Security Managemnet Platform Shared Services

Security Guide

© 2026 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.
10801 N. Mopac Expressway
Building 3, Suite 400
Austin, TX 78759

Refer to our website (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 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 www.quest.com/legal. Microsoft, Active Directory, ActiveSync, Excel, Lync, and Skype are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. 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, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Security Managemnet Platform Shared Services Security Guide
Updated - September 2026

Contents

About Security Management Platform Shared Services 5
About Security Management Platform Core 5

Architecture Overview 6

Authentication and Consents 7
User Authentication 7
Quest Security Management Platform Application Consent 7
Admin Consent and Service Principals 8

About the On-Premises Agent 8

Role Based Access Control 9

Auditing 9

Public API 9

Data Egress Service 10

Azure Datacenter Security 10

AWS Data Center Security 10

Overview of Data Handled by Security Management Platform Core 11
Data Handled by Core 11
Email Handling by the Data Egress Service 12
AI Services 12
Data Handled by Common Storage Services 12

Location of Customer Data 13

Privacy and Protection of Customer Data 14

Separation of Customer Data 14

Network Communications 14

FIPS 140-2 Compliance 15

SDLC and SDL 16

Third party Assessments and Certifications 17
Penetration testing 17
Certification 17

Operational Security 18
Access to Data 18

Permissions Required to Configure and Operate Security Management Platform 18
Operational Monitoring 18
Production Incident Response Management 18
Security Incident Response Management 18

Customer Measures 19

About us 20

About Security Management Platform Shared Services

Managing information system security is a priority for every organization. In fact, the level of security provided by software vendors has become a differentiating factor for IT purchase decisions. Quest strives to meet standards designed to provide its customers with their desired level of security as it relates to privacy, confidentiality, integrity and availability.

This document describes the security features of Quest Security Management Platform core services such as the Security Management Platform Notification Service and other shared services. This includes access control, protection of customer data, secure network communication, and cryptographic standards.

About Security Management Platform Core

Security Management Platform Core is a cloud-based service that provides core services to other Quest Software as a Service (SaaS) product solutions.

