

Foglight<sup>®</sup> 7.3.0

### Integration with SAML 2.0 in ADFS



#### © 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 <a href="https://www.quest.com/legal">https://www.quest.com/legal</a>.

#### 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.

Foglight  $^{\odot}$  7.3.0 – Integration with SAML 2.0 in ADFS Foglight Version– 7.3.0

### Contents

Foglight and SAML 2.0 Integration in ADFS	4
Before you begin	5
Step 1: Adding Relying Party Trust in ADFS	5
Step 2: Editing Claim Rules	8
Step 3: Configuring Endpoints	10
Step 4: Configuring Signature and Hash Algorithm	12
Step 5: Exporting the Certificate	14
Step 6: Configuring the Trust Relationship	15
Step 7: Setting up SAML in Foglight	15
About us	17

# Foglight and SAML 2.0 Integration in ADFS

Starting with release 5.9.3, Foglight<sup>®</sup> Management Server supports Active Directory Federation Services (ADFS) 2.0 and PingFederate 8.x (and later) using the Security Assertion Markup Language (SAML) 2.0 protocol. Follow the below steps in sequence to completely integrate SAML SSO with the Foglight Management Server on the ADFS sever.

- **NOTE:** ADFS requires https protocol, so Foglight's http SAML login cannot be used on ADFS. Foglight https SAML login could be using either IP address or the host name. For detailed configurations about IP or host name logon, see Before you begin, step 8 & 9 in the Step 1: Adding Relying Party Trust in ADFS section, and step 3 in the Step 3: Configuring Endpoints section.
- Before you begin
- Step 1: Adding Relying Party Trust in ADFS
- Step 2: Editing Claim Rules
- Step 3: Configuring Endpoints
- Step 4: Configuring Signature and Hash Algorithm
- Step 5: Exporting the Certificate
- Step 6: Configuring the Trust Relationship
- Step 7: Setting up SAML in Foglight

### Before you begin

#### 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 Sever 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 a Security 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.



## Step 1: Adding Relying Party Trust in ADFS

To add Relying Party Trust:

- 1 Open the ADFS Management Console.
- 2 Navigate to Trust Relationships > Relying Party Trusts. Right click Relying Party Trusts, and then select Add Relying Party Trust… from the context menu.

🐚 AD F5 2.0		
翰 File Action View W	indow Help	
🗢 🔿 🔰 🖬 🚺 🖬	9	
AD FS 2.0	Relying Party Trusts	
🖃 🚞 Service		
Endpoints		
Certificates		
Claim Descriptions		
🖃 🧮 Trust Relationships		
Claims Provider Tr	usts	
Relving Party Tru		
Attribute Stores	Add Relying Party Trust	
- Handado Stores		
	View •	
	New Window from Here	
	Definish	
	Kerresii	
	Help	
1		
1		

- 3 Click **Start** on the *Add Relying Party Trust Wizard*.
- 4 Select Data Source: Select Enter data about the relying party manually and click Next.

Steps	Select an option that this wizard will use to obtain data about this relying party.
Velcone     Select Data Source     Specity Display Name     Croce Profile     Configure Certificate     Configure URL     Presh	Sector at robot in the robot window model on date to date and date date date. The hyperty party  Leve this option to input the necessary date and certificates from a relying party organization that  publishes its fideration metadate only file of the necessary date and certificates from a relying party organization that  publishes its fideration metadate on https://www.certificates.from a relying party organization that  publishes its fideration metadate on https://www.certificates.from a relying party organization that  publishes its fideration metadate on https://www.certificates.from a relying party organization that  has  response to the relying party from a file  Leve the option to fideration the necessary date and certificates from a relying party organization that  has  response to the fideration metadate on the file. Federation metadate file location: Federation metadate

- 5 Specify Display Name: Specify a display name and click Next.
- 6 Choose Profile: Select AD FS 2.0 and click Next.



7 Configure Certificate: Click Next.

i

- 8 *Configure URL*: Select **Enable support for the SAML 2.0 WebSSO protocol**, and then input Foglight's SAML 2.0 metadata URL in https, which is:
- **NOTE:** ADFS requires https protocol, so Foglight's http SAML login cannot be used on ADFS.

