Quest® Quest On Demand Audit

Release Notes

Last Updated September 2021

These release notes provide information about the Quest On Demand Audit release.

About this module

On Demand Audit provides extensive auditing of critical activities and detailed reports about vital changes taking place in Microsoft Office 365 Exchange Online, SharePoint Online, and OneDrive for Business. Continually being in-the-know helps you to prove compliance, drive security, and improve up time while proactively auditing changes to configurations and permissions.

Integrating with Change Auditor, provides a single view of activity across hybrid Microsoft environments and turns on-premise events into rich visualizations to investigate incidents faster. Events sent to On Demand Audit include historical events gathered up to 30 days prior to upgrade to Change Auditor 7.0.0 (or higher).

On Demand Audit audits:

- When Exchange Online mailboxes are created, deleted, and accessed.

- Permission changes to see which users are granted access to a mailbox.

- Mailbox activity by non-owner such as messages sent, read, deleted, and folders deleted

- Mailbox activity by owner for sensitive and high value mailboxes.

- When files and folders are accessed, created, deleted, uploaded, moved, renamed, and checked in and out of SharePoint Online and OneDrive for Business sites.

- When user and group attributes are changed.

- When users and groups are added to and removed from the directory.

- Successful and failed logins.

- Suspicious sign-in activity.

- Teams user and administrator activity.

New features

New features in On Demand Audit:

- Anomaly detection added to the Critical Activity page to help identify unusual spikes in activity, that may indicate a threat to your organization. Including a visualization that details, baselines, anomalies, and total values for the following activity:

  - Unusual increase in AD account lockouts

  - Unusual increase in failed AD changes

  - Unusual increase in permission changes to AD objects

  - Unusual increase in tenant sign-in failures

  - Unusual increase in successful tenant sign-ins

  - Unusual increase in files shared from OneDrive and SharePoint

  - Unusual increase in Office 365 activity by guest users

  - Unusual increase in Office 365 activity by anonymous users

  - Unusual increase in Teams guest participants

- Anomaly Activity search category that includes the following built in searches:

  - Unusual increase in tenant sign-in failure events in the past 30 days

  - Unusual increase in AD account lockout events in the past 30 days

  - Unusual increase in successful tenant sign-in events in the past 30 days

  - Unusual increase in failed AD change events in the past 30 days

  - Unusual increase in permission changes to AD object events in the past 30 days

  - Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days

  - Unusual increase in Office 365 activity by guest user events in the past 30 days

  - Unusual increase in Office 365 activity by anonymous user events in the past 30

  - Unusual increase in Teams guest participant events in the past 30 days

  - All anomaly detected events in past 30 days

- Ability to audit Change Auditor installation setting changes (Change Auditor Installation is paused, Change Auditor Installation is resumed, Change Auditor Installation was removed).

- Additional search filter: Installation Name.

- Critical Activity page that displays a full list of security-related activity that may be a threat to your organization. This includes tailored visualizations and metrics to provide more context about the activity and related search and a high-level overview of the item.

- An alert plan cannot be removed until all alerts linked to it are removed or reassigned.

- Ability to audit Azure AD successful application consent events in the past 30 days.

- Updates dashboard that provides the following information:

  - Indicators that allow you to quickly see if there has been a change in risky activity over a specific period of time.

  - My Favorite Searches that displays your selected top 5 searches.

  - Critical Activity that highlights security-related activity that may pose a threat to your organization and require further investigation.

  - Top Active Users in the last 24 hours with each service represented by a different color bar.

  - On-premises and Azure Active Directory sign-in trends over the last 7 days.

- Ability to see at a glance all the alerts assigned to a particular alert plan.

- Ability to audit AD inheritance settings changed events in the past 30 days.

- Ability to audit irregular domain replication activity:

  - Irregular AD replication activity detected alert added to the critical activity tile on the dashboard.

  - AD Irregular domain replication detected events in the past 30 days built in search.

- Active Directory Federation Service enhancements:

  - AD FS All claims provider trust events in the past 30 days built-in search.

  - AD FS All endpoint events in the past 30 days built in search.

