to Quest Nova Delegation and Policy Control web UI.

- Connection from On-Premise Agent

All external communication is secured with HTTPS TLS 1.2.

The Quest Nova Delegation and Policy Control user interface uses OAuth authentication with JWT token issued to a logged in user.

11

Authentication of users

The customer logs in to the application either via Azure Active Directory Single Sign On, or by providing Quest Nova user account credentials.

Role based access control

Quest Nova Delegation & Policy Control does provide the common authentication via Quest Id. Quest Nova is configured with default roles that can be edited or deleted, and also allows you to add custom roles to make permissions more granular. Each access role has a specific set of permissions that determines what tasks a user assigned to the role can perform.

- **Account Administrator** - This gives access to be able to create and manage policies in Delegation and Policy Control.
- **Auth Policy Admin** - This gives users the ability just to manage policies within Quest Nova.
- **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.
- **Config Policy Admin**
- **IT Administrator** - This gives a user the ability to use Quest Nova, but restricts them from changing the configuration or security of Quest Nova itself.
- **License Admin** - This gives people the ability to create and maintain License Policies.
- **Organization Unit Admin** - This gives users the ability to maintain virtual organizational units.
- TMS admin
- **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.
- **System Administrator** - This roles gives access to the Tenant Management System, and does not give any direct access to the Quest Nova application (unless it is combined with other roles).
- **TMS License Admin**

FIPS 140-2 compliance

Quest Nova Delegation & Policy Control cryptographic usage is not based on Azure FIPS 140-2 compliant cryptographic functions. For more information, see: https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations

SDLC and SDL

The Quest Nova Delegation & Policy Control team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on Quest's corporate network have access to these systems. Therefore, should an Quest Nova Delegation & Policy Control developer leave the company, this individual will no longer be able to access Quest Nova Delegation & Policy Control systems

- All code is versioned in source control.

- All product code is reviewed by another developer before check in

In addition, the Quest Nova Delegation & Policy Control Development team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices

- OWASP guidelines

- Regularly scheduled static code analysis is performed on regular basis

- Regularly scheduled vulnerability scanning is performed on regular basis

- Segregated QA, Staging, and Production environments. Customer data is not used in Development and Pre-Production environments

Quest Nova Delegation & Policy Control developers go through the same set of hiring processes and background checks as other Quest employees.

15

Operational security

Source control and build systems can only be accessed by Quest employees on Quest's corporate network (domain security.) If a developer (or any other employee with access to Quest Nova Delegation & Policy Control) leaves the company, the individual immediately loses access to the systems.

All code is versioned in source control.

Access to data

Access to Quest Nova Delegation & Policy Control data is restricted to:

- Quest Operations team members

- Particular Quest Support team members working closely with Quest Nova Delegation & Policy Control product issues.

- The Quest Nova Delegation & Policy Control development team to provide support for the product

Access to Quest Nova Delegation & Policy Control data is restricted through the dedicated Quest Azure AD security groups. For different types of data (e.g., product logs, customer data, and sensitive data) different access levels and lists of allowed people are assigned.

Operational monitoring

Quest Nova Delegation & Policy Control internal logging is available to Quest Operations and Quest Nova Delegation & Policy Control development teams during the normal operation of the platform. Some customers or Personally Identifiable Information (PII) data (e.g. error messages reporting user names or email addresses, etc.) can become a part of internal logging for troubleshooting purposes.

Production Incident Response Management

Quest Operations and Quest Support have procedures in place to monitor the health of the system and ensure any degradation of the service is promptly identified and resolved. Quest Nova Delegation & Policy Control relies on Azure infrastructure and as such, is subject to the possible disruption of these services.
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/

Customer measures

Quest Nova Delegation & Policy Control security features are only one part of a secure environment. Customers must implement their own security practices when proceeding with data handling. Special care needs to be given to protecting the credentials of the Azure Active Directory tenant global administrator accounts and Office 365 tenants global administrator accounts.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

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 discussions

- Chat with support engineers online

- View services to assist you with your product