

Quest® On Demand Migration For Email

Security Guide



Copyright 2022 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, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. in the U.S.A. and other countries. For a complete list of Quest Software trademarks, please visit our website at <https://www.quest.com/legal>. All other trademarks, servicemarks, registered trademarks, and registered servicemarks 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.

Contents

Introduction	1
About On Demand Migration for Email	2
Permissions Required to Configure and Operate ODME	4
Overview of Data Handled by ODME	5
Location of Customer Data	6
Separation of Customer Data	7
Privacy and Protection of Customer Data	8
Who at Quest Software has Access to ODME	9
Azure Region Security	10
Auditing	11
Single Layer of Access Control	12
Network Communications	13
Authentication of Users	14
Validation of Input from Users	15
Third Party Assessments and Certifications	16
Penetration testing	16
Certification	16
Operational Security	17
Customer Measures	18
Conclusion	19
Appendix. On Demand Migration for Email and FISMA Compliance	20
Notes	25
About us	26
Technical support resources	26

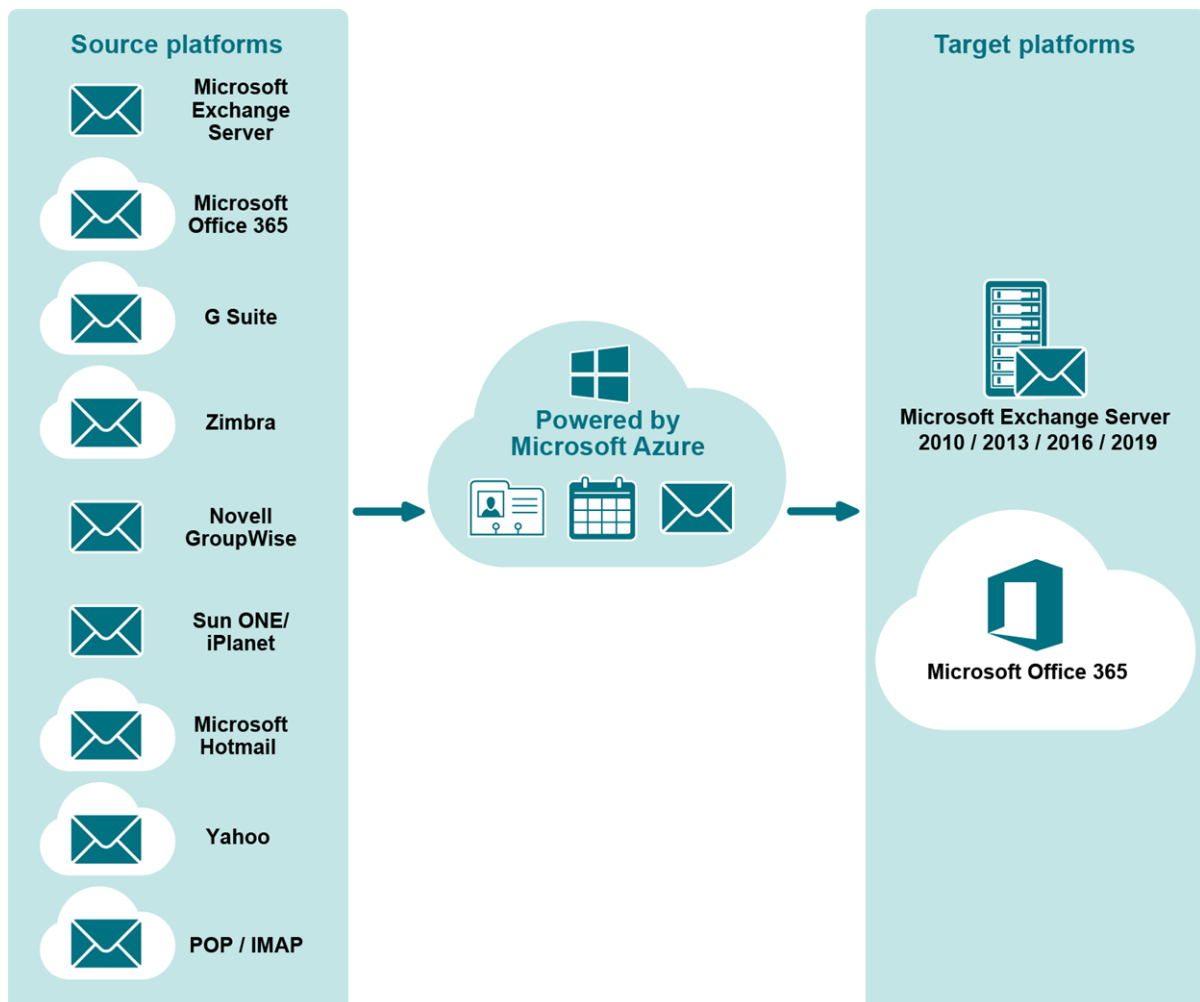
Introduction

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 Software strives to meet standards designed to provide its customers with their desired level of security, whether it relates to privacy, authenticity and integrity of data, availability, or protection against malicious users and attacks.

This document describes the security features of Quest On Demand Migration for Email. It reviews access control, protection of customer data, secure network communication, and more. There is also an appendix that describes how On Demand Migration for Email's security features meet the NIST's recommended federal information security standards as detailed in the Federal Information Security Management Act (FISMA).

About On Demand Migration for Email

Quest On Demand Migration for Email (ODME) securely migrates data to Office 365 and on-premises Exchange or hosted Exchange email platforms without requiring organizations to install or maintain migration servers for the move. From a single console, administrators can migrate multiple users simultaneously and migrate data such as email, calendars and folders in a phased approach. Administrators can filter to clean up unwanted data and shorten the time it takes to migrate.



With Quest On Demand Migration for Email, you can quickly and securely migrate data from on-premises Exchange 2007 and above, Google G Suite or other platforms to Office 365 or Exchange 2010/2013/2016/2019.

Fast, reliable migration with Zero Footprint

Quest On Demand Migration for Email offers:

- Concurrent migration – it supports multiple, simultaneous migrations, ensuring your project completes on time.
- Flexibility – Email, calendars, contacts and tasks can be migrated in a phased approach.
- Data filtering – Clean up unwanted data and complete the migration faster by filtering email data by age, or excluding source email folders by name.