  - AD FS All relying party trust events in the past 30 days built in search.

  - AD FS All authentication method changes in the past 30 days

  - AD FS All server farm events in the past 30 days

  - AD FS Authentication method registered and unregistered events in the past 30 days

  - Active Directory Federation Services sign-ins built in searches.

  - Active Directory Federation Services search category for sign-ins and configuration changes made through Active Directory Federation Services.

- Additional search filters: RelyingPartyTrustName, RelyingPartyType, RelyingPartyResource, AuthenticationMethod, AuthenticationMethod, AccessControlPolicy, AutoUpdateFromFederationMetadata, BrowserAuthenticationURL, Enabled, Identifiers, MonitorFederationMetadata, Alert Rule Name, Alert Rule Type, Search Type, Alert Plan Name, Alert Plan Type, Creator, Category Name, Category Type, Search Name, Search Type, Url Path, Server Farm Name, Server Farm Node Name, Max Behavior Level, Server Farm Node Type.

- Additional On Demand Audit built in searches:
    - All On Demand Audit configuration events in the past 30 days
    - On Demand Audit alert plan management events in the past 30 days
    - On Demand Audit alert rule management events in the past 30 days
    - On Demand Audit all shared search and shared category events in the past 30 days
- Additional internal events are gathered:
    - Alert Plan Created
    - Alert Plan Renamed
    - Alert Rule Created
    - Alert Rule Enabled
    - Alert Rule Disabled
    - Backing Search for Alert Rule Renamed
    - Backing Search for Alert Rule Updated
    - Alert Plan Added to Alert Rule
    - Alert Plan Removed from Alert Rule
    - Search Created
    - Search Deleted
    - Search Renamed
    - Search Updated
    - Search Category Changed
    - Search Ran
    - Category Created
    - Category Deleted
    - Category Renamed
- Addition of an information icon that allows you to see when shared searches, alerts, and alert plans were created, last saved, and by whom.
- Ability to create private and shared categories for searches.
- Ability to create alerts for both private and shared searches.
- Ability to create both private and shared alert plans.
- Updated and new access roles for private and shared searches and alert plans.
- All Private Searches category.
- Updated workflow for saving searches. By default, the new search are created in the category selected when clicking New Search.

- MailItemsAccessed events gathered when the Exchange Online - Mailbox Activity service is configured for auditing. The event and its details (Operation Count and the Folder Item found under Source Folders) provide an auditing trail to help understand which emails may have been compromised during a security breach. Note: A Microsoft 365 E5 license is required to audit this activity.

- Ability to export search results to a csv or csv.zip file.

- Can Export Search Results permission for Audit Administrators and Audit Operators.

- Ability to audit Teams user and administrator activity such as when teams (and associated settings, members, and applications) are created, updated, removed and when users sign in.

- New Teams searches:

  - Teams app events in the past 7 days

  - Teams bot events in the past 7 days

  - Teams channel events in the past 7 days

  - Teams client configuration changes in the past 30 days

  - Teams connector events in the past 7 days

  - Teams events in the past 7 days

  - Teams guest access configuration changes in the past 30 days

  - Teams guest access enabled or disabled in the past 30 days

  - Teams guest members added in the past 7 days

  - Teams member role changes in the past 7 days

  - Teams member changes in the past 7 days

  - Teams notification and feeds policy changes in the past 30 days

  - Teams organization setting changes in the past 30 days

  - Teams tab events in the past 7 days

  - Teams targeting policy changes in the past 30 days

  - Teams team created events in the past 30 days

  - Teams team deleted events in the past 30 days

  - Teams team setting changes in the past 7 days

  - Teams user sign-in events in the past 7 days

- Additional search columns and filters available for Teams auditing: Add On GUID, Add on Name, Add on Type, Cmdlet Name, Team GUID, Team Name, Team Property Name, Team Role

- Australia, Canada, and UK regions available to host your On Demand Audit data.

- Additional search columns and filters available for logon activity: Logon Activity all excessive Kerberos ticket lifetime events in the past 30 days, Logon Activity all NTLM authentication failures in the past 24 hours, Logon Activity all NTLM authentications in the past 24 hours, Logon Activity all NTLM version 1 logons in the past 7 days.