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

steps	AD FS 2.0 supports the WS-Trust_WS-Federation and SAML 2.0 WebSS0 protocols for relying parties. If
Welcome     Select Data Source     Specity Display Name     Chross Piolie     Configure Certificate     Configure URL     Configure URL     Configure URL     Configure Identifiers     Chaose Issuence     Authorization Fulses     Ready to Add Trust     Finish	Bit Subscription       Bit Subscription         Bit Subscrit Subscripti

9 *Configure Identifiers*: Input Foglight's SAML 2.0 metadata https URL used in step 8 in the **Relying** party trust identifier field, click **Add**, and then click **Next**.

Madd Relying Party Trust	Wizard D
Steps Welcome Select Data Source Specify Display Name	Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust. Relying party trust identifier. Inter://acgs@d22.prod quest.com/8443/console/cam/2/metadata.vml
Choose Profile     Configure Certificate     Configure URL     Configure Identifiers	Exemple: https://it.contexs.com/adfs/services/itust Relying party trust identifies: Bernove Be
<ul> <li>Choose Issuance Authorization Rules</li> <li>Ready to Add Trust</li> <li>Finish</li> </ul>	
	<previous 1000="" cancel="" help<="" td=""></previous>

10 *Choose Issuance Authorization Rules*: Select **Permit all users to access this relying party** and click **Next**.



- 11 Ready to Add Trust: Click Next.
- 12 *Finish*: Make sure to select **Open the Edit Claim Rules dialog for this relying party trust when the wizard closes**, and then click **Close**.

Steps	The relying party trust was successfully added to the AD FS configuration database.
Welcome Select Data Source	You can modify this relying party trust by using the Properties dialog box in the AD FS 2.0 Management map in.
Specify Display Name	Open the Edit Claim Rules dialog for this relving party trust when the wizard closes
Choose Profile     Configure Certificate	
Configure URL	
Contigure Identifiers     Choose Issuance     Authorization Rodes	
Ready to Add Trust	
Finish	

#### **Step 2: Editing Claim Rules**

To edit Claim Rules:

1 On the prompted Edit Claim Rules dialog box, click Add Rule…

🙀 Edit Claim Rules for jason test		×
Issuance Transform Rules Issuance Authorization Rule	s Delegation Authorization Rules	
The following transform rules specify the claims that wil	I be sent to the relying party.	
Order Rule Name	Issued Claims	
	Ť	
Add Rule Edit Rule Remove Rule		
OK Ca	ancel Apply Help	1

2 Choose Rule Type: Select Send LDAP Attributes as Claims and click Next.

Steps	Select the template for the claim rule that you want to create	e from the following list. The description		
Choose Rule Type	provides details about each claim rule template.			
Configure Claim Rule	Claim rule template:			
	Send LDAP Attributes as Claims	-		
	Claim rule template description:			
	coste a rule thui wit entitical athoba e values for softwerko. telephoneNume Active Declose) tabutates and then our en- clasmin. The rule may also be used to ared all of the user i individual groups methorithique, user the Sind Charlow Method Tel me more about the sub-template	arte uizen forn the disaja/Name and di fore values as di vos different cuoping group nemberitips. Il you want to only send enship as a Claim wile template.		

3 *Configure Claim Rule*: Specify a rule name, and select **Active Directory** as the **Attribute store**. Add LDAP attributes mapping as below, and then click **Finish**.