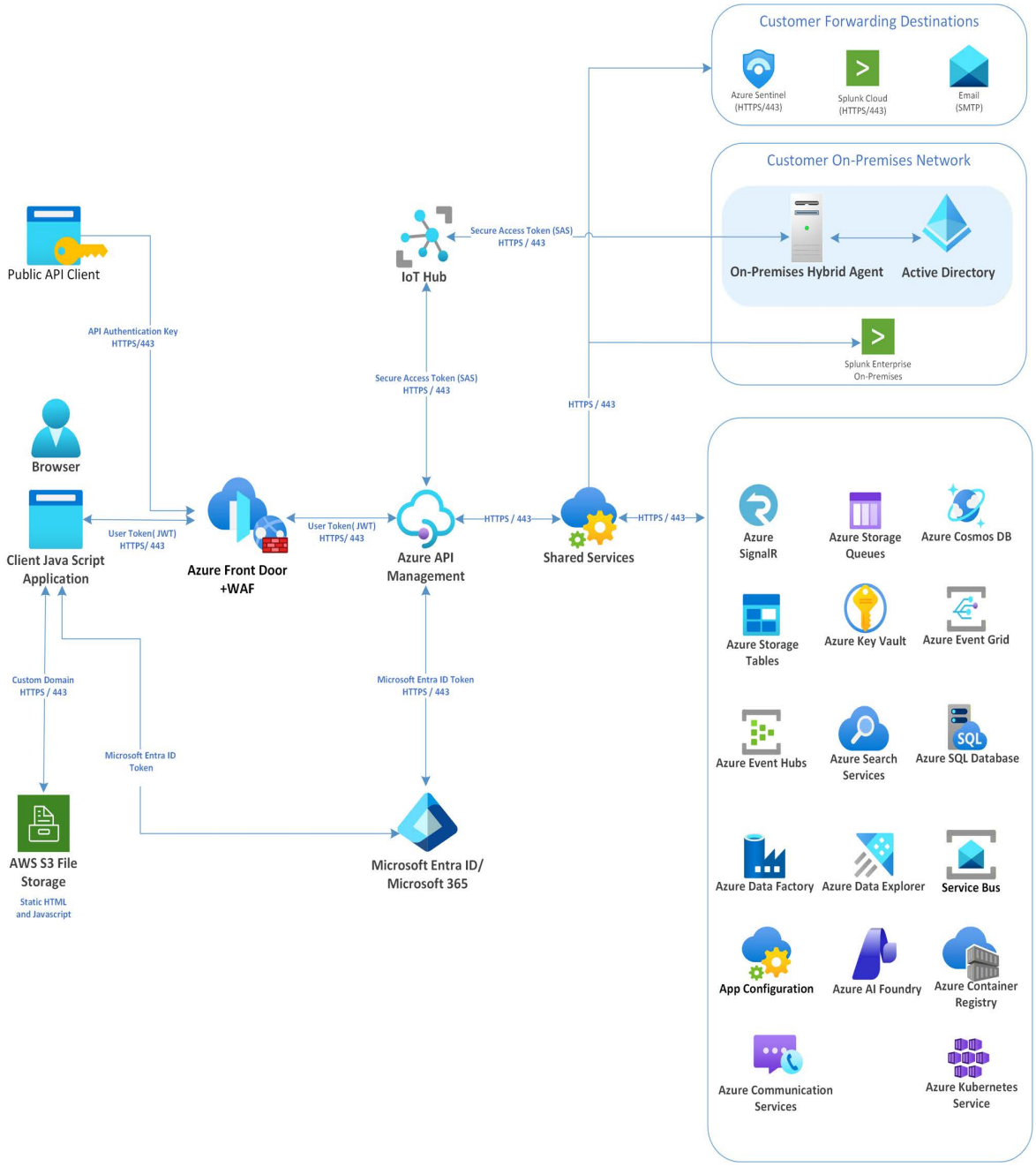
The core services provided are as follows:

- Uniform user interface experience
- Direct Microsoft Entra ID Identity Management integration for secure and seamless authentication
- Authorizing access to Microsoft Entra ID tenant (admin consent)
- Common auditing and logging
- Notifications to other Quest SaaS products about key events
- Subscription management (records of purchases)
- Role Based Access Control where each role has a specific set of permissions that determines tasks a user can perform
- Connectivity to on-premises Active Directory domains in hybrid environments to perform management activities
- Common storage services allowing storage and fast ad-hoc searching of big data in the form of activity data or snapshot data collected from integrated Security Management Platform services
- Services for providing alerting on changes to data stored with common storage services

The majority of these services are delivered through Microsoft Azure cloud services. The exception being the user interface, which is delivered using Amazon Web Services CDN network.

Architecture Overview

The following schema shows the key shared components of the Security Management Platform configuration.



NOTE: Azure Active Directory is now Microsoft Entra ID.

Authentication and Consents

Authentication is required when you log on to Security Management Platform. Authorization is the consent required to create and access an Security Management Platform organization.

User Authentication

Signing into Security Management Platform is done through Microsoft Entra ID. Authenticating through Microsoft Entra ID provides native granular control and allows you to manage your configuration from a central location. It allows configuring advanced security layers through your own conditional access policies, such as MFA, integration with OKTA and other applications that work with the Microsoft Authentication Library (MSAL).

A Microsoft Entra ID access token (constrained to the Quest Security Management Platform application) is obtained when the user proceeds through the authentication step. This Microsoft Entra ID access token has a lifetime limit of 10 minutes after which it is automatically refreshed if the user is actively using application. The user is automatically logged out following a period of inactivity. If the user token is revoked in Microsoft Entra ID, the user will continue to have access to Security Management Platform until the token expiry, for a maximum of 10 minutes. User access to Security Management Platform organizations can be also revoked within Security Management Platform by a Security Management Platform Organization Administrator, resulting in access loss after token expiry.