- Additional logon activity searches;
    - Logon Activity all excessive Kerberos ticket lifetime events in the past 30 days
    - Logon Activity all NTLM authentication failures in the past 24 hours
    - Logon Activity all NTLM authentications in the past 24 hours
    - Logon Activity all NTLM version 1 logons in the past 7 days
- Ability to audit logon activity.
- Additional search columns and filters available for risk events: Activity Time, Detection Timing, Request Id, Risk Activity, Risk Detected Time, Risk State, Risk Type, Risk Correlation Id, Risk Detail, Risk Source, Token Issuer, Previous User Agent.
- Property After Value, Property Before Value, and Property Name available in the search details for Azure Active Directory, Active Directory, and Group Policy searches.
- Property After Value, Property Before Value, and Property Name filters available for Azure Active Directory, Active Directory, and Group Policy searches.
- Permission enforcement using additional Audit Operator role to help you manage your security and compliance auditing.

Release History

Current release

2021/9/14

Enhancements

Enhancement	ID
Anomaly detection to help identify unusual spikes in activity, that may indicate a threat to your organization. Including a visualization that details, baselines, anomalies, and total values for the following activity: - Unusual increase in AD account lockouts - Unusual increase in failed AD changes - Unusual increase in permission changes to AD objects - Unusual increase in tenant sign-in failures - Unusual increase in successful tenant sign-ins - Unusual increase in files shared from OneDrive and SharePoint - Unusual increase in Office 365 activity by guest users - Unusual increase in Office 365 activity by anonymous users - Unusual increase in Teams guest participants	261904

Enhancement	ID
Additional built in searches under the Anomaly Activity category: - Unusual increase in tenant sign-in failure events in the past 30 days - Unusual increase in AD account lockout events in the past 30 days - Unusual increase in successful tenant sign-in events in the past 30 days - Unusual increase in failed AD change events in the past 30 days - Unusual increase in permission changes to AD object events in the past 30 days - Unusual increase in files shared from OneDrive and SharePoint events in the past 30 days - Unusual increase in Office 365 activity by guest user events in the past 30 days - Unusual increase in Office 365 activity by anonymous user events in the past 30 - Unusual increase in Teams guest participant events in the past 30 days - All anomaly detected events in past 30 days	280820

Previous releases

2021/8/31

Enhancements

Enhancement	ID
Ability to audit Change Auditor installation setting changes (Change Auditor Installation is paused, Change Auditor Installation is resumed, Change Auditor Installation was removed). Additional search filter: - Installation Name	278719

2021/8/24

Enhancements

Enhancement	ID
An alert plan cannot be removed until all alerts linked to it are removed or reassigned.	241156

2021/8/10

Enhancements

Enhancement	ID
Full page critical activity pie chart flyout that display information by percentage of user,	257083

Enhancement	ID
target, or activity.	
Ability to hide, unhide and dismiss items in the critical activity page.	257084
Filtering support for critical activity item list.	264660
AD all inheritance settings changed events in the past 30 days built in report.	256843
Irregular AD replication activity detected alert added to the critical activity tile on the dashboard.	257279
AD Irregular domain replication detected events in the past 30 days built in search.	
Azure AD successful application consent events in the past 30 days built in report.	265009

2021/7/06

Enhancements

Enhancement	ID
Ability to see the alerts associated with each alert plan.	262139
Audit health tile in the dashboard that allows you to see the status of your auditing configuration, identify any issues, and make the required updates to ensure you are keeping informed of the vital and critical changes to your organization.	253362
Manage Organization Private Alerts and Private Alert Plans role that allows users to view and control all private alerts and private alert plans organization-wide.	260250

