Binary Tree® Power365®

Security Guide

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 Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are 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.

Power365 - Security Guide
Updated – May 26, 2022

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.

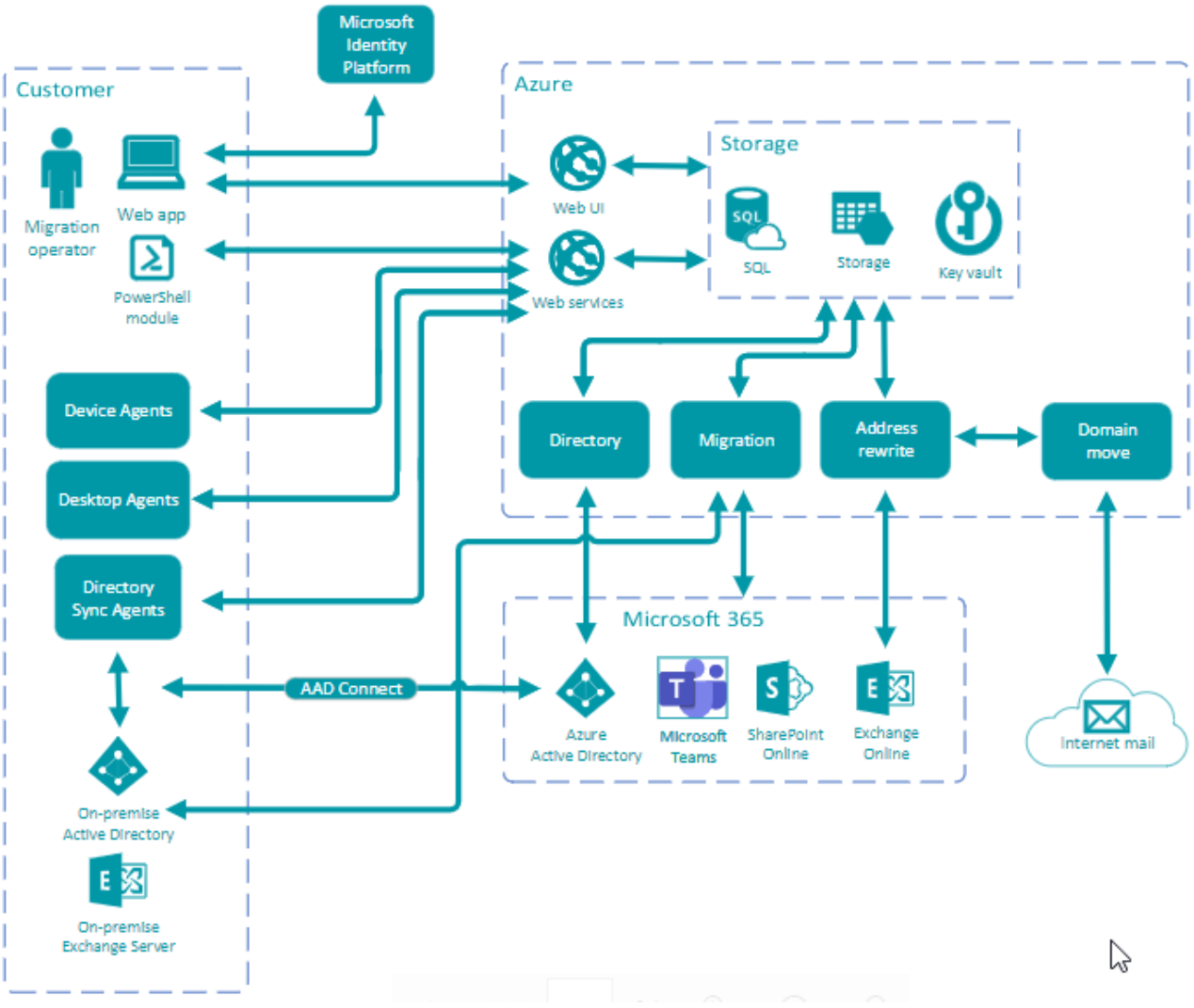
This document describes the security features of Binary Tree Power365. It reviews access control, protection of customer data, secure network communication, cryptographic standards and more.

