



Foglight® 5.9.5

Integration with SAML 2.0 in Azure AD



© 2019 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 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



WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death



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

- Configure Foglight with Azure AD.....4**
 - Before you begin4
 - Step 1: Adding Enterprise Application in AAD.....5
 - Step 2: Configuring SAML SSO on AAD7
 - Step 3: Selecting Attribute Key.....10
 - Step 4: Exporting the Certificate11
 - Step 5: Setting up SAML in Foglight.....12
- About us13**

Configure Foglight with Azure AD

i NOTE: To use SAML SSO with Azure Active Directory (AAD), a Premium edition of AAD is required. Go to: <https://azure.microsoft.com/en-us/pricing/details/active-directory/> for more details. AAD requires HTTPs protocol, therefore Foglight's HTTP SAML login cannot be used on AAD. Foglight HTTPs SAML login supports either the IP address or the host name. For detailed configurations about IP or host name login, see [Before you begin](#) and [Step 2: Configuring SAML SSO on AAD](#).

Before you begin

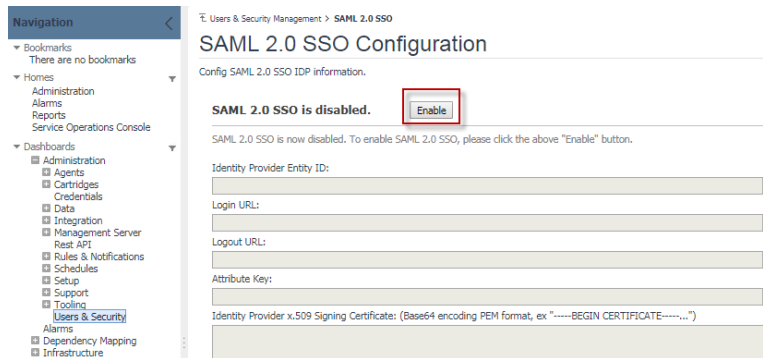
i NOTE:

- If you are about to use SAML IP login, make sure to run the following command:
"-Dquest.saml.hostname=<foglight-server-ip>" to start up your Foglight Management Server.
- When logging into your Foglight Management Server, make sure to keep using the same approach as what you configured during the SAML integrations. For example, if you set up the HTTPS SAML login using the IP address, you must log in to your Management Server with `https://<foglight-server-ip>:<foglight-server-port>`.

You need to enable SAML 2.0 SSO Configuration in your Foglight Management Server prior to setting up the SAML integration. Follow the steps below to enable SAML 2.0 SSO Configuration:

- 1 Log into the Foglight Management Server as Administrator.
- 2 Under **Dashboards**, click **Administration > Users & Security**, and then click **SAML 2.0 Integration Settings**. The *SAML 2.0 SSO Configuration* dashboard appears.

3 Click **Enable**.



4 Download the metadata file, which will be imported to Azure AD in [Step 2: Configuring SAML SSO on AAD](#).

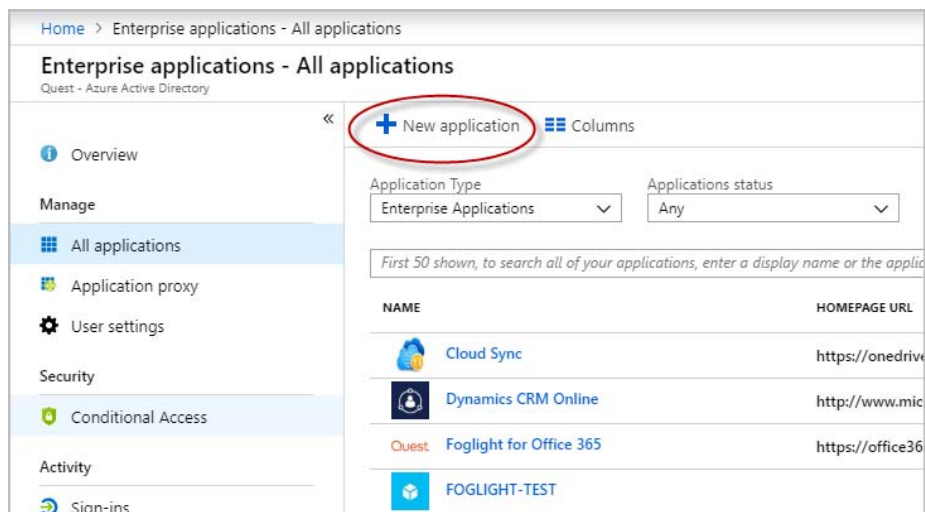
Get the metafile from the Foglight server URL:

