Quest® Nova Core

Security Guide

© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656
Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents
Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

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

Legend

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

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

Quest® Quest® Nova Security Guide
Updated January 2024

Contents

Introduction **4**

About Quest Nova Core **5**

Architecture overview **6**

Azure datecenter security **7**

Overview of data handled by Quadrotech Nova Core **8**

Admin Consent and Service Principals **9**

Location of customer data **10**

Privacy and protection of customer data **11**

Separation of customer data **12**

Network communications **13**

Authentication of users **15**

Role based access control **16**

FIPS 140-2 compliance **17**

SDLC and SDL **18**

Operational security **19**

- Access to data 19
- Permissions required to configure and operate Nova Core 19
- Operational monitoring 19
- Production Incident Response Management 19

Customer measures **20**

Technical support resources **21**

1

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 Core. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

2

About Quest Nova Core

Quest Nova Core provides the following functionality and basic building blocks for other Quest Nova applications to be built upon:

- Provides identity for users and clients by using OpenID Connect standard
- Provides organization hierarchy for partners and end organization enforcing security access validation
- Allows users assignments to roles and organizations for access
- Exposes notification mechanism for all services (Alerting)
- Implements service lookup for internal service-to-service communication and description of service endpoints for UI (to call region specific service based on provisioning for customers data storage)
- Provides dashboard and widget(s) configuration storage to UI
- Ability execute and deliver (via email) reports on user configurable schedule

Quest Nova Core is hosted in Microsoft Azure and delivers most of its functions via Microsoft Azure cloud services.

3

Architecture overview

The following scheme shows the key components of the Quest Nova Core configuration.

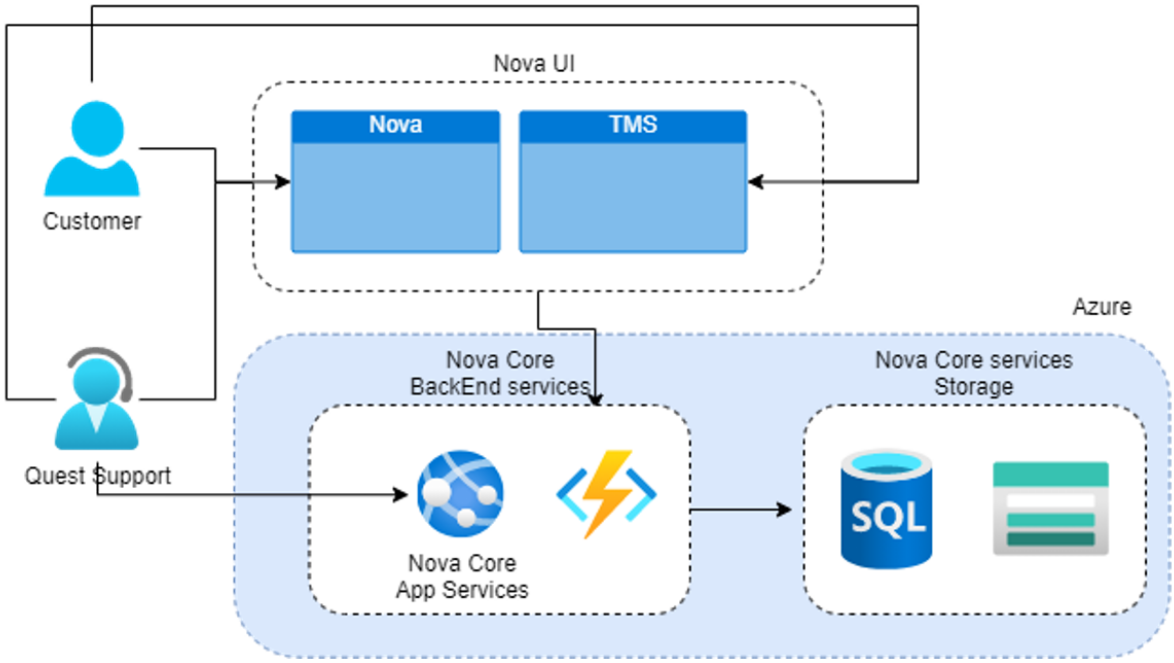


Figure 1 High-Level Architecture

4

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

5

Overview of data handled by Quadrotech Nova Core

Quest Nova Core manages the following type of customer data:

