

# Quest<sup>®</sup> Security Guardian

## March 10, 2025

These release notes provide information about Quest<sup>®</sup> Security Guardian deployments.

Quest<sup>®</sup> Security Guardian is an integrated On Demand solution that helps you keep the Active Directory domain(s) and Entra ID tenant(s) in your organization secure.

You can:

- Identify Tier Zero objects in Active Directory.
- Identify Privileged objects in Entra ID.
- Certify that objects are indeed Tier Zero or Privileged and, when Quest Change Auditor version 7.4 is integrated, protect Active Directory Tier Zero objects against unauthorized or accidental modification or deletion