- Mailbox authentication - Administrators with authorized administrator or service account credentials can migrate user mailboxes without knowing or resetting user passwords. This reduces administrative effort while ensuring the security of your environment. For Office 365, you can also use Modern Authentication to connect to your tenant. The Use Modern Authentication option lets you grant consent to ODME instead of providing Administrative credentials with Application Impersonation rights.

Permissions Required to Configure and Operate ODME

The main interface through which the customer interacts with and configures ODME is its web application. ODME does not require the installation of any software components on the customer's systems. In order to create an ODME user account, a customer representative goes to Quest Software's ODME website and enters the necessary user account information, including information about the customer's company and an email address (user name) and password.

In order to configure an email migration job, the user needs admin privileges on both the source and target email repositories. Specifically, the user requires privileges which allow access (read only) to all email accounts on the source system that will be migrated.

Overview of Data Handled by ODME

ODME manages the following type of customer data:

- Source and target server locations and credentials
- Source and target mailbox names
- Mailbox data including email, calendar, contacts, personal distribution lists and tasks
- Email meta-data such as subject line, date, size (but not the email body)

The following customer data will, by default, be persisted by ODME:

- Source and target server locations & credentials
- Source and target mailbox names
- Product logs data which can include structured error message entries, containing email meta-data such as subject line, date, size, the folder name (if any) in which the email resides, but not the email body, for items, that ODME failed to transport.
- MIME content of mailbox item: to facilitate troubleshooting, the MIME content of mailbox item may be stored when an error occurs during migration. This is turned off by default, and is only enabled when the customer grants permission.

The persisted data is stored until a customer's subscription expires. The data is stored in Azure Storage, including Table, Queue and BLOB (binary large object) storage, and is persisted as long as a customer's subscription is active. Once a customer decides to unsubscribe from ODME, their data will be deleted 30 days after their subscription expires. The customer is notified of this upon their subscription termination.

ODME does not persist the actual emails that get migrated. They only exist in memory while they are in process of getting migrated. The only exception occurs when the customer specifically gives the ODME product team permission to turn on full logging mode in order to capture sufficient data to help in identifying and solving an error.