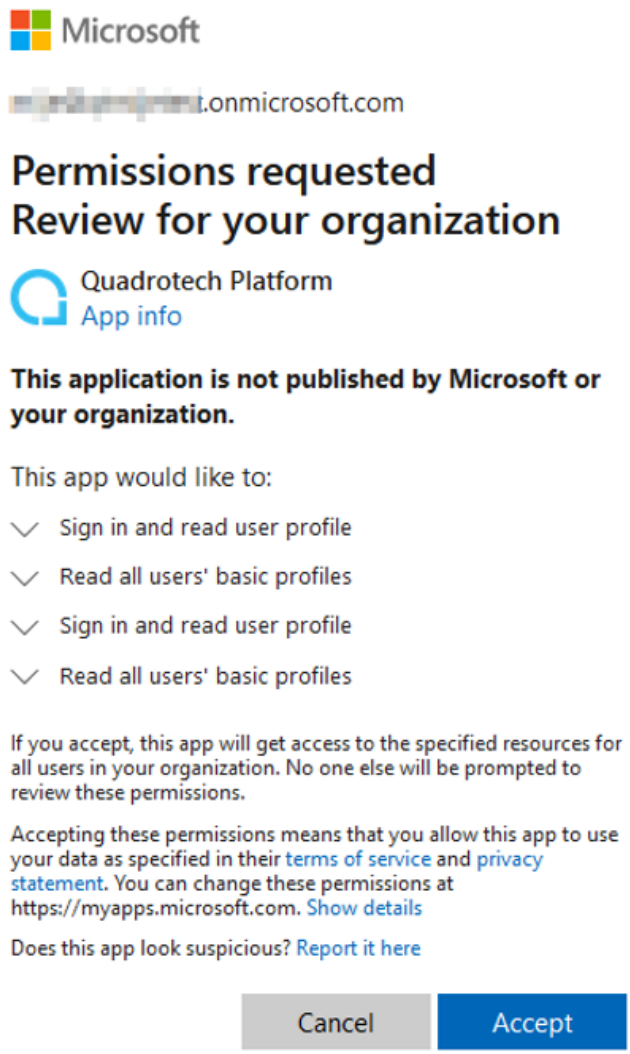
- Azure Active Directory tenant information and other properties. Part of the information is stored in the product database.
- User metadata (Name, Email) as configured from Azure AD or Quest Identity Broker (common identity broker for Quest SaaS solutions) - QIB, incl. the access/id tokens (encrypted at rest)
- Scheduled reports attachment data stored in Azure Blob storage encrypted at rest
- Internal identifier of user (Guid) and access to APIs will be tracked via Application Insight and is encrypted at rest.
- The application does not store or deal with end-user passwords of Azure AD objects.
- The application stores multiple client secret of the application accessing Azure AD via MS Graph (some are read-only, some are customer provided ones for white-label deployments). The data are stored in Azure Key Vault and is encrypted at rest.
- The application stores administrative account name and password to perform certain data collection jobs using PowerShell cmdlets. The data are encrypted by the data collection applications public key and stored in Azure Key Vault and is encrypted at rest and in transit.

6

Admin Consent and Service Principals

Quest Nova Core itself does not require access to the customer's Azure Active Directory and Office 365 tenancies. It does however provide capabilities for applications built upon Quest Nova Core to ask and store additional consents and/or service credentials. Quest Nova Core itself will not utilize service principals as entities defined in Azure Active Directory by default. Quest Identity (QID) is able to utilize Azure Active Directory as login provider and then will ask for consent for "Quest Platform" Azure application, resulting in adding of this application into customer's Azure Active Directory.

Following is the base consent required by Quest Nova Core (for the Identity application).



In addition to the base consents required by Quest Nova Core additional applications might request additional consents.

7

Location of customer data

When a customer signs up for Quest Nova, we store metadata about customers organization (incl. tenant metadata) into a centralized storage, which currently resides in EU West/North Azure data centers. Also, any users' metadata (email, name) invited to the platform will be stored into the same locations.