2021/6/15

Enhancements

Enhancement	ID
Ability to view the top active users in the last 24 hours in the dashboard.	246968
Active Directory irregular domain replication detected alert added to the critical activity tile on the dashboard.	257279
AD all irregular domain replication detected events in the past 30 days built in search.	
Active Directory Federation Services server farm event auditing: • AD FS All server farm events in the past 30 days search. • Active Directory Federation Services - Server Farm added as a pre-defined value under activity category • Server Farm Name, Server Farm Node Name, Max Behavior Level, Server Farm Node Type added as a search filter.	256578
Active Directory Federation Services endpoint event auditing: • AD FS All Endpoint events in the past 30 days search. • Active Directory Federation Services - Endpoints added as a pre-defined value under activity category. • Url Path added as a search filter.	238938
Active Directory Federation Services claims provider trust event auditing:	248748

Enhancement	ID

- AD FS All claims provider trust events in the past 30 days built-in search.
- Active Directory Federation Services - Claims Provider Trusts added as a pre-defined value under activity category.

Active Directory Federation Services sign-ins built-in searches:

- AD FS All Active Directory Federation Services sign-ins in the past 24 hours
- AD FS All Failed Active Directory Federation Services sign-ins in the past 7 days   235518
- AD FS All Successful Active Directory Federation Services sign-ins in the past 24 hours
- Additional Active Directory Federation Services search category.
- Additional search filters: RelyingPartyTrustName, RelyingPartyType, RelyingPartyResource, AuthenticationMethod, AccessControlPolicy, AutoUpdateFromFederationMetadata, BrowserAuthenticationURL, Enabled, Identifiers, and MonitorFederationMetadata.   235517 235522
- AD FS All relying party trust events in the past 30 days built in search.

Active Directory Federation Services Authentication method event auditing:

- AD FS All authentication method changes in the past 30 days search.
- AD FS Authentication method registered and unregistered events in the past 30 days search.   235521
- Activity Category = Active Directory Federation Services - Authentication Methods added as a search filter.

2021/6/01

Enhancements

Enhancement	ID
Dashboard indicators at that allow you to quickly see if there has been a change in risky activity over a specific period of time.	245512

2021/5/11

Enhancements

Enhancement	ID
All On Demand Audit configuration changes in the past 30 days built in search and Audit Configuration added as an available Activity Category value.	253358
Ability to view sign-in trends on the dashboard.	245863
Ability to view critical activity on the dashboard	247766
Ability to view favorite searches on the dashboard.	238722

2021/2/23

Enhancements

Enhancement	ID
Search and category management internal events, search filters, and built in search.	229658

2021/2/16

Enhancements

Enhancement	ID
Alert plan management internal events, search filters, and built in search.	226736
Alert rule management internal events, search filters, and built in search.	226733

2021/1/26

Enhancements

Enhancement	ID
Addition of an information icon that allows you to see when shared searches, alerts, and alert plans were created, last saved, and by whom.	234730

2021/1/5

Enhancements

Enhancement	ID
Ability to create private and shared categories for searches.	214658
Ability to create both private and shared searches.	214859
Ability to create alerts for both private and shared searches.	215122
Ability to create both private and shared alert plans.	214669
Updated and new access roles for private and shared searches and alert plans.	215128

2020/12/08

Enhancements

Enhancement	ID
All Private Searches category that lists all private searches.	214642
Ability to enable private alerts for searches.	215122

2020/10/20

Enhancements

Enhancement	ID
Updated workflow when saving searches. By default, new searches are created in the category selected when clicking New Search.	214640

2020/10/09

Enhancements

Enhancement	ID
Ability to export searches to a csv or csv.zip file	203805
Can Export Search Results permission available for Audit Administrators and Audit Operator roles.	198485

2020/10/05

Enhancements

Enhancement	ID
Ability to see MailItemsAccessed events when monitoring the Exchange Online - Mailbox Activity service is enabled. The event details includes Operation Count and the Folder Item (under Source Folders) information. Note: A Microsoft 365 E5 license is required to audit this activity.	213364

2020/07/21

Enhancements

Enhancement	ID
Ability to audit Teams user and administrator activity and access Teams built in searches.	206295

2020/06/23

Enhancements

Enhancement	ID
Australia, Canada, and UK regions available to host your On Demand Audit data.	199987