Location of Customer Data

When customers subscribe to ODME they are able to select between having their data stored in the Central United States, Canada, Australia, Northern Europe and Asia Pacific Microsoft Azure regions.

Beside the above regions, there is a specific instance of ODME designed for United States Public Sector customers only and addresses their requirements of:

- Content is stored within the United States.
- Content is restricted to Quest personnel that are US Citizens and these personnel undergo background investigations in accordance with relevant government standards.

ODME uses only LRS storage accounts. No data is replicated to another region.

Separation of Customer Data

A common concern related to cloud based services is the prevention of commingling of data belonging to different customers. ODME has architected its solution to specifically prevent such data commingling by logically separating its customers' data stores.

Customer data is differentiated using an internal Customer Identifier value (specific to individual customers) as well as a Customer Partition key. In virtually all cases, the Customer Partition Key is used to identify data for individual customers.

For shared storage tables, a column in the table is used to identify the customer. All queries and updates to the storage tables must include the Customer Partition key. Shared tables include a central log table (write only), job management table (includes migration status & counts), and a settings table that has customer specific settings, such as the 'capture MIME' flag.

Most storage objects are logically partitioned using the Customer Partition Key. This means that the name of the storage table, queue or blob container has the customer's partition key prefixed to it. This makes it safer to access these storage objects, because queries or updates don't need to always include the partition key column.

Privacy and Protection of Customer Data

The most sensitive customer data collected and stored by ODME are the admin account credentials on the source and target email environments. These credentials are required by ODME in order to execute email migration operations. ODME protects these credentials by encrypting them with the AES (Advanced Encryption Standard) algorithm. AES is operated in CBC (chain block cipher) mode with a 256-bit encryption key. AES is on the list of FIPS 140-2 compliant cryptographic algorithms, and ODME specifically uses the FIPS 140-2 certified `AesCryptoServiceProvider()` class in Microsoft's CryptoAPI.

Who at Quest Software has Access to ODME

The production access permissions granting/revoking/editing workflow is ISO 27001 compliant.

Select members of the product development team have read-only access to the data held in the Azure Storage account. The deployment manager has read and write access to the storage accounts as required for managing deployments, configuration of customer specific settings, as well as troubleshooting.

All members of the development team and support have access to an internal ODME "Support Dashboard" tool, which provides access to migration jobs configuration, logs and statistics (excluding credentials).

Azure Region Security

Microsoft Windows Azure regions 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 SAS 70 Type I and Type II and ISO/IEC 27001:2005. Relevant references with additional information about the Windows Azure region security can be found here:

- Windows Azure Trust Center: <https://www.microsoft.com/en-us/trustcenter/cloudservices/azure>
- Whitepaper: Standard Response to Request for Information – Security and Privacy: <http://www.microsoft.com/en-us/download/details.aspx?id=26647>

Auditing

A central audit log is kept which contains event information about migration jobs. No email body contents or user account credentials are stored within the log. Certain email meta-data is kept, such as subject lines and statistics around migration jobs.

The admin user has the ability to view log data pertaining to their migrations. Note that this admin user, by virtue of their privileges, already has the ability to view all data about mailboxes in the source environment (independent of ODME).

Single Layer of Access Control

ODME provides a single level of access in order to access the administrator services (e.g. executing an email migration).

Network Communications

All communications to and from the ODME web application goes over TLS, and the SSL certificates need to be issued by certificate authorities that are, by default, trusted in Windows Server 2019. Self-signed certificates are allowed as well when connecting to on-premises servers. Please refer to ODME documentation for more details.

For on-premise Microsoft Exchange migrations, the default port used (during the migration) is port 443 (HTTPS). A customer has the choice of using a non-encrypted connection using HTTP. It is also possible for a customer to use non-standard ports, and specifying these port numbers in the URL (e.g. <https://xyz:454>).

ODME communicates with Exchange servers (on-premise Exchange, Live@edu and Office 365) over port 443 by default. Port 80 may be used if the customer configures their on-premise server that way.

To communicate with G Suite, ODME uses Gmail API. The default port is 443. OAuth 2.0 is used for read-only access to directory service. For fetching email, calendar and contacts ODME uses Service account's certificate credentials.