- IP login: https://<foglight_server-ip>:<port>/console/saml2/metadata.xml
- Host name login: https://<foglight_server-host-name>:<port>/console/saml2/metadata.xml

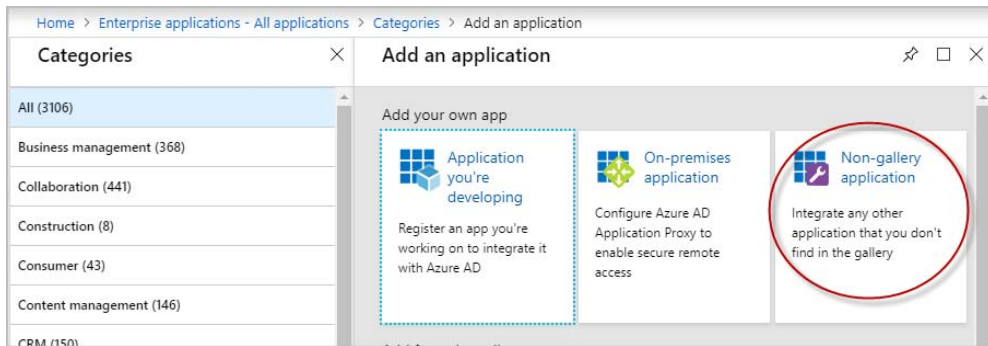
Step 1: Adding Enterprise Application in AAD

To add an Enterprise Application in AAD:

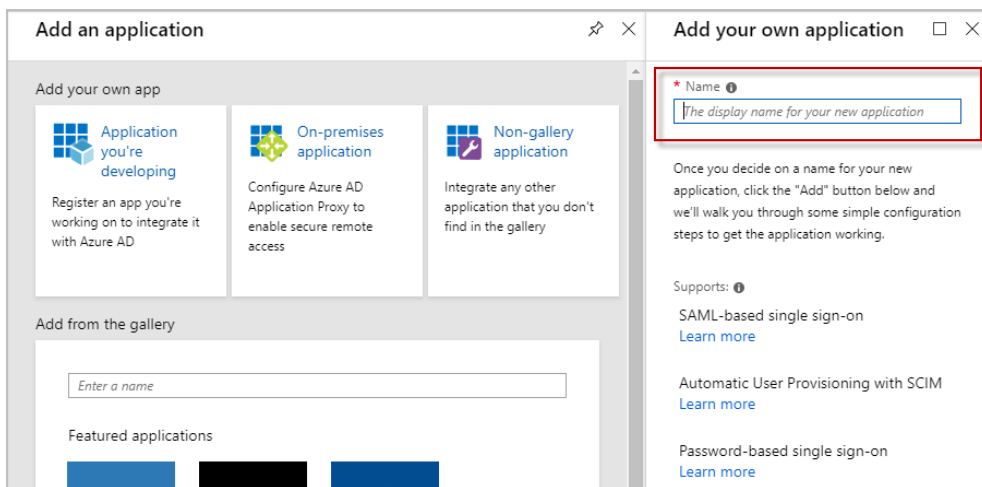
- 1 Go to:
https://portal.azure.com/#blade/Microsoft_AAD_IAM/StartboardApplicationsMenuBlade/AllApps/management/
- 2 Click **New Application** as shown in the figure below.