Quest Security Management Platform Application Consent

As part of the login process with Microsoft Entra ID, users must consent to the set of minimal permissions required by the Quest Security Management Platform application. By default, all users are allowed to consent to applications for permissions that do not require administrator consent. This behavior might be disabled in some Microsoft Entra tenants and may require tenant administrators to enable user consent flow for the Quest Security Management Platform application.

NOTE:

- The ability to consent on behalf of your organization is available if logging in as the global administrator in the tenant.
- The ability to request consents will only be available if the global administrator has enabled the admin consent workflow. See https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-admin-consent-workflow#enable-the-admin-consent-workflow.
- The verified publisher domain and permissions will be clearly labeled and detailed.

Table 1. Quest Security Management Platform Application required permissions

Permission	Description
View your basic profile	Permission required for Quest to access users name and email to display the logged in user.
Maintain access to data you have given it access to	Permission is automatically included and required by Microsoft for Single Page Applications as it gives access to critical refresh tokens for proper functionality. This permission scope is required for single sign on (SSO) and allows a refresh token to be returned from the authentication flow to avoid Security Management Platform prompting the user every time their primary authentication token times out.

Admin Consent and Service Principals

Security Management Platform requires some access to Microsoft Entra ID when adding tenants to your organization. You grant that access by using the Microsoft Admin Consent process. Customers can revoke Admin Consent at any time. See https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/delete-application-portal?pivots=portal#delete-an-enterprise-application.

Quest is a Microsoft Verified Publisher and, as an additional security measure during the Admin Grant process, the customer can verify that the grant request is indeed initiated by Quest.

Details on Verified Publisher are available at https://learn.microsoft.com/en-us/entra/identity-platform/publisher-verification-overview.

The Admin Consent process of Security Management Platform - Core - Basic will create a Service Principal in the customer Microsoft Entra tenant with the following permissions.

- Read organization information
- Read all audit log data
- Read all usage reports
- Read directory data
- Read all applications
- Sign in and read user profile

About the On-Premises Agent

The Quest Security Management Platform On-Premises Agent provides connectivity to on-premises Active Directory domains in hybrid environments to perform management activities such as modifying group memberships and collecting Active Directory object attribute data. All On-Premises Agent communication with Security Management Platform is secured by means of a MQTT-based Shared Access Signature (SAS) token authenticated connection.

For more information about adding and configuring the On-Premises Hybrid Agent, see the “Adding an on-premises agent” section of the Quest Security Management Platform User Guide.

Role Based Access Control

Security Management Platform is configured with default roles that cannot be edited or deleted, and also allows you to add custom roles to make permissions more granular. Each access control role has a specific set of permissions that determines what tasks a user assigned to the role can perform.

For more details, see “Adding Users to an Organization “in the Security Management Platform Global Settings User Guide.

Auditing

Security Management Platform Core provides an activity trail log for the following actions:

- Adding and removing an Office 365 tenant
- Granting of Admin Consent for the tenant
- Adding and removing hybrid agents, domains and relevant capabilities
- Authorizing and de-authorizing users as a Security Management Platform administrator
- Notification settings modification
- Privileged actions on system objects for Security Management Platform products
- Any role granted to users in the organization, not only Security Management Platform Administrator.
- Changes in the subscription status in organization and offboarding events.

NOTE:

-
- Audit data is stored in Azure SQL database and is available via JWT authenticated access to Security Management Platform administrators only.
- Account creation, password reset, and everything around authentication is not tracked by Security Management Platform. This data is stored in the Microsoft Entra ID log found in the tenant Audit Logs.