🎭 Add Transform Claim Rule	Wizard					×
Configure Rule						
Steps Choose Rule Type Configure Claim Rule	You c which issued Claim ( Email 1) Rule b Attribu Active	en configure this rule to send the to extract LDAP attributes. Speci from the rule. use name: to Learn emplate: Send LDAP Attributes a le store: Directory	a values of L illy how the	DAP athibutes as claims. S athributes will map to the or	Select an athibute store from urgoing claim types that will be	
	) ) ) ) )	DUAP Ambué E MaiAddesses SAM-Accourt Name Display-Name	y dan que	Outgoing Claim Type E-Mail Address Name Common Name	v v v	
			< Pre	wious Finish	Cancel Help	J

4 Click Add Rule… button again to add another rule on the Edit Claim Rules wizard.

🕽 Edit Cla	im Rules for jason test		_ 🗆 🗙
Issuance	Transform Rules Issuance Authorization R	ules Delegation Authorization F	ules
The fol	, owing transform rules specify the claims that	will be sent to the reluing party	
	r	million to the toying party.	
Order	Rule Name	Issued Claims	
	Email to Learn	E-Mail Addless,Naille,Co	
			<u> </u>
			+
		1	
Add	Remove Rule		
	OK	Cancel Apply	Help

5 *Choose Rule Type*: Select **Transform an Incoming Claim** and click **Next**.



6 *Configure Claim Rule*: Specify a rule name and configure it as below, and then click **Finish**.

. As an option, you ning claim type to new claim value.
new claim value.
•
*
-
•
V\$8
2012

7 Click Apply to apply the configuration then click OK to close the Edit Claim Rules wizard.

Edit Claim Rules for jason test	
ssuance Transform Rules   Issuance Authorization R	ules Delegation Authorization Rules
The following transform rules specify the claims that	will be sent to the relying party.
Order Rule Name	Issued Claims
1 Email to Learn	E-Mail Address,Name,Co
2 Transform Command Name to NameID	Name ID
were there is not	-1
Add Hule Edit Hule Hemove Hule	<u>.</u>
ОК	Cancel Apply Help

#### **Step 3: Configuring Endpoints**

To configure endpoints:

1 Right click the Relying party Trusts item that you added above, and then click **Properties**.



2 Select Endpoints on the Properties wizard, and then click Add.

Monitoring Ide Accepted Claims Orga Specify the endpoints to protocols.	entifiers anization use for SAM	Encr Endpoint	vption   s Notes	Signature
Specify the endpoints to protocols.	use for SAM			Auvanceu
		IL and WS	-FederationP	assive
URL		Index	Binding	Default F
SAML Assertion C	onsumer E	ndpoints		
https://gcgq6q52.p	rod.quest	0	POST	No
				F
Add Re	move	Edit	Sel	t Default
ПК	1 Cano	sel 1	Annlu	Help

- **3** You need add two Endpoints, including SAML Assertion Consumer endpoint and SAML Logout endpoint.
  - **a** For the URL field of SAML Assertion Consumer endpoint, the value is:
    - IP logon: https://<foglight-server-ip>:<foglight-sslport>/console/saml2/saml\_assertion\_consumer
    - Host name logon: https://<foglight-server-host-name>:<foglight-sslport>/console/saml2/saml\_assertion\_consumer

Configure the other fields as below, and then click **OK** when you finish.

jason test Properties 🛛 🔀
Monitoring Identifiers Encryption Signature
Add an Endpoint 🛛 🔀
Endpoint type:
SAML Assertion Consumer
Rinding
Index: 2
URL:
https://qcgq6q52.prod.quest.corp:8443/console/saml2/saml_assertion_c/
Example: https://sts.contoso.com/adfs/ls
Response URL:
Example: https://sts.contoso.com/logout
UK Cancel Help
OK Cancel Apply Help

- **b** Both the URL and Response URL fields of SAML Logout endpoint are:
  - □ IP logon: https://<foglight-server-ip>:<foglight-ssl-port>/console/saml2/slo
  - Host name logon: https://<foglight-server-host-name>:<foglight-sslport>/console/saml2/slo

Configure the other fields as below, and then click **OK** when you finish.

jason test Properties 🔀
Monitoring Identifiers Encryption Signature
Add an Endpoint
Endpoint type:
SAML Logout
Binding:
Redirect
Index: 0
URL:
https://qcgq6q52.prod.quest.corp:8443/console/saml2/slo
Example: https://sts.contoso.com/adfs/ls
Response URL:
https://qcgq6q52.prod.quest.corp:8443/console/saml2/slo
Example: https://sts.contoso.com/logout
OK Cancel Help
OK Cancel Apply Help

c Select the default **SAML Assertion Consumer Endpoint** which index is 0, and then click **Remove** to delete it.