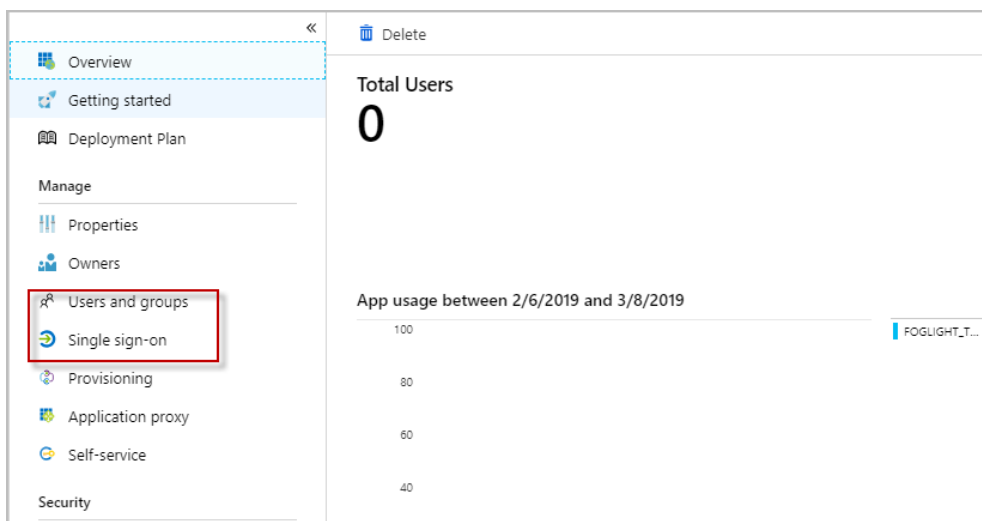
- 3 Then, click **Non-gallery application** as shown in the figure below.

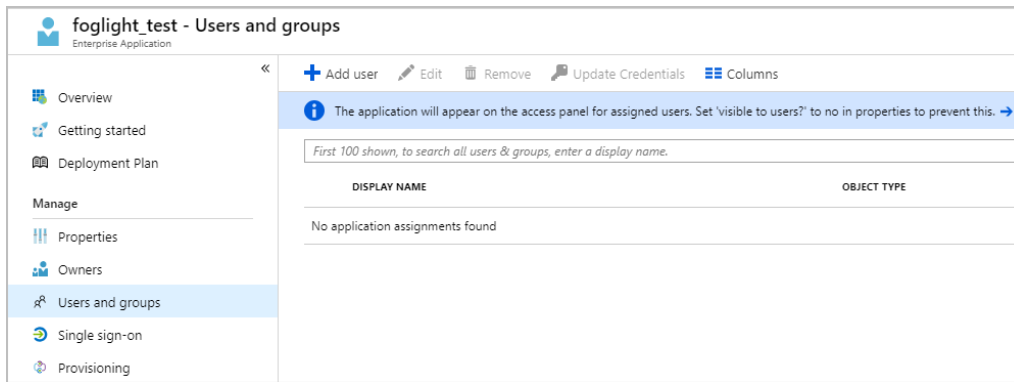


- 4 Input the Name of your application and click **Add**.



- 5 Click **Users and groups** to add a user or a group who needs an access to the application. The assigned user will be able to see the application on the access panel.

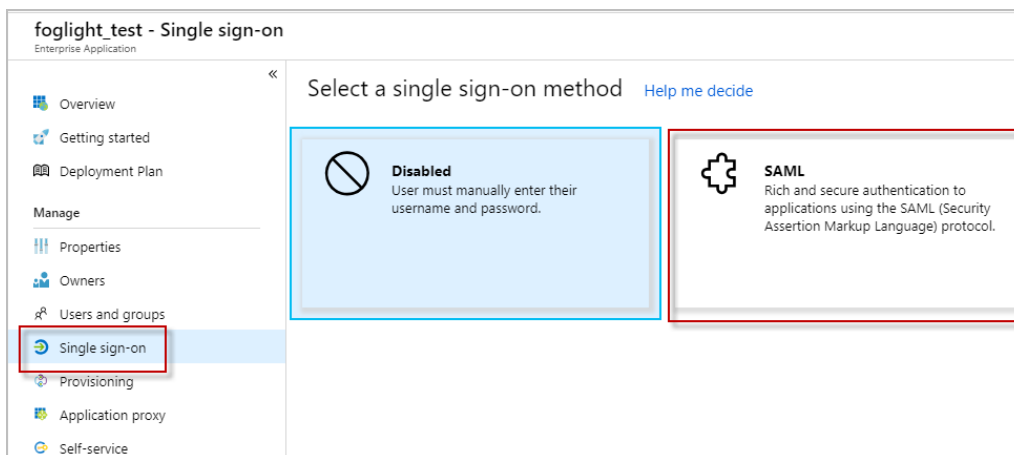




Step 2: Configuring SAML SSO on AAD

To configure SAML SSO on AAD:

- 1 Click **Single sign-on** > **SAML**. A *SAML-based sign-on* page will open.



foglight_test - SAML-based sign-on

Enterprise Application

Overview

Getting started

Deployment Plan

Manage

Properties

Owners

Users and groups

Single sign-on

Provisioning

Application proxy

Self-service

Security

Conditional Access

Permissions

Token encryption (Preview)

Activity

Sign-ins

Audit logs

Troubleshooting + Support

Virtual assistant (Preview)

Troubleshoot

New support request

Change single sign-on mode

Switch to the old experience

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback.

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating foglight_test.

1

Basic SAML Configuration

Identifier (Entity ID)

Reply URL (Assertion Consumer Service URL)

Sign on URL

Relay State

Logout Url

Required

Required

Optional

Optional

Optional

2

User Attributes & Claims

Givenname

Surname

Emailaddress

Name

Unique User Identifier

user.givenname

user.surname

user.mail

user.userprincipalname

user.userprincipalname

3

SAML Signing Certificate

Status

Thumbprint

Expiration

Notification Email

App Federation Metadata Url

Certificate (Base64)

Certificate (Raw)

Federation Metadata XML

Active

4578EEED29167DC0224B44FA49859092EC8B2817

3/8/2022, 11:22:29 AM

ixue@questfive.onmicrosoft.com

<https://login.microsoftonline.com/94172181-7df0-4...>

Download

Download

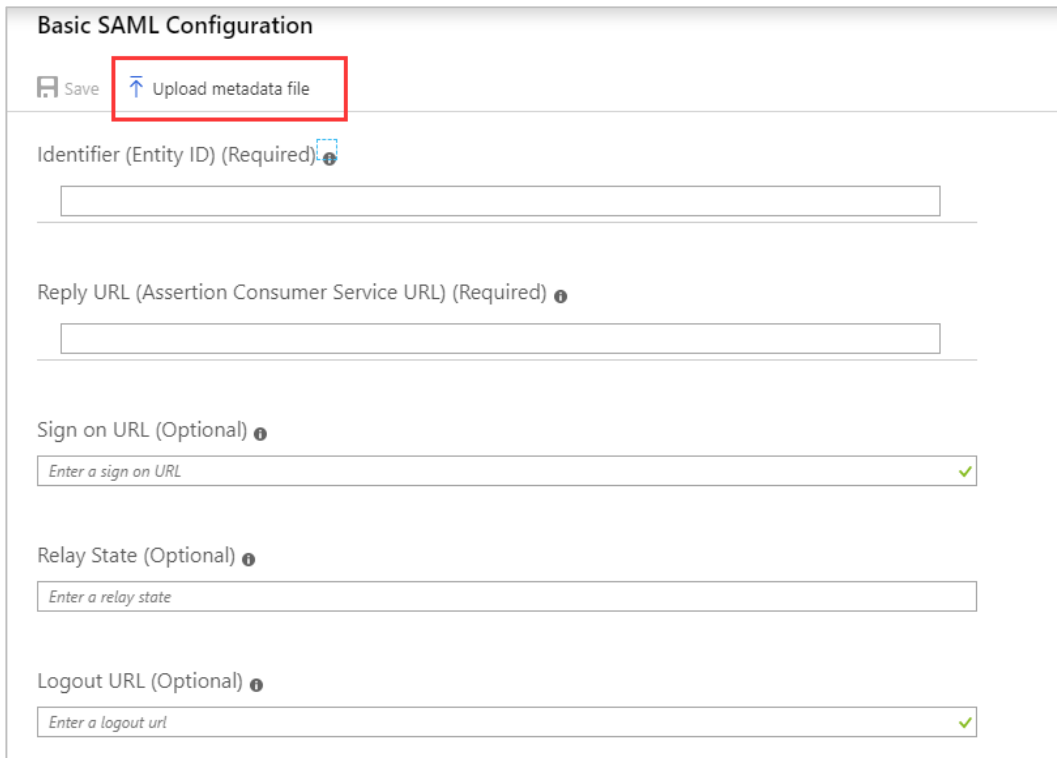
Download

- 2 Click the edit icon on the upper right of **Basic SAML Configuration** section as shown in the figure above. Then, upload the Foglight SSO metadata file.