Public API

The Platform provides a GraphQL-based Public API that enables customers to securely integrate with platform services and automate reporting and monitoring tasks. The API supports programmatic access to platform data and functionality while enforcing the same security boundaries, authorization controls, and tenant isolation used throughout the Platform user interface. Access to the Public API is restricted to authenticated tokens and is governed by the Platform Role Based Access Control (RBAC) system. The Public API does not provide a mechanism to bypass security controls or access data beyond the permissions assigned to the calling identity.

All communication with the Public API is protected using industry-standard HTTPS encryption. Requests are authenticated using Microsoft Entra ID and authorized within the context of the customer's Platform organization. As with all Platform services, customer data accessed through the Public API remains logically separated from

other customer organizations and is subject to the same data protection, encryption, and operational security controls applied throughout the Platform.

Data Egress Service

The Egress Service is a cloud based service delivered through Azure Services, which provides functionality to transfer incoming events to given destination.

Data egress service enables customers to set up event forwarding to SIEM Tools like Splunk, Sentinel or via Email Notifications.

Azure Datacenter Security

Microsoft Azure datacenters have the highest possible physical security and are considered among the most secure and well protected datacenters in the world. They are subject to regular audits and certifications including Service Organization Controls (SOC) 1, SOC 2 and ISO/IEC 27001:2005. Relevant references with additional information about the Windows Azure datacenter security are listed below.

- 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

AWS Data Center Security

Amazon Web Services (AWS) data centers have the highest possible physical security and are considered among the most secure and well protected data centers in the world. They are subject to regular audits and certifications including SOC 2 and ISO/IEC 27001.

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

- AWS Security and Infrastructure: https://aws.amazon.com/products/security/
- AWS Compliance: https://aws.amazon.com/compliance/

Overview of Data Handled by Security Management Platform Core

This section describes how Security Management Platform core services handle data.

Data Handled by Core

- Managed Data Types
- Subscription Services

Managed Data Types

Security Management Platform Core manages the following types of customer data. By default, the data is persisted in Security Management Platform Core.

- Microsoft Entra Tenant Name
- Microsoft Entra Subscription Active Directory Object Id (GUID)
- Microsoft Entra Administration Consent Token
- Microsoft Entra User Object Identifiers (GUID)
- Microsoft Entra Group Object Identifiers (GUID)
- Audit log of Security Management Platform Core user activities, including user name in email form (name@domain.com)

Subscription Services

The Subscription Service stores customer contact information and can process credit card transactions associated with subscription purchases and renewals.

- Cybersource is the credit card payment gateway. Cybersource receives the necessary information required for purchase transactions. Required fields are as follows:
  - credit card number
  - expiration date
  - name
  - address
  - email address
- Tradesphere is the trade compliance system. Tradesphere receives name, address, and country information.
- Salesforce is the subscription billing system. Salesforce receives all the product details along with the customer billing and shipping information that is required for invoicing. In addition, customer quotes are quoted in Salesforce using the account, contact, and product details housed in Salesforce. Orders are billed and invoiced through Salesforce billing. Details of a new subscription, subscription amendment, and subscription renewal orders are passed to Security Management Platform for the purposes of provisioning tenant environments on Security Management Platform.

Email Handling by the Data Egress Service

To help protect recipients and maintain email deliverability, outbound email messages sent through the Data Egress Service are subject to automated email hygiene and security screening provided by the underlying email delivery platform. These controls include:

- Malware and virus scanning
- Detection and blocking of malicious URLs
- Spam and fraud detection
- Sender authentication validation (SPF and DKIM)

AI Services

The Platform includes AI Services that enable AI-powered experiences within supported Quest solutions. AI Services may be used to analyze customer-provided content, retrieve relevant knowledge, generate summaries, and support intelligent assistance scenarios. These services operate within the platform security boundaries and follow the same authentication, authorization, auditing, and data protection controls applicable to other platform services. AI Services are consumed only by platform features that explicitly require AI-powered functionality and are not required for general operation of the platform.