2020/06/02

Enhancements

Enhancement	ID
Additonal logon activity searches; • Logon Activity all excessive Kerberos ticket lifetime events in the past 30 days • Logon Activity all NTLM authentication failures in the past 24 hours • Logon Activity all NTLM authentications in the past 24 hours • Logon Activity all NTLM version 1 logons in the past 7 days	192548
Additional filters (and values) for logon activity searches: • Authentication Protocol (NTLM) • Authentication Protocol Version (V1, V2) • NTLM Impersonation Level (Default, Anonymous, Identify, Impersonate, Delegate) • NTLM Key Length • Kerberos Ticket Lifetime (Hours)	193574

Previous release

2020/05/12

Enhancements

Enhancement	ID
Additional search columns and filters available for risk events: • Activity Time • Detection Timing • Request Id • Risk Activity • Risk Detected Time • Risk State • Risk Type • Risk Correlation Id • Risk Detail • Risk Source • Token Issuer • Previous User Agent.	188576 188295
Logon activity searches;	193004

- Logon Activity all authentication activity in the past 7 days

- Logon Activity all failed logon activity in the past 7 days

- Logon Activity all interactive logon activity in the past 24 hours

- Logon Activity all Kerberos authentication activity in the past 24 hours

- Logon Activity all logon activity in the past 24 hours

- Logon Activity all logon session activity in the past 24 hours

- Logon Activity all remote logon activity in the past 24 hours

2020/04/21

Enhancements

Enhancement	ID
Azure Active Directory, Active Directory, and Group Policy search summary displays the Property After Value, Property Before Value, and Property Name.	186138 191584
Property After Value, Property Before Value, and Property Name filters added for Azure Active Directory, Active Directory, and Group Policy searches.	190047

2020/04/14

Enhancements

Enhancement	ID
Permission enforcement with additional Audit Operator role that allows users to manage searches and create alerts.	176138
Historical event collection is limited when using a trial license.	185662

2019/11/26

Enhancements

Enhancement	ID
Ability to assign multiple alert plans to searches providing increased flexibility on alert notifications within your organization.	173062

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. On Demand relies on Azure and AWS infrastructure and as such, is subject to the possible disruption of these services.You can view the following status pages:

- Quest On Demand: https://status.quest-on-demand.com/

- Azure Services: https://azure.microsoft.com/en-ca/status/

- AWS Services: https://status.aws.amazon.com/

System requirements

The following web browsers are supported with On Demand:

- Internet Explorer 11

- Microsoft Edge

- Google Chrome (latest version)

- Mozilla Firefox (latest version)

Product licensing

Quest On Demand is a Software as a Service (SaaS) application where application software is hosted in the cloud and made available to users through quest-on-demand.com.

Use of this software is governed by the Software Transaction Agreement found at www.quest.com/legal/sta.aspx and the SaaS Addendum at www.quest.com/legal/saas-addendum.aspx. This software does not require an activation or license key to operate.

You can sign in to Quest On Demand as a Guest user and sample the solutions the product can offer. As a Guest user, you can add your Azure AD tenant and look for problems that can be solved by Quest On Demand. To sign in as a Guest user, go to quest-on-demand.com and click **Continue as Guest**.

Trial licenses are available. To enable a trial license, you must use a Quest account to sign up for Quest On Demand. Use one of the following procedures:

- To enable a trial license with an existing Quest account

- To create a Quest account and enable a trial license

To enable a trial license with an existing Quest account

1. Go to https://www.quest.com/on-demand/

2. Scroll down to the module you are interested in and click **Try Online**.

3. On the Free Trial of <Module Name> page, click **Sign In for your Free Trial**.

4. Fill in your Quest account credentials and click **Sign In**. The Welcome to Quest On Demand page opens.

5. In the **Add organization name** field, enter a name for your Quest On Demand organization.

6. In the **Select Region** field, select the region where you want your data to reside.

7. Click **Create New Organization**.

You can now add your Azure AD tenant and begin using the module. See the Global Settings User Guide for more information on working with Quest On Demand.