## Step 4: Configuring Signature and Hash Algorithm

To configure Signature and Hash algorithm:

1 Select Signature on the Properties wizard, and then click Add.

son test Properti	es			I
Accepted Claims Monitoring	Organization   Identifiers	rganization Endpoints Note Identifiers Encryption		Advanced Signature
Specify the signal party.	ure verification ce	tificates for requ	ests from	this relying
Subject	Issuer	Effective	e Date	Expiratio
·	ם ה		1	
Add	View	Remove	]	
	JK Can	cel Ap	ply	Help

2 Add a Foglight server's signature file. You can get a default one from *<foglight-serverdirectory>/config/sam\_certificate.pem* or you can generate your own signature file.

jason test Properti	es			>
Accepted Claims	Organization	Endpoints	Notes	Advanced
Monitoring	Identifiers	rs Encryption S		Signature
Specify the signa party.	ture verification ce	tificates for req	uests from t	his relying
Subject	Issuer	Effectiv	/e Date	Expiratio
۲ Add.	View	Remove	]	Þ
(	JK Can	cel A	.pply	Help

3 After adding the signature file, select **Advanced** and choose **SHA-1** option for the **Secure hash algorithm** field, and then click **Apply**.



4 Click **OK** to finish the Properties configuration.

## **Step 5: Exporting the Certificate**

To export the certificate:

1 Navigate to Service > Certificates on the ADFS Management Console, right click the Token-signing item, and then click View Certificate…

N- 10 55 0.0					
MD FS 2.0					
🗌 File Action View Window Help					
🗢 🔿 🔁 🖬 🛛 🖬					
AD F5 2.0	Certificates				
E Service	Subject	Issuer	Effective D		
Certificates	Service communications				
Claim Descriptions  Trust Relationships	E CN=zhuvm-fog-2639.sub1.ssoexample.com	CN=zhuvm-fog-2639.sub1	5/2/2018		
Claims Provider Trusts	Token-decrypting				
Attribute Stores	CN=ADFS Encryption - zhuvm-fog-2639.sub1.ssoexample.com	CN=ADFS Encryption - zh	5/2/2018		
	Token-signing				
	E CN=ADFS S View Certificate 1.ssoexample.com	CN=ADFS Signing - zhuv	5/2/2018		
	Set as Primary				
	Help				

2 Select **Details** on the pop-up **Certificate** wizard and click **Copy to File**... to export the certificate which will be used in the following Foglight SAML setup.

ertificate General Details Certification Pat	h)
Show: <all></all>	
Field	Value 🔺
Version	V3
Serial number	78 6F f9 22 80 95 0b 8d 4b 81
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADF5 Signing - zhuvm-fog-263
Valid from	Wednesday, May 02, 2018 4:
🛅 Valid to	Thursday, May 02, 2019 4:20:
Subject	ADF5 Signing - zhuvm-fog-263 💌
Learn more about <u>certificate detai</u>	Edit Properties
	OK

3 Select Base-64 encoded X.509 (.CER) format as the export file type.



## Step 6: Configuring the Trust Relationship

To configure the trust relationship:

- 1 On the ADFS server machine, run PowerShell as administrator.
- 2 Run the following command to load the ADFS PowerShell module.

Add-PSSnapin Microsoft.Adfs.PowerShell

- 3 Run the following two commands to set up the trust relationship. You need to change the *<relying-party-trust-display-name>* to the **Display Name** of the Relying Party Trust that you have added in Step 1: Adding Relying Party Trust in ADFS.
- Set-ADFSRelyingPartyTrust TargetName <relying-party-trust-display-name> -SigningCertificateRevocationCheck None
- Set-ADFSRelyingPartyTrust TargetName < relying-party-trust-display-name> -EncryptionCertificateRevocationCheck None

## Step 7: Setting up SAML in Foglight

To set up SAML in the Foglight Management Server:

- 1 Log into the Foglight Management Server as a Security Administrator.
- 2 Under **Dashboards**, click **Administration** > **Users & Security** > **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 should be https://<ADFS\_SERVER>/federationmetadata/2007-06/federationmetadata.
- **b** *Login URL:* The value should be https://<ADFS\_SERVER>/adfs/ls/.
- c Logout URL: The value should be https://<ADFS\_SERVER>/adfs/ls/.
- **d** *Attribute Key*: It depends on the identity key selected to identity the user. 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 which you have exported in Step 5: Exporting the Certificate.