Also, ODME uses the [limilabs Mail.dll](#) library. This library supports the latest Transport Layer Security (TLS) protocol to authenticate the server and secure client-server communication.

Authentication of Users

When a customer creates an ODME user account, a designated individual from the customer chooses his or her username and password for this account. These credentials are required when this individual wishes to manage email migration jobs.

Validation of Input from Users

ODME performs input validation on data submitted by its users. Specifically, it employs field level validation for URLs, user names and email addresses, amongst others. The import file containing mailbox names is pre-processed to ensure that all mailbox names are valid.

Third Party Assessments and Certifications

Penetration testing

On Demand has undergone a third party security assessment and penetration testing yearly since 2017. The assessment includes but is not limited to:

- Manual penetration testing
- Static code analysis with Third Party tools to identify security flaws

A summary of the results is available upon request.

Certification

On Demand is included in the scope of the Platform Management ISO/IEC 27001, 27017 and 27018 certification:

- ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements :**Certificate Number: 1156977-3** , valid until **2025-07-28**.
- ISO/IEC 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **Certificate Number: 1156977-3**, valid until **2025-07-28**.
- ISO/IEC 27018 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **Certificate Number: 1156977-3**, valid until **2025-07-28**.

Quest Software, Inc. has successfully completed a SOC 2 examination of its On Demand solution. The examination was performed by an independent CPA firm for the scope of service described below:

Examination Scope: **Quest On Demand Platform**

Selected SOC 2 Categories: **Security**

Examination Type: **Type 2**

Review Period: **January 1, 2022, to July 31, 2022**

Service Auditor: **Schellman & Company, LLC**

Operational Security

All the product code is versioned in source control. All product code changes are reviewed by authorized 'Code Owner' before check in. Access to source control and build systems is protected by domain security, meaning that only employees that are on Quest's corporate network have access to these systems. Therefore, should an ODME developer depart from the company, this individual will lose access to the corporate network and therefore no longer be able to access ODME systems.

ODME developers go through the same set of hiring processes and backgrounds checks as other Quest employees. ODME developers should also pass additional background checks in order to comply with MSFT requirements for US Federal customers.

Customer Measures

On Demand Migration of Email's security features are only one part of a secure environment. The customer's operational and policy decisions will have a great influence on the overall level of security. Customers need to operate by their own best security practices when proceeding with email migration jobs. Special care needs to be given to protecting the credentials of the administrator email accounts within the source and target email environments, including the credentials' privacy as well as only permitting dedicated individuals to gain access.

Conclusion

On Demand Migration of Email is built with security in mind. All communications take place over TLS. Sensitive credentials are encrypted with the FIPS 140-2 compliant AES algorithm with a 256-bit encryption key. Encryption key is different for each customer. It is obtained by KDF based on SHA256 hash. Customer data is logically separated to avoid commingling. All developed code is reviewed by another ODME "Code Owner" before it gets checked in to source control. On Demand Migration of Email will continue to prioritize security as new features are developed and enhancements get made.

Appendix. On Demand Migration for Email and FISMA Compliance

The Federal Information Security Management Act¹ (FISMA) was passed by the U.S. Congress and signed by the president as part of the Electronic Government Act of 2002. It requires “each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information system that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.”

A major component of FISMA implementation is the publication by the National Institute of Standards and Technology (NIST), entitled “Recommended Security Controls for Federal Information Systems”, listed as NIST Special Publication 800- 532. This document presents 17 general security categories that can be used to evaluate an information security control program to measure its level of compliance with FISMA. For this reason, this appendix offers the 17 categories listed in 800-53 and describes how On Demand Migration for Email addresses them.

We would like to emphasize that the secure deployment of On Demand Migration for Email is only one part of an information security program. If the appendix states that a particular security category is “applicable” to On Demand Migration for Email, this means that On Demand Migration for Email contains security features that may be relevant to some or all aspects of the category in question. It may not mean that On Demand Migration for Email fully meets all of the requirements described in that security category, or that the use of On Demand Migration for Email by itself will guarantee compliance with any information security standards or control programs. The specification, selection and implementation of a successful security program ultimately depends on how the customer deploys, operates, and maintains its entire network and physical infrastructure, including On Demand Migration for Email.