About Binary Tree Power365

Binary Tree Power365 provides the following functionality:

- Full tenant discovery of users, groups, domains and more.
- Match, create, license and sync mailboxes, OneDrive, Teams and Microsoft 365 groups.
- Cross-tenant collaboration with calendar sharing, unified address lists and free/busy lookups
- Automated mail flow management before and after user migrations
- Move domains between tenants.
- Synchronize Active Directory and Azure Active Directory directories with customizable workflows.
- Migrate workstations, computers, servers, objects, users, groups and more.
- No servers, trusts, or network connectivity required.
- Data transformation and customizable mapping of directory attributes.
- Near-real time password hash synchronization.
- Trustless SID History migration.

Architecture Overview



Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure 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:

- Azure Trust Center: https://azure.microsoft.com/en-us/support/trust-center/
- Microsoft Trust Center Compliance: https://www.microsoft.com/en-us/TrustCenter/Compliance?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-at-rest Encryption Best Practices: https://docs.microsoft.com/en-us/azure/security/azure-security-data-encryption-best-practices

Overview of Data Handled by Binary Tree Power365

Tenant-to-Tenant Migrations

Power365 Tenant-to-Tenant migrations collect data for a variety of Azure Active Directory objects. The directory locations and objects collected are configurable to ensure only the desired objects are processed.

- Directory objects are processed using Microsoft Graph API and PowerShell.
- Objects include users, groups, contacts, teams, and Microsoft 365 groups.
- Properties include account name, email addresses, contact information, department, membership and more.
- Access to Azure Active Directory is granted by the customer using the Microsoft Admin Consent process and requires administrative credentials. Customers can revoke Admin Consent at any time. See https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.
- Power365 does not store credentials for administrative accounts.
- Power365 generates and manages dedicated service accounts in each Microsoft 365 tenant used for PowerShell queries. The service accounts password is randomly generated to be unique and highly complex. The password is also encrypted with AES 256-bit encryption using Azure Key Vault and is never stored unencrypted.
- Power365 service accounts are assigned access to individual mailboxes that are in scope for content migration. This access is removed after migration, if configured from the user interface.
- Messages for mailboxes, public folders and Team channels are temporarily stored during migration and deleted as soon as they are written to the target. The temporarily stored messages are encrypted using AES symmetric-key encryption with a 256-bit key that is unique per message, randomly generated and only held in memory.
- OneDrive and other Teams content is streamed directly from the source to the target environment.
- Power365 can be configured to migrate Outlook, Teams and OneDrive accounts when an end user downloads and runs the Power365 Desktop Agent. No data is collected by the agent. Settings related to Outlook, Teams and OneDrive are modified to redirect end users to their migrated account(s).

Email Rewrite Service

Power365 rewrites email message recipients to provide seamless message delivery during migration of users, groups, and domains.

- Email messages are temporarily stored during processing and deleted as soon as they are written to the target. The temporarily stored messages are encrypted using AES symmetric-key encryption with a 256-bit key that is unique per message, randomly generated and only held in memory.

Directory Synchronization & Migration

Power365 Directory Synchronization collects data for a variety of on premises and Azure active directory objects. The directory locations, objects and properties collected are configurable to ensure only the desired objects and properties are processed.

Azure Active Directory

- Directory objects are processed using Microsoft Graph API and PowerShell.
- Objects include users, groups, contacts, teams, and Microsoft 365 groups.
- Properties include account name, email addresses, contact information, department, membership and more.
- Access to Azure Active Directory is granted by the customer using the Microsoft Admin Consent process and requires administrative credentials. Customers can revoke Admin Consent at any time. See https://msdn.microsoft.com/en-us/skype/trusted-application-api/docs/tenantadminconsent for details.
- Power365 does not store credentials for administrative accounts.
- Power365 generates and manages dedicated service accounts in each Microsoft 365 tenant used for PowerShell queries. The service accounts password is randomly generated to be unique and highly complex. The password is also encrypted with AES 256-bit encryption using Azure Key Vault and is never stored unencrypted.

