Quest® Nova Reporting

Security Guide

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.

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

Quest® Quest® Nova Security Guide
Updated January 2024

Contents

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

2

About Quest Nova Reporting

Quest Nova Reporting provides more than 100 customizable Office 365 reports and dashboards, which can help you to make fast decisions and manage your licenses, user adoption, mail flow, security settings, permissions, storage optimization and much more.

- Drill-down based on AD attributes
- Correlate data from Teams, SharePoint Online, Exchange Online, Yammer and the native audit log
- Visualize data with charts, heat maps and more
- Export, schedule and share insights across your entire organization in a secure and controlled manner
- Share free/busy information between tenants.

Quest Nova Reporting is hosted in Amazon Web Services and delivers most of its functions via Amazon Web Services cloud services.

Architecture overview

The following diagram shows the key components of the Quest Nova Reporting configuration.

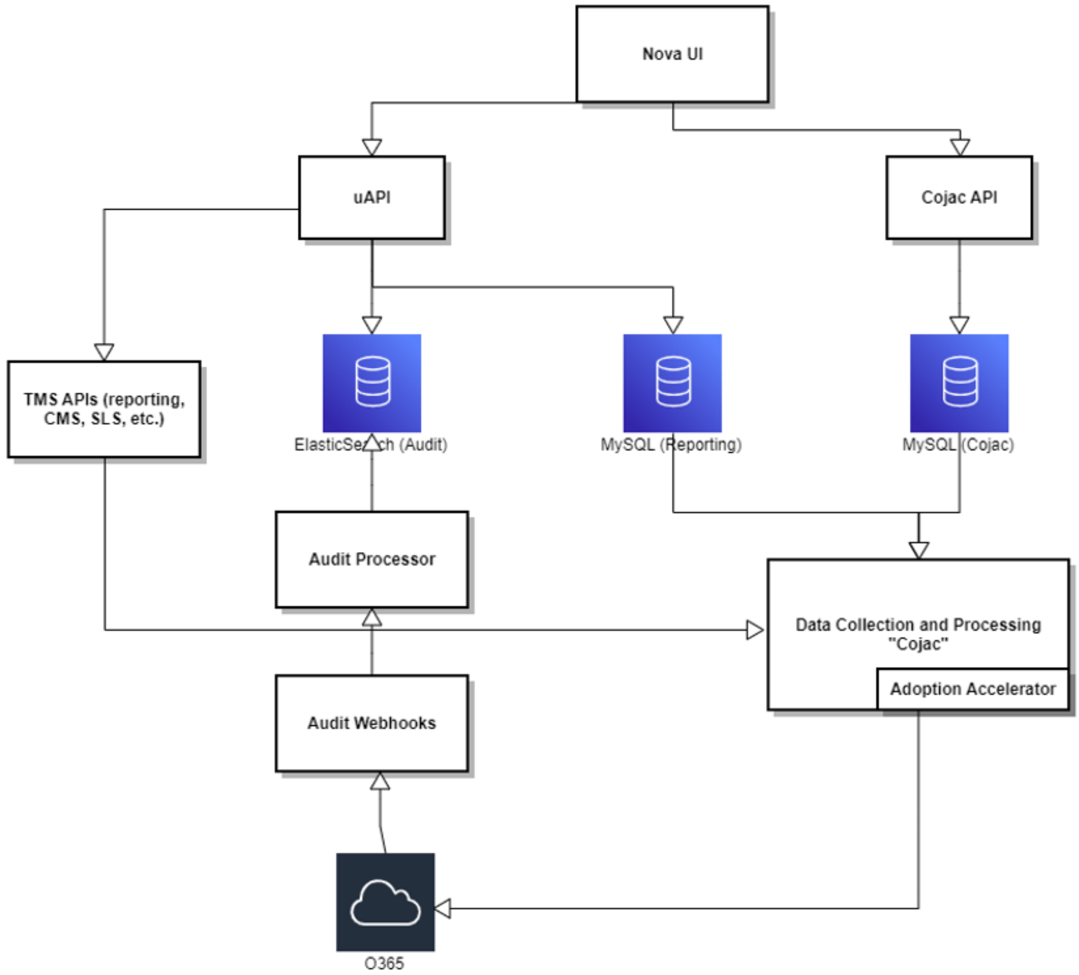


Figure 1: High-Level Architecture

AWS and Azure datacenter 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

Amazon Web Services (AWS) 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 SOC 1, SOC 2 and ISO/IEC 27001:2005.

Relevant references with additional information about the AWS datacenter security are listed below.