8

Privacy and protection of customer data

The most sensitive customer data processed by Quest Nova Core is the Azure Active Directory tenant metadata. Reporting service also stores into blob storage any attachments, which are being sent to customers. This might be data which is provided by another Quest Nova application and using Quest Nova Cores' reporting and alerting shared services.

- Notifications and emails sent through Alerting shared service stores the attachments to Azure Blobs. Data is stored encrypted at rest by Azure. Data in transit is protected by TLS.
- Third party service (SendGrid) is used to send emails with reports. Data transfer to SendGrid is protected by TLS and our API key.
- Other data are stored in SQL. Transparent data encryption is utilized to encrypts databases, backups, and logs at rest.

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

9

Separation of customer data

A common concern related to cloud based services is the prevention of commingling of data that belongs to different customers. Quest Nova Core has architected its solution to specifically prevent such data commingling by logically separating customer data stores.

Customer data are differentiated using a Customer Organization Identifier. The Customer Organization Identifier is a unique identifier obtained from the Quest Nova Core that is created when the customer signs up with the application.

Quest Nova Core does not create additional resources when new customer is added to system. Each organization/tenant entity which is persisted has an attribute of `OrganizationId` linking it to the unique identifier obtained from Quest Nova Core. Data requests are then restricted to particular single or multiple organization (organization group). Multiple organizations access is only allowed for multi-tenant customers, as each organization can only have single tenant associated to it. An AzureAD tenant can only be added to one organization.

10

Network communications

Internal network communication within Azure includes:

- Inter-service communication between Quest Nova Core components
- Communication to customer Azure AD/Office 365 tenants (mostly by Quest Nova apps)

The following scheme shows the communication configuration between key components of Quest Nova Core.