On Premises Active Directory

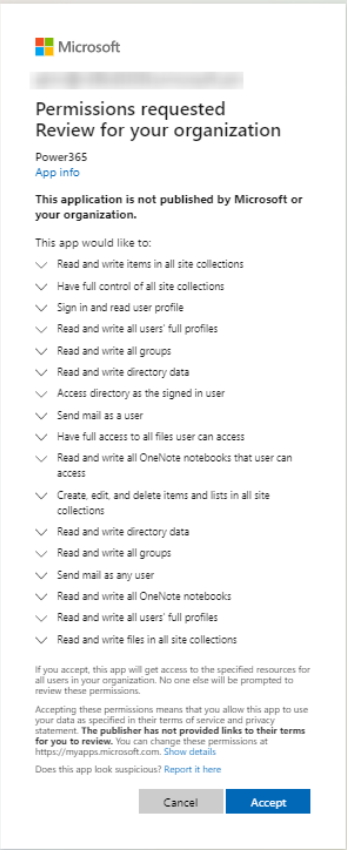
- On-premises directory sync agents, running within the customers network, process Active Directory objects using LDAP or LDAPS (TLS 1.2) as configured within the user interface. Objects include users, groups, contacts, computers, and servers. Object properties include account name, email addresses, contact information, department, membership and more.
- When the optional password sync feature is enabled, the password hash of all user accounts in scope are collected and stored encrypted with AES256 in Azure SQL Storage. The AES256 bit key is stored in Azure Key Vault. Once co-existence is no longer required for a specific user, the customer should use the reconcile option to ensure that information is promptly deleted.
- On-premises directory sync agents, running within the customers network, securely encrypt and store administrative credentials locally on the agent's computer.
- On-premises device agents running locally on the end user's workstation collect device properties using WMI and PowerShell. Device properties include device name, domain name, user profile locations and more.
- Power365 optionally stores credentials required for network share re-permission and Active Directory domain joins. These credentials are provided by migration operators, encrypted with AES 256-bit encryption using Azure Key Vault and are never stored unencrypted.

Admin Consent and Service Principals

Power365 requires access to the customer's Azure Active Directory and Office 365 tenants. 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. The Service Principal is created using Microsoft's OAuth auth code grant flow https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-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.

Below is the Admin Consent screen, see Operational Security > Permissions Required to Configure and Operate for a complete list of permissions required by Power365.



Location of Customer Data

When a customer signs up for Power365, they select the region in which to run their Power365 organization. All computation is performed in and all customer data is stored in the selected region. The currently supported regions are the United States, Australia, and European Union. Other regions may be added over time. Power365 customer data is stored in the selected region, entirely within Azure Services provided by Microsoft. For more information, see Achieving Compliant Data Residency and Security with Azure.

- Customer data is stored in Azure SQL and is automatically replicated for failover using Azure SQL Active Geo replication. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview
- Application data and logs are stored in Azure storage tables. Windows Azure Storage, including the Blobs, Tables and Queues storage structures, by default get replicated three times in the same datacenter for resiliency against hardware failure. The data are replicated across different fault domains to increase availability. All replication datacenters reside with the geographic boundaries of the selected region. See this Microsoft reference for details: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy
- DKIM and TLS certificates used by Power365 Email Rewrite Services are stored in Microsoft Key Vault.

Privacy and Protection of Customer Data

- All data is secured at rest using SQL Transparent Data Encryption (TDE) with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/azure-sql/database/transparent-data-encryption-tde-overview
- Azure storage account data is secured at rest using storage service encryption with Microsoft managed keys. For more information see https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
- Service account passwords and password hashes (while already encrypted at-rest) are additionally encrypted with AES 256-bit encryption using Azure Key Vault.
- Power365 Migration encrypts mailbox and public folders messages using AES encryption and a unique, randomly generated 256-bit key that is unique per message and only held in memory.
- Power365 Email Rewrite Services encrypts email messages using AES encryption and a unique, randomly generated 256-bit key that is unique per message and only held in memory.