- AWS Security Center: https://aws.amazon.com/security/
- AWS Compliance: https://aws.amazon.com/compliance/
- Global Infrastructure: https://aws.amazon.com/about-aws/global-infrastructure/

5

Overview of data handled by Nova Reporting

Quest Nova Reporting manages the following types of customer data:

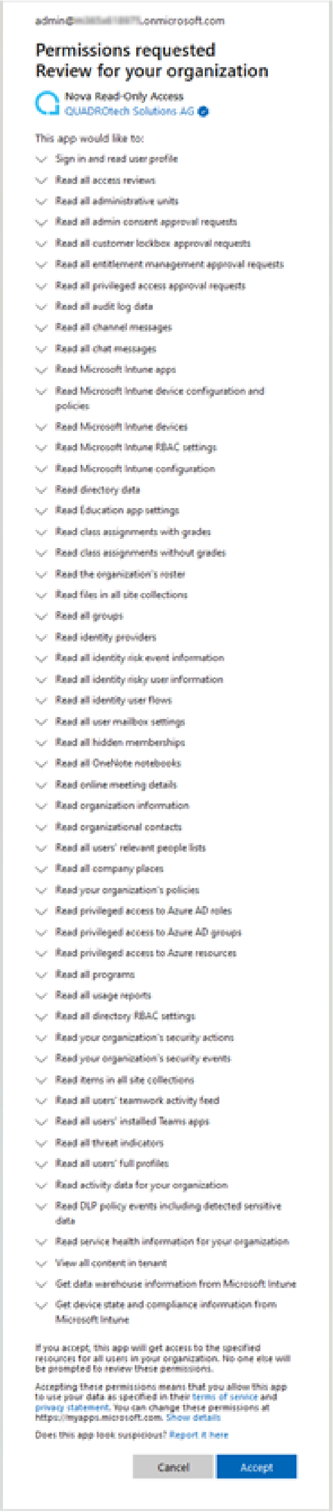
- Azure Active Directory and Office 365 users, groups and contacts with their properties returned by the Microsoft Graph API including account name, email addresses, contact information, department, membership, licenses, and other properties.
- Microsoft product usage statistics and activity, such as Exchange emails, Yammer posts, Skype messages, Teams calls, OneDrive storage, SharePoint files, etc.
- The application does not store or deal with any product contents, such as Exchange/Teams messages or OneDrive file contents - only statistics relating to counts and sizes are stored.
- Audit events returned by the Management Activity API
- Service Status Messages returned by the Management Activity API
- Exchange objects are collected via the Microsoft Exchange Online PowerShell API
- The application does not store or deal with end-user passwords of Azure AD objects.
- The application stores administrative account name and password to perform data collections. The data are stored in Azure Key Vault and is encrypted at rest.

6

Admin Consent and Service Principals

Quest Nova Reporting 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 minimum consents required by Quest Nova Reporting. The Service Principal is created using Microsoft's OAuth certificate 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 Reporting.



admin@[redacted].onmicrosoft.com

Permissions requested
Review for your organization

Nova Read-Only Access
QUADROtech Solutions AG

This app would like to:

- 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 user mailbox settings
- Read all hidden memberships
- Read all OneNote notebooks
- Read online meeting details
- Read organization information
- Read organizational contacts
- Read all users' relevant people lists
- Read all company places
- Read your organization's policies
- Read privileged access to Azure AD roles
- Read privileged access to Azure AD groups
- Read privileged access to Azure resources
- Read all programs
- Read all usage reports
- Read all directory RBAC settings
- Read your organization's security actions
- Read your organization's security events
- Read items in all site collections
- Read all users' teamwork activity feed
- Read all users' installed Teams apps
- Read all threat indicators
- Read all users' full profiles
- Read activity data for your organization
- Read DLP policy events including detected sensitive data
- Read service health information for your organization
- View all content in tenant
- Get data warehouse information from Microsoft Intune
- Get device state and compliance information from Microsoft Intune

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. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

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:

- US (hosted in the AWS us-east-1 region in North Virginia)
- EMEA (hosted in the AWS eu-west-1 region in Ireland)

The databases are hosted in AWS RDS with read-replicas in alternative Availability Zones for resiliency against hardware failure and to increase availability. All replication datacenters reside within the geographic boundaries of the selected region. Daily snapshots are stored for 30 days.

Management Activity API Audit events are stored in Elasticsearch clusters hosted on Microsoft Azure Virtual Machines, in the following regions:

- US (hosted in the Azure westus2 region in Washington, snapshot hosted in AWS us-west-1region)
- EU (hosted in the Azure northeurope region in Ireland, snapshot hosted in AWS eu-west-2)

8

Privacy and protection of customer data

The most sensitive customer data processed by Quest Nova Reporting is the Azure Active Directory and Office 365 data including users, groups and contacts and their associated properties. Quest Nova Reporting does not store or deal with end-user passwords of Azure AD objects, nor user-generated data such as Email/Teams message content or OneDrive files. All data and logs are encrypted at rest.

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 Reporting 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 that is created when the customer signs up with the application.

This identifier is used throughout the solution to ensure strict data separation of customers' data in both the MySQL and Elasticsearch storage solutions and during processing.