Data Handled by Common Storage Services

Customer search configurations for both shared and private searches. This includes any user entered data that are used to parameterize the search.

Customer alerting configurations for both shared and private alert rules. This includes the email address of the receipts of alert emails.

- Activity data and object data collected from any configured tenants and on-premises environments originating from Security Management Platform products using Common Storage Services. For further details on data handled and stored, see the Identity Defense Security Guides.

Location of Customer Data

When a customer signs up for Security Management Platform, they select the region in which to run their Security Management Platform organization. All computation is performed in, and all data is stored in the selected region. The currently supported regions can be found https://regions.quest-on-demand.com/.

Security Management Platform customer data is stored in the selected Security Management Platform region, entirely within Azure Services provided by Microsoft. For more information, see Achieving Compliant Data Residency and Security with Azure.

For US Organizations:

- All Security Management Platform data is stored and processed within the United States, using a single Azure Datacenter. Azure “West US 2” is used for all processed data within Security Management Platform. For disaster recovery duplicate copies of all data are stored in Azure “East US 2” and Azure “Central US”.

For Europe Organizations:

- All Security Management Platform data is stored and processed within the European Union, using a single Azure Datacenter. Azure “Northern Europe” is used for all processed data within Security Management Platform. For disaster recovery duplicate copies of all data are stored in Azure “Western Europe”.

For UK Organizations:

- All Security Management Platform data is stored and processed within the UK, using a single Azure Datacenter. Azure “UK South” is used for all processed data within Security Management Platform. For disaster recovery duplicate copies of all data are stored in Azure “UK West”.

For Canada Organizations:

- All Security Management Platform data is stored and processed within Canada, using a single Azure Datacenter. Azure “Canada Central” is used for all processed data within Security Management Platform. For disaster recovery duplicate copies of all data are stored in Azure “Canada East”.

For Australia Organizations:

- All Security Management Platform data is stored and processed within Australia, using a single Azure Datacenter. Azure “Australia East” is used for all processed data within Security Management Platform. For disaster recovery duplicate copies of all data are stored in Azure “Australia Southeast”.

Azure

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 is replicated across different fault domains to increase availability. All replication datacenters reside within the geographic boundaries of the selected region.

See this Microsoft reference for more details: https://docs.microsoft.com/en-us/azure/storage/storage-redundancy.

Subscription Services

Subscription services are provided to Security Management Platform through a combination of internal software and our partners Cybersource, Tradesphere, and Salesforce, all of which are in the US.

Privacy and Protection of Customer Data

Customer data is differentiated using a unique organization identifier. This organization identifier is generated securely during customer sign-up. This organization identifier is passed to the user interface via a tamper proof (signed) token (JSON Web Token). This is passed with all requests made and is used to provide the organization context for all back-end services. The signed token (JSON Web Token) has a 'Time to Live' of 10 minutes and must be refreshed and re-authorized at this time. Failure to do so results in access being lost to Security Management Platform Core.

Security Management Platform Core relies on MSAL (Microsoft Authentication Library) cache to silently refresh access tokens. This cache is encrypted at rest and accessible only by service account.

Quest Software employees and Microsoft employees do not have access to and cannot see the keys used for encryption and decryption. The process of encryption and decryption is transparent to Security Management Platform and takes place between the Azure Key Vault Service and Azure Storage Tables. The keys are stored in a Hardware Service Module within the Azure Key Vault which is FIPS-2 level validated by Microsoft Azure. These keys are rotated hourly. For more information, see: https://azure.microsoft.com/en-us/services/key-vault/.

Customer data passed within a notification to the Notification Service is stored but cannot be retrieved.

Separation of Customer Data

For Azure Data Explorer, each organization is contained within a separate database ensuring no mixture of data.

For Azure Storage, a combination of techniques is employed. In Azure Blob Storage the primary technique employed is to keep each organization in a separate container. For other Azure Storage services and when Azure Blob Storage data cannot be separated using containers, the architecture will employ careful use of the organization identifier to ensure data is kept separate.