Separation of Customer Data

Power365 is architected to prevent data commingling by logically separating customer data. Customer data are differentiated using a Customer Identifier. The Customer Identifier is a unique identifier generated by Power365 when the customer signs up for the application. This identifier is used throughout the solution to ensure strict data separation of customers' data.

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

- All communication to Power365 - including the user interface and associated Azure services - are secured with HTTPS. There are no unsecured external HTTP calls within Power365.
- All communication with Azure Active Directory uses OAuth2 access tokens for Microsoft Graph API operations and HTTPS for PowerShell operations.
- On-premises directory sync agents communicate with on-premises Active Directory using LDAP or LDAPS over TLS 1.2 as configured within the user interface and communicate with Power365 cloud services using HTTPS.
- On-premises device agents poll the Device Agent Cache Service (DACS) using unencrypted UDP or HTTP for efficiency. No sensitive information is exchanged, just a Boolean value indicating when there are jobs queued for the device agent. If DACS indicates there are jobs queued, the device agent communicates securely with the Power365 web service using HTTPS to retrieve the job details.
- Power365 Desktop Agent communicates with Power365 web services using HTTPS over TLS 1.2.
- Power365 Migration reads and writes content using HTTPS over TLS 1.2 data channels.
- Power365 Email Rewrite Services communicates with Microsoft 365 tenants using TLS 1.2 encrypted data channels.

Authentication of Users

- Power365 relies upon Microsoft 365 for authentication which provides customers with an integrated authentication experience where you can move from Power365 to a Microsoft portal seamlessly, without multiple logins and passwords. All while keeping your account security under your organization's policies, rules, and security protocols.
- Power365 also supports Multi Factor Authentication (MFA) for organizations that have enabled MFA within Microsoft 365.
- Registering an Azure Active Directory tenant into Power365 is handled through the Azure Admin Consent workflow and customers can revoke Admin Consent at any time. See https://docs.microsoft.com/en-us/skype-sdk/trusted-application-api/docs/tenantadminconsent for details.

Role Based Access Control

Power365 is configured with role-based access that can be modified only by authorized administrators within the customer's organization and by system administrators.

Each role has a specific set of permissions that determines what tasks a user assigned to the role can perform:

- System Administrator – Reserved for Internal Use. Grants an authenticated user full access to all clients within Power365. This role may grant other users access to applications and assign a permission role to their account.
- Client Administrator – Grants an authenticated user full access to the assigned client's projects. This role may grant other users access to applications and assign a permission role to their account.
- Power User – Grants an authenticated user full access to the assigned client's projects. This role may navigate projects, view reports, and modify application configurations but cannot view Power365 licenses or grant others access.
- Operator – Grants an authenticated user access to the assigned client's migration project and Directory Sync workflow functionality. This role may navigate projects, mange schedules, waves, and migration related actions. This role cannot view Power365 licenses or reports, grant others access or modify application configurations including what is in and out of scope for migration. The Operator role also cannot access the edit, remove, or add functionality for configurations and profiles in Active Directory.

For more information on role-based access control, please refer to the Binary Tree Power365 product documentation.

FIPS 140-2 compliance

Power365 services are built with Azure FIPS 140-2 compliant cryptographic functions. Power365 services make use of FIPS 140-2 compliant encryption keys that are stored in Microsoft Key Vault.

More information:

- Microsoft and FIPS: https://docs.microsoft.com/en-us/compliance/regulatory/offering-FIPS-140-2?view=o365-worldwide
- Encryption in the Microsoft Cloud: https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-encryption-in-the-microsoft-cloud-overview
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide

SDLC and SDL

The Power365 Development team follows a managed Software Development Lifecycle (SDLC).

The Power365 team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security. Only employees on Quest's corporate network have access to these systems. If a Power365 developer leaves the company, they will no longer be able to access Power365 systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

In addition, the Power365 team follows a managed Security Development Lifecycle (SDL) which includes:

- MS-SDL best practices
- Threat modeling
- OWASP guidelines
- Static code analysis is performed on regular basis
- 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

Power365 developers go through the same set of hiring processes and background checks as other Quest employees.

Third party assessments and certifications

Penetration testing

Power365 has undergone a third-party security assessment and penetration test.