10

Network communications

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

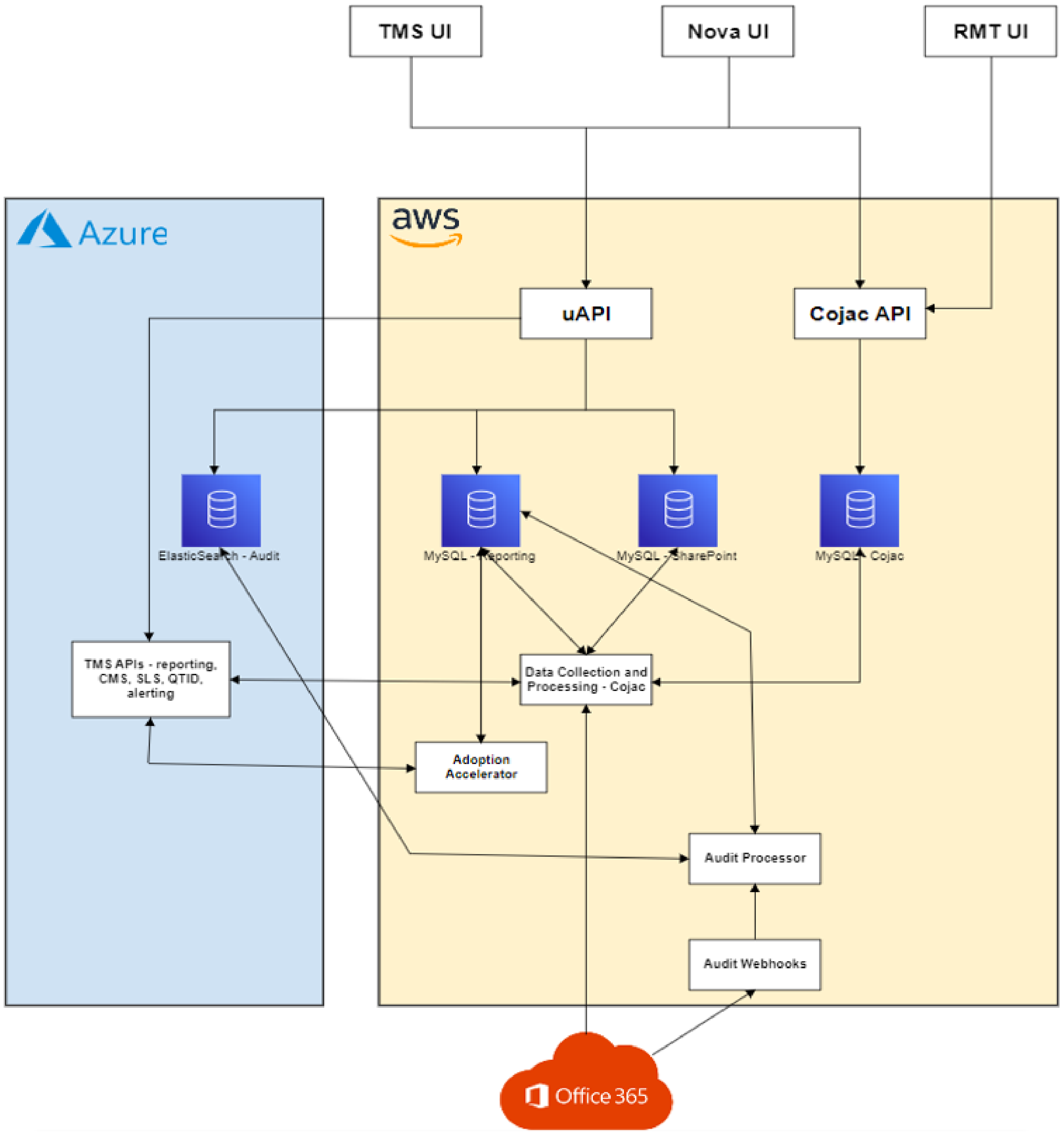


Figure 2: Nova Network Communication Architecture

Internal network communication for Quest Nova reporting includes:

- Inter-service communication between Quest Nova Reporting components

- Communication to customer Azure AD/Office 365 tenants
- Communication between backend and frontend

All network communication is secured with HTTPS TLS1.2.

Inter-service communication uses OAuth authentication using a Quest Azure AD service account with the rights to access the services. Backend services of Quest Nova Reporting can be accessed by UI with the signed-in user.

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 Reporting.

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.

12

Role based access control

Quest Nova Reporting 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**

13

FIPS 140-2 compliance

Quest Nova Reporting cryptographic usage is based on Azure FIPS 140-2 compliant cryptographic functions. For more information, see: https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations.

14

SDLC and SDL

The Quest Nova 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 Quest Nova systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

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

- MS-SDL best practices
- Threat modelling.
- OWASP guidelines.
- Regularly scheduled static code analysis is performed on regular basis.
- Regularly scheduled vulnerability scanning is performed on regular basis.
- Segregated Development, Pre-Production, and Production environments. Customer data is not used in Development and Pre-Production environments.

Quest Nova 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 Reporting) 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 Reporting data is restricted to:

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

Access to Quest Nova Reporting 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 Reporting internal logging is available to Quest Operations and Quest Nova Reporting development teams during the normal operation of the platform. Some customer 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 Reporting 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/
- AWS status page is available at https://status.aws.amazon.com/

16

Customer measures

Quest Nova Reporting 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