Identifier and *Reply URL* should be automatically filled.

Make sure the contents are as expected.

- IP login: <https://<foglight-server-ip>:<foglight-ssl-port>/console/saml2/metadata.xml>.
- Host name login: <https://<foglight-server-host-name>:<foglight-ssl-port>/console/saml2/metadata.xml>.



Basic SAML Configuration

Save Upload metadata file

Identifier (Entity ID) (Required) ⓘ

Reply URL (Assertion Consumer Service URL) (Required) ⓘ

Sign on URL (Optional) ⓘ

Enter a sign on URL ✓

Relay State (Optional) ⓘ

Enter a relay state

Logout URL (Optional) ⓘ

Enter a logout url ✓

- 3 Click **Save**.

Step 3: Selecting Attribute Key

To select an attribute key:

- 1 In the *SAML-based sign-on* blade, click the edit icon on the upper right of *User Attributes & Claims* section.

The screenshot shows the 'SAML-based sign-on' configuration page. It has three main sections, each with an edit icon (pencil) in the top right corner. Section 1, 'Basic SAML Configuration', lists fields like Identifier (Entity ID), Reply URL, Sign on URL, Relay State, and Logout Url, with their requirements (Required or Optional). Section 2, 'User Attributes & Claims', lists attributes like Givenname, Surname, Emailaddress, Name, and Unique User Identifier, each with a corresponding value (e.g., user.givenname). This section's edit icon is highlighted with a red box. Section 3, 'SAML Signing Certificate', shows the status (Active), Thumbprint, Expiration, Notification Email, and App Federation Metadata Url.

- 2 Record the **CLAIM NAME** you want to use, which will be needed later in [Step 5](#).

The 'User Attributes & Claims' dialog box is shown. It has a title bar with a close button. Below the title bar is a '+ Add new claim' button. The 'Name identifier value' is set to 'user.userprincipalname [nameid-format:emailAddress]' and 'Groups returned in claim' is set to 'None'. Below this is a table of existing claims.

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

Step 4: Exporting the Certificate

To export the certificate:

- 1 In the *SAML-based sign-on* blade, click the Download link of Certificate (Base64) in *SAML Signing Certificate* section.

Change single sign-on mode Switch to the old experience

Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →

Set up Single Sign-On with SAML - Preview

Read the [configuration guide](#) for help integrating tete.

- 1 Basic SAML Configuration**

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State	Optional
Logout Url	Optional
- 2 User Attributes & Claims**

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- 3 SAML Signing Certificate**

Status	Active
Thumbprint	BD79AB1F2EA91FFFE13C1041522C0FD3AD1574EB
Expiration	2022/3/7 下午4:38:12
Notification Email	mark.bai@questfve.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/94172181-7df0-4...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

- 2 Open the downloaded certificate file as a text file, which will be needed in [Step 5](#).

Step 5: Setting up SAML in Foglight

To set up SAML in Foglight Management Server:

- 1 Log in to the Foglight Management Server as Administrator.
- 2 Under **Dashboards**, click **Administration** > **Setup** > **SAML 2.0 SSO**. The SAML 2.0 SSO Configuration dashboard appears.
- 3 Click **Edit Settings** and configure the SAML settings as below.
 - a) *Identity Provider Entity ID*: The value is in AAD *SAML-based sign-on* blade section 4, marked as *Azure AD Identifier*.
 - b) *Login URL*: The value is in AAD *SAML-based sign-on* blade section 4, marked as *Login URL*.
 - c) *Logout URL*: The value is in AAD *SAML-based sign-on* blade section 4, marked as *Logout URL*.
 - d) *Attribute Key*: It is the CLAIM NAME you chose in Step 3. For example, it can be <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name>.
 - e) *Identity Provider x.509 Signing Certificate*: Copy the content of the certificate file exported in [Step 4: Exporting the Certificate](#).
- 4 Click **Apply Configuration** to save the configuration.

Then, the configuration of integrating SAML 2.0 SSO with the Foglight Management Server in AAD is completed.

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.