NIST 800-53 Categories

Category:	Access Control (AC)
Applicable:	Yes
Description:	On Demand Migration for Email enforces access control by only permitting users with sufficient administrator privileges to execute migrations. based upon a user’s Active Directory privileges in. Permissions to perform specific operations are controlled by access roles.
Further Details:	Section(s) Permissions Required to Configure and Operate ODME, Who at Quest Software has Access to ODME Data, Single Layer of Access Control.

Category:	Awareness and Training (AT)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing all security awareness and training policies.
Further Details:	N/A

Category:	Audit and Accountability (AU)
Applicable:	Yes
Description:	On Demand Migration for Email keeps a central audit log that contains information about migration jobs. No email body contents or user account credentials are stored within the log.
Further Details:	Section(s) Auditing

Category:	Certification, Accreditation and Assessments (CA)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing all assessment, accreditation and certification policies.
Further Details:	N/A

Category:	Configuration Management (CM)
Applicable:	Yes
Description:	By default, ODME is configured to force all communications over the TLS protocol. Customers can configure ODME to use non-standard network ports.
Further Details:	Section(s) Network Communications

Category:	Contingency Planning (CP)
Applicable:	No
Description:	As defined by NIST (publication 800-34), disruptive events to IT systems include power outages, fire and equipment damage, and can be caused by natural disasters or terrorist actions. For this reason, this category does not apply to On Demand Migration for Email; it is the responsibility of the customer to design and implement contingency plans.
Further Details:	N/A

Category:	Identification and Authentication (IA)
Applicable:	Yes
Description:	On Demand Migration for Email requires a customer representative to create an initial ODME user account. To manage migration jobs, the user needs to enter credentials for email user accounts (in the source and target environments) that have sufficient administrative privileges.
Further Details:	Section(s) Permissions Required to Configure and Operate ODME

Category:	Incident Response (IR)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing incident response policies and procedures.
Further Details:	N/A

Category:	Maintenance (MA)
Applicable:	Yes
Description:	Quest Software monitors the software components and libraries used by On Demand Migration for Email for security developments and flaws and produces software updates when necessary.
Further Details:	N/A

Category:	Media Protection (MP)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing media protection policies.
Further Details:	N/A

Category:	Physical and Environmental Protection (PE)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing physical and environmental policies.
Further Details:	N/A

Category:	Planning (PL)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing security planning policies.
Further Details:	N/A

Category:	Personnel Security (PS)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for enforcing personnel security policies, including personnel screening and termination.
Further Details:	N/A

Category:	Risk Assessment (RA)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing risk assessment policies.
Further Details:	N/A

Category:	System and Services Acquisition (SA)
Applicable:	No
Description:	This category does not apply to On Demand Migration for Email; the customer is responsible for developing and reviewing system and services acquisition policies.
Further Details:	N/A

Category:	System and Communications Protection (SC)
Applicable:	Yes
Description:	During setup, On Demand Migration for Email customers are able to specify which geographical Microsoft Azure region to store their data in. ODME prevents commingling of data from different customers by logically separating their data in its storage containers. The AES encryption algorithm (with a 256-bit encryption key) is used to protect the credentials of the admin accounts on the source and target email environments. ODME enforces all that communications with the web application occur over TLS enabled

	connections.
Further Details:	Section(s) Location of Customer Data, Separation of Customers' Data, Privacy and Protection of Customer Data, Network Communications
Category:	System and Information Integrity (SI)
Applicable:	Yes
Description:	On Demand Migration for Email performs input validation on data submitted by its users. Third-party software components and libraries used by On Demand Migration for Email are monitored through US-CERT, and Quest will take appropriate action when applicable vulnerabilities are published.
Further Details:	Section(s) Validation of Input from Users

Notes

Note that under 800-53, these seventeen listed categories define general security control “families” (e.g., “AC”), and that each family in turn contains several subcategories (e.g., “AC-1”, “AC-2”, “AC-3”, etc.) that further detail related aspects of information security and assurance. Consult Appendix F of 800-53 for further information.

About us

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