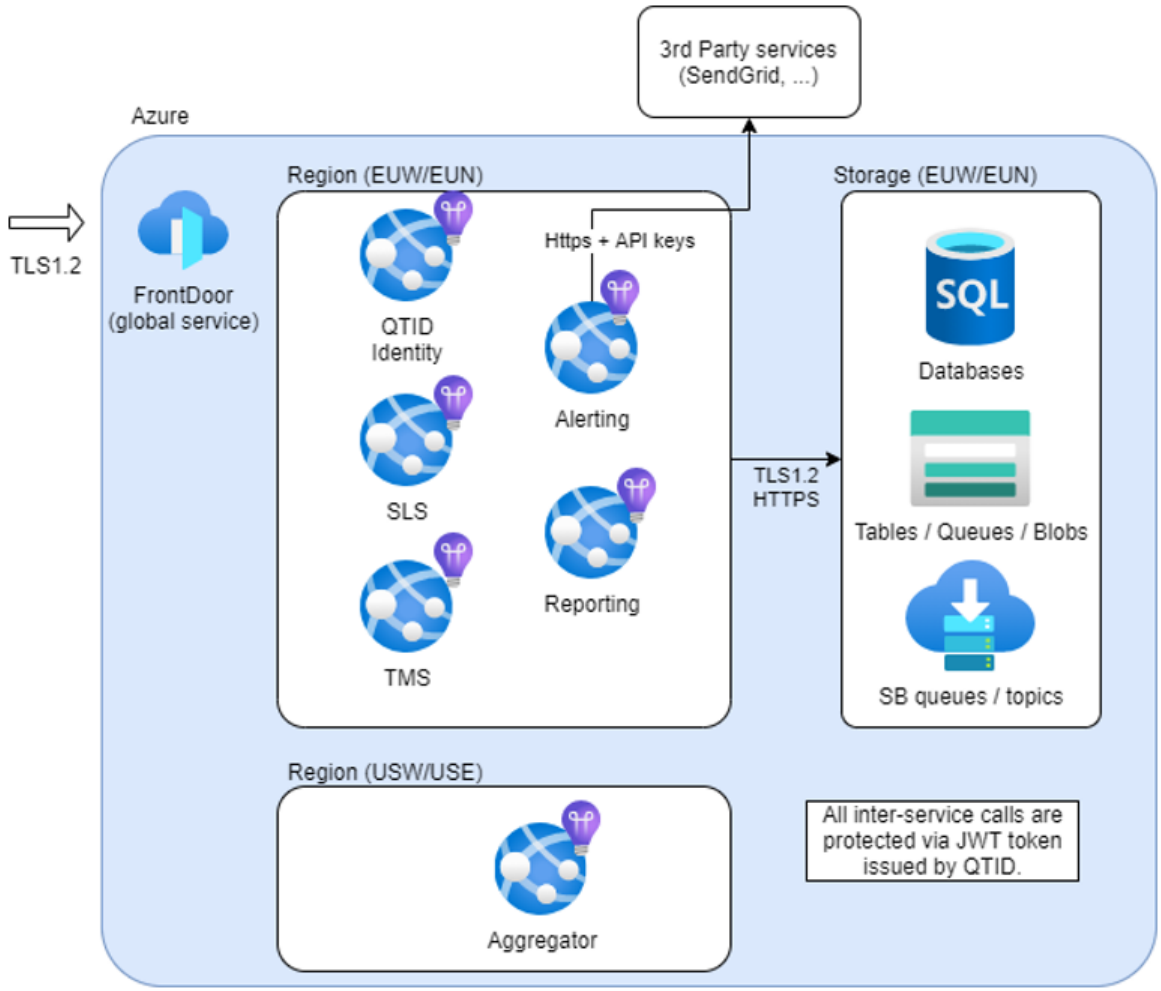


Figure 2 Component Communication Architecture

The network communication is secured with HTTPS and is visible to the external public internet, as all services are communicating directly with each other.

Inter-service communication uses OAuth authentication using a QTID client service account with the rights to access the services. Backend services of Quest Nova Core is accessed by UI with the signed-in user token. The access is then differentiated by user or client tokens.

Quest Nova Core accepts the following network communication from outside Azure:

- Access from web UI.
- Access from other Quest Nova Core based application (Reporting, DPC, TXP, …)

All external communication is secured with HTTPS TLS1.2.

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

There are no unsecured HTTP calls within Quest Nova Core.

11

Authentication of users

The customer logs in to the application by providing QTID user account credentials.

The process of registering an Azure AD tenant into Quest Nova Core is handled through the well-established Azure Admin Consent workflow. For more information about the Azure Active Directory Admin Consent workflow, please refer the Quest On Demand Core technical documents.

12

Role based access control

Quest Nova Core does provide the common authentication via Quest Identity (QTID) service. Quest Nova Core is configured with default roles that cannot be edited or deleted. Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform.

13

FIPS 140-2 compliance

Quest Nova Core cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions, except for certain legacy code specified in following paragraph. For more information, see: https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations

Certain legacy part of user authentication code leverages BCrypt to store hash of users credentials. This flow is only accessible to users coming from old Radar application. Quest customers are forced to utilize QIB (Azure AD), hence this part of code is not in effect.

14

SDLC and SDL

The On Demand 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 On Demand developer leave the company, this individual will no longer be able to access On Demand systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

In addition, the On Demand 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 Development, QA, and Production environments. Customer data is not used in Development and QA environments.

On Demand developers go through the same set of hiring processes and background checks as other Quest employees.

15

Operational security

Access to data

Access to Quest Nova Core data is restricted to:

- Quest Quest Nova Core PM team members
- Particular Quest Support team members working closely with Quest Nova Core product issues.
- The Quest Nova Core development team to provide support for the product

Access to Quest Nova Core 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.

Permissions required to configure and operate Nova Core

Quest Operations team members have access to the Quest's production Azure Subscription and monitor this as part of normal day to day operations. Lead Quest Nova Core developers will be granted limited access to Quest's production Azure Subscription for troubleshooting purposes as necessary.

To access Quest Nova UI, a customer representative needs to be invited by Quest personal, or needs to sign up for a trial. The account is verified via email; thus a valid email address must be provided during registration.

An organization is automatically created once the new account is created.

Operational monitoring

Quest Nova Core internal logging is available to Quest Operations and Quest Nova Core development teams during the normal operation of the platform. Some customer or Personally Identifiable Information (PII) data (e.g. mail item subject, OneDrive file names, 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 Core relies an 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/

16

Customer measures

Quest Nova Core 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.

17

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