To create a Quest account and enable a trial license

1. Go to https://www.quest.com/on-demand/

2. Scroll down to the module you are interested in and click **Try Online**.

3. To try online, you must create a Quest account and then sign up for Quest On Demand.

4. Create a Quest account.

    a. Click **Create a Trial Account**.

    b. Fill in the fields on the Create Account page. Note that the email and password entered here will be the credentials you use to sign in to Quest On Demand.

    c. Click **Create Account**.The "We've sent you an email" page opens.

5. Sign in to Quest On Demand.

    a. Go to your email account and open the email from support.quest.com. Click on the verification link. The Welcome to Quest On Demand page opens.

    b. In the **Add organization** name field, enter a name for your Quest On Demand organization.

    c. In the **Select Region** field, select the region where you want your data to reside.

    d. Click **Create New Organization**.

You can now add your Azure AD tenant and begin using the module. See the Global Settings User Guide for more information on working with Quest On Demand.

More resources

Additional information is available from the following:

- Online product documentation (enter On Demand Audit in the Product search field)
- Quest On Demand Audit community
- Product trials and subscriptions

Third-party contributions

This product contains the following third-party components. For third-party license information, go to https://www.quest.com/legal/license-agreements.aspx.

Table 1: List of Third-Party Contributions

Component On Demand Audit Third Party	License or Acknowledgement
Automapper 8.1.1	Use of this component is governed by the MIT 1.0 license. https://github.com/AutoMapper/AutoMapper/blob/master/LICENSE.txt
CefSharp Chromium 69.0.0	BSD 3-Clause License N/A Copyright © The CefSharp Authors. All rights reserved.
Copyright © 2018 Software Freedom Conservancy.Support 3.141.0	Use of this component is governed by the Apache 2.0 license.

Component	License or Acknowledgement
	Copyright © 2018 Software Freedom Conservancy
CsvHelper 12.1.2	Dual licensing under MS-PL and Apache 2.0 1.0
	Copyright © 2009-2019 Josh Close and Contributors
Fluent Assertion 5.7.0	Use of this component is governed by the Apache 2.0 license.
	Copyright Notice - Fluent Assertion 5.7.0
FluentValidation 8.4.0	Use of this component is governed by the Apache 2.0 license.
	Copyright Notice - FluentValidation 8.4.0 Apache
Mailosaur 5.0.14	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2019 Mailosaur Ltd (https://mailosaur.com)
	MICROSOFT SOFTWARE LICENSE TERMS - Microsoft Net Library UPDATED 1.0
	Copyright © Microsoft Corporation
Microsoft Azure Active Directory Graph Client Library 2.1.1	Note: To the extent Microsoft is a processor or sub-processor of personal data in connection with the software, Microsoft makes the commitments in the European Union General Data Protection Regulation Terms of the Online Services Terms to all customers effective May 25, 2018, at http://go.microsoft.com/?linkid=9840733.
Microsoft.ApplicationInsights 2.8.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.ApplicationInsights.Web 2.4.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.AspNetCore.WebUtilities 2.2.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Azure.ConfigurationManager 4.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Azure.Devices.Client 1.18.1	Use of this component is governed by the MIT 1.0 license. - Microsoft Azure IoT SDK 1.0
	Copyright (c) Microsoft Corporation
Microsoft.Azure.DocumentDB 2.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014 Microsoft Corporation
Microsoft.Azure.DocumentDB.Core 2.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014 Microsoft Corporation
Microsoft.Azure.EventGrid 2.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2015 Microsoft
Microsoft.Azure.KeyVault.Core 1.0.0	Use of this component is governed by the Apache 2.0 license.
	Copyright (c) Microsoft Corporation
Microsoft.Azure.KeyVault.Core 2.0.4	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Azure.Search 5.0.3	Use of this component is governed by the MIT 1.0 license.