SAML 2.0 SSO Configuration
Config SAML 2.0 SSO IDP information.
SAML 2.0 SSO is enabled. Disable
SAML 2.0 SSO is now enabled. IDP information can be edited as below.
Identity Provider Entity ID:
https://zhuvm-fog-2639.sub1.ssoexample.com/federationmetadata/2007-06/federationmetadata.xml
Login URL:
https://zhuvm-fog-2639.sub1.ssoexample.com/adfs/ls/
Logout URL:
https://zhuvm-fog-2639.sub1.ssoexample.com/adfs/ls/
Attribute Key:
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Identity Provider x.509 Signing Certificate: (Base64 encoding PEM format, ex "BEGIN CERTIFICATE")
BEGIN CSRTIFICATE MIDADCC-49,amiBaQLogCiSIoC/C+11_gVQGVHuoPJANBglkqhkiG9w0BAQsFADA8 MTowOAYDVQQDEF8REZTIFNQZ35bmcgLS86aHV265Inhz2dflyz055adWUxInkz b2V4W1Vib6UV29MB4VKDT4HDOUM4A9HqliL11X0TESMDUwH4PIAJ1A11w0PDE6 M0gGALUEAvhQURGUV29MB4VKDT4HDOUM4A9HqliL11X0TESMDUwH36AHQJA110xPDE6 M0gCALUEAvhQURGUV29MB4VKDT4ZDLWAUA8DA00gEFADCCAQcQgEBA91qOrU bywyhtiOCQD+Cz8uGrgfMSGlb/SQGGMy40wW5x+VQuZMenll2a29jh1MvA0hFBu XyH2YY1B0HC4VSGU/4+xpUKeABVEABVWW5x+VQuZMenll2a29jh1MvA0hFBu KyH2Y1KB1GCZ28PKPK8hbteHM0DKu-d+HNLwTICorytb0HISJSQUR3VWFCQAUCUB 4QW0B85aqaz2Z8PkR4hbteHM0DKu-d+HNLwTICorytb0HISJSQUR3VWFCQAUCUB 4QW0B4C5GAV47Q2CELB4QH4A95HG284X2/VXXKdFxtXVVPHF8WISJMPK2AUCUB 4QW0FB4D9bcC/w4cATA14Bqhki6S9WC31+4+F8K4ACQE2LTVF18HbtF8WISJMPIIz H70vFJ7hIEK4Q23mgdebuzpc4PH47y80+Xp2C+q22Q2PI7E18+1VUJAk 3=945aZ2782FkR4hde3Hd1293HcZ73+pQMv8A2G72F97LF3+14QUZM1 4yW0534qnAlB8VH7873hHt21d1g92Thy4aB41Q-3mvZ247fz2+1sqvZDFTT 4g4bLH47gastHvd55JHH4730488PKr31+4+LF3CF12F44F42CF2LF2+15QVZDFTT 4g4bLH47gastHvd55JHH47305HZ74F42F2F42F42F42F42F44F4 4g4bLH47gastHvd55JH44735JH274773F2F744F42F11F44F44F4 4g4bLH47gastHvd55JH44735JH2747742F472F474F42F474F44F4745H474744 4g4bLH47gastHvd55JH44735JH2747745F4747474744F45414945H4277478F4747444F4541447474747474747474747474747474747474
Edit Settings Apply Configuration

4 Click **Apply Configuration** to save the configuration.

Then configurations of integrating SAML 2.0 SSO with the Foglight Management Server in ADFS are 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<sup>™</sup>.

#### 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.