For Azure Cosmos DB, the architecture will employ careful use of the organization identifier to ensure data is kept separate.

Network Communications

- All external communication is secured with HTTPS to the Security Management Platform User Interface.
- The external HTTPS certificate used on AWS S3 Content Delivery Network is a Level 2 domain certificate created and managed by Quest DevOps.
- There are no unsecured external HTTP calls within Security Management Platform.
- All internal network communication within Azure among Security Management Platform services and components is secured with HTTPS and is not visible to the external public internet.
- Integration with on-premises Change Auditor installations:

  All communication with on-premises Change Auditor uses secure TLS 1.2 connections over Web Sockets.

FIPS 140-2 Compliance

Security Management Platform Core cryptographic usage is based on Azure and AWS FIPS 140-2 compliant cryptographic functions.

- Security Management Platform Core leverages the Azure Key Vault and AWS KMS data-in-transit and data-at-rest built-in mechanisms.
- More information on Azure Key Vault is available at https://azure.microsoft.com/en-us/services/key-vault/
- More information on AWS KMS is available at https://aws.amazon.com/kms/
- More information on approved crypto functions is available at NIST FIPS 140-2 https://csrc.nist.gov/publications/detail/fips/140/2/final
- Azure Storage: https://docs.microsoft.com/en-us/azure/storage/common/storage-security-guide
- Azure Data Explorer: Enable infrastructure encryption: https://docs.microsoft.com/en-us/azure/data-explorer/double-encryption
- Enable infrastructure encryption for double encryption of data: https://docs.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable

SDLC and SDL

The Security Management Platform team follows a strict Quality Assurance cycle.

- Access to source control and build systems is protected by domain security, meaning that only employees on the Quest corporate network have access to these systems. Therefore, should a Security Management Platform developer leave the company, this individual can no longer access Security Management Platform systems.
- All code is versioned in source control.
- All product code is reviewed by another developer before check in.

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

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

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

Third party Assessments and Certifications

Penetration testing

Security Management Platform 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

Security Management Platform is included in the scope of the Platform Management ISO/IEC 27001, 27701, 27017 and 27018 certification:

ISO/IEC 27001:2022 Information technology — Security techniques — Information security management systems — Requirements: **Certificate Number: 1156977-8**, valid until **2028-07-27**.

ISO/IEC 27701:2019 Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance: **Certificate Number: 1156977-8,** valid until **2028-07-27.**

ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services: **Certificate Number: 1156977-8**, valid until **2028-07-27.**

ISO/IEC 27018:2019 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors: **Certificate Number: 1156977-8,** valid until **2028-07-27**.

Quest Software, Inc. has successfully completed a SOC 2 examination of its Security Management Platform 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: **August 1, 2024, to July 31, 2025**

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

Operational Security

Access to Data

Access to Security Management Platform Core data is restricted to Quest Operations team members. Security Management Platform developers have no access to customer production data.

Permissions Required to Configure and Operate Security Management Platform

Quest Operations team members have access to Quest's production Azure Subscription and monitor this as part of normal day to day operations. Security Management Platform developers have no access to Quest's production Azure Subscription.

Operational Monitoring

Security Management Platform internal logging is available to Quest Operations and Security Management Platform development teams during the normal operation of the platform. No customer or Personally Identifiable Information (PII) data is placed in internal logging and this is reviewed as part of the SDL process.

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. Security Management Platform relies on Azure and AWS infrastructure and as such, is subject to the possible disruption of these services.

- Quest Security Management Platform services status page is available at https://status.quest-on-demand.com/
- Azure services status page is available at https://azure.microsoft.com/en-ca/status/
- AWS services status page is available at https://status.aws.amazon.com/

Security Incident Response Management

For its Security Management Platform 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

Security Management Platform security features are only one part of a secure environment. Customers must implement their own security best practices.

About us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

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.