Component	License or Acknowledgement
	Copyright (c) 2018 Microsoft
Microsoft.Azure.WebJobs.Extensions.DurableTask 1.8.3	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions.EventGrid 2.0.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Azure.WebJobs.Extensions.Http 3.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation. All rights reserved.
Microsoft.Extensions.Caching.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Caching.Memory 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.DependencyInjection 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.DependencyInjection.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Logging 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.Extensions.Logging.Abstractions 2.2.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.IdentityModel.Clients.ActiveDirectory 4.5.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.IdentityModel.Protocols.OpenIdConnect 5.5.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.NET.Sdk.Functions 1.0.29	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.PowerBI.Api 2.0.14	Use of this component is governed by the MIT 1.0 license. © Microsoft Corporation. All rights reserved.
Microsoft.PowerShell.3.ReferenceAssemblies 1.0.0	Use of this component is governed by the MIT 1.0 license. Copyright Microsoft Corporation. All rights reserved.
Microsoft.Rest.ClientRuntime 2.3.20	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Rest.ClientRuntime.Azure 3.3.6	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.WindowsAzure.ConfigurationManager 3.2.3	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation
Moq 4.12.0	New BSD N/A license

Component	License or Acknowledgement
	Copyright (c) 2007, Clarius Consulting, Manas Technology Solutions, InSTEDD
Newtonsoft.Json 11.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2007 James Newton-King
Newtonsoft.Json 9.0.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2007 James Newton-King
Polly 6.1.2	BSD - Polly 7.1license Copyright (c) 2015-2017, App vNext
Selenium.Support 3.141.0	Use of this component is governed by the Apache 2.0 license. Copyright © 2019 Software Freedom Conservancy
SeleniumExtras.WaitHelpers 3.11.0	Use of this component is governed by the Apache 2.0 license. Copyright 2018, Software Freedom Conservancy
Serilog 2.8.0	Use of this component is governed by the Apache 2.0 license. Copyright Serilog Contributors
Serilog.Extensions.Logging 1.4.0	Use of this component is governed by the Apache 2.0 license. https://github.com/serilog/serilog-extensions-logging/blob/dev/LICENSE
Serilog.Sinks.AzureTableStorage 4.0.0	Use of this component is governed by the Apache 2.0 license. http://www.apache.org/licenses/LICENSE-2.0 Apache
SpecFlow 2.4.1	Licence (New BSD License) 2.1 Copyright (c) 2009, TechTalk SpecFlow
System.CodeDom 4.5.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation and Contributors
System.IdentityModel.Tokens.Jwt 5.1.5	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation. All rights reserved
WindowsAzure.Storage 7.2.1	Use of this component is governed by the Apache 2.0 license. Copyright (c) 2013 Microsoft Corp
WindowsAzure.Storage 9.3.1	Use of this component is governed by the Apache 2.0 license. © Microsoft Corporation. All rights reserved.

On Demand Shell Third Party

Angular 4.3	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014-2017 Google, Inc. http://angular.io
angular2-hotkeys 2.0	Use of this component is governed by the MIT 1.0 license. MIT © Nick Richardson
angular2-materialize 9.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2015 InfomediaLtd.

Component	License or Acknowledgement
Application Insights for .NET Web Applications. 2.6	Use of this component is governed by the MIT 1.0 license. Copyright © Microsoft. All Rights Reserved.
AWS SDK for .NET 3.3.21	Use of this component is governed by the Apache 2.0 license Copyright Notice - AWS SDK for .NET 3.3.21
AWS SDK for JavaScript in Node.js 2.9.0 .	Use of this component is governed by the Apache 2.0 license Copyright 2012-2017 Amazon.com, Inc. or its affiliates. All Rights Reserved
chart.js 2.7	Use of this component is governed by the MIT 1.0 license Copyright (c) 2013-2015 Nick Downie
Common Library for Hyak Code Generator 1.2.2	Use of this component is governed by the Apache 2.0 license. Copyright © Microsoft Corporation.
core-js 2.5.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2014-2017 Denis Pushkarev.
dragula 3.7	Use of this component is governed by the MIT 1.0 license. Copyright © 2015-2016 Nicolas Bevacqua.
Hammer.js 2.0	Use of this component is governed by the MIT 1.0 license. Copyright (C) 2011-2017 by Jorik Tangelder (Eight Media).
Intl.js 1.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2013 Andy Earnshaw.
JQuery 2.0.0	Use of this component is governed by the MIT 1.0 license. Copyright JS Foundation and other contributors, https://js.foundation/.
jwt-decode 2.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) npm, Inc. and Contributors All rights reserved.
Materialize-css 0.98	Use of this component is governed by the MIT 1.0 license. Code copyright 2017 Materialize.
Microsoft Azure Common Library 2.2.1	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation.
Microsoft Azure Common Library Dependencies 1.0.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation.
Microsoft Azure DocumentDB Node.js SDK 1.21	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation.
Microsoft Azure Key Vault Core Library 1.0.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation.
Microsoft Azure Key Vault Extensions Library 1.0.4	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation.
Microsoft.Azure.KeyVault 2.3.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation

Component	License or Acknowledgement
Microsoft.Azure.KeyVault.WebKey 2.0.7	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.Azure.Services.AppAuthentication 1.0	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft NETCore Platforms 1.1	Use of this component is governed by the MIT 1.0 license. Copyright (c) .NET Foundation and Contributors
Microsoft.IdentityModel.Clients.ActiveDirectory 3.14.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft.PowerBI.Api 2.4	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation. All rights reserved.
Microsoft.Rest.ClientRuntime 2.3.8	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2018 Microsoft
Microsoft.Rest.ClientRuntime.Azure 3.3.7	Use of this component is governed by the MIT 1.0 license. Copyright (c) Microsoft Corporation
Microsoft Unity 4.0	Use of this component is governed by the Apache 2.0 license. Copyright (c) Microsoft Corporation.
Moment.js 2.18.x	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2016 Saeid Zebardast.
mousetrap 1.6	Use of this component is governed by the Apache 2.0 license. Copyright [2013] Craig Campbell
NCrontab 3.3	Use of this component is governed by the Apache 2.0 license. Copyright (c) 2008 Atif Aziz
Newtonsoft.Json 11.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2007 James Newton-King.
ng2-charts 1.6	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2015-2017 Dmitriy Shekhovtsov <valorkin@gmail.com> Copyright (c) 2015-2017 Valor Software
ng2-dragula 1.5	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2015-2016 Dmitriy Shekhovtsov <valorkin@gmail.com>. Copyright (c) 2015-2016 Valor Software. Copyright (c) 2015-2016 Nathan Walker <NathanWalker>.
ngrx/core 1.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2016 Brandon Roberts, Mike Ryan, Rob Wormald.
ngrx/effects 2.0.2	Use of this component is governed by the MIT 1.0 license. Copyright (c) 2016 Brandon Roberts, Mike Ryan, Rob Wormald.
ngrx/router-store 1.2.5	Use of this component is governed by the MIT 1.0 license.

Component	License or Acknowledgement
	Copyright (c) 2017 Brandon Roberts.
ngrx/store 2.2.3	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2015 ngrx.
ngrx-store-freeze 0.1	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2017 Brandon Roberts.
pg 7.4	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) npm, Inc. and Contributors All rights reserved.
psycopg2 2.7.3	Copyright © 1990-2017, Python Software Foundation GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999
rxjs 5.5	Use of this component is governed by the Apache 2.0 license.
	Copyright (c) Microsoft.
StackExchange.Redis 1.2.6	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2014 Stack Exchange
svgxuse 1.2	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) IcoMoon (icomoon.io)
swimlane/ngx-datatable 11.2	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2016 Swimlane <info@swimlane.com>
System Spatial 5.8	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2018 Microsoft. All rights reserved.
System.Diagnostics.DiagnosticSource 4.4.0	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) .NET Foundation and Contributors
systemjs 0.19	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) npm, Inc. and Contributors All rights reserved.
WindowsAzure.Storage 9.1	Use of this component is governed by the Apache 2.0 license.
	Copyright (c) 2013 Microsoft Corp
zone.js 0.8.x	Use of this component is governed by the MIT 1.0 license.
	Copyright (c) 2016 Google, Inc.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

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

Patents

Trademarks

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.

On Demand Audit Release Notes
Last Updated - May 2021