Assessment includes but is not limited to:

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

Certification

Power365 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: C710-ISMS222-07-19, valid until 2022-07-29.
- ISO/IEC 27001 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: C711-ITCS2-07-19, valid until 2022-07-29.
- ISO/IEC 27001 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: C712-ITPII2-07-19, valid until 2022-07-29.

Operational Security

Source control and build systems can only be accessed by Quest employees. If an employee with access to Power365 leaves the company the individual loses access to all systems. All code is versioned in source control.

Who at Quest has Access to Data

Access to Power365 data is restricted to:

- Quest Operations team members
- Selected Quest Support team members working on product issues.
- Selected development team members working with the Operations and Support teams.

Access to Power365 data and resources is restricted through Azure RBAC and Azure AD security groups. For each type 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

To access Power365, a customer representative goes to Power365 website and signs up for an Power365 account. When an account is created an organization is also automatically created.

An Azure Active Directory Global Administrator must give the Admin Consent to provision Power365 with the following Microsoft.Graph permissions:

Sign in and read user profile (User.Read)
Permission Definition: Allows users to sign-in to the app and allows the app to read the profile of signed-in users. It also allows the app to read basic company information of signed-in users.
Application Purpose: Used by Power365 Authentication services to connect a tenant or environment using an authorized administrator account.

Read and write all users' full profile (User.ReadWrite.All)
Permission Definition: Allows the app to read and write the full set of profile properties, reports, and managers of other users in your organization, on behalf of the signed-in user. Also allows the app to create and delete users as well as reset user passwords on behalf of the signed-in user.
Application Purpose: Used by Power365 Sync services to provide OneDrive migration activities.

Read and write all groups (Group.ReadWrite.All)

Permission Definition: Allows the app to create groups and read all group properties and memberships on behalf of the signed-in user. Additionally, allows group owners to manage their groups and allows group members to update group content.
Application Purpose: Used by Power365 Sync services to provide OneDrive migration activities.

Read and write directory data (Directory.ReadWrite.All)
Permission Definition: Allows the app to have the same access to information in the directory as the signed-in user.
Application Purpose: Used by Power365 Discovery and Provisioning Services to discover all workloads (such as Organizations, available SKUs, users, groups, contacts, etc.) and to automate M365 licensing.

Access directory as the signed in user (Directory.AccessAsUser.All)
Permission Definition: Allows the app to read and write data in your organization's directory, such as users, and groups. It does not allow the app to delete users or groups or reset user passwords.
Application Purpose: Used by Power365 Discovery & Tenant Health services to provision the Binary Tree PowerShell account and assign the required administrative roles to the account for migration and integration services.

Send mail as user (Mail.Send)
Permission Definition: Allows the app to send mail as users in the organization.
Application Purpose: Used by Power365 Content Migration to send the User Cutover email notification from the administrator's mailbox.

Have full access to all files user can access (Files.ReadWrite.All)
Permission Definition: Allows the app to read, create, update, and delete all files the signed-in user can access.
Application Purpose: Used by Power365 Content Migration to read & write OneDrive files during migration activities.

Operational Monitoring

Power365 internal logging is available to Quest Operations and Power365 support teams during the normal operation of the platform. Some Personally Identifiable Information (PII) (e.g. usernames, email addresses, email aliases, etc.) can become a part of internal logging for troubleshooting purposes. Quest Operations team members have access to Power365's production Azure Subscription and monitor this as part of normal day-to-day operations.

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. Power365 relies on Azure infrastructure and as such, is subject to the possible disruption of these services.

- Power365 status page is available at https://support.quest.com/binary-tree-power365/current
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/

Security Incident Response Management

For its Power365 solution, Quest has established a formal process of preparation, detection, analysis, containment, eradication, recovery, and post-incident activities. As well, in accordance with international privacy laws, Quest has established a Security Breach Notice process.

Customer Measures

Power365 security features are only one part of a secure environment. Customers need to operate by their own best security practices when proceeding with auditing their data. Special care needs to be given to protecting the credentials of the Azure Active Directory Tenants Global Administrator accounts and On Premises Active Directory Administrator accounts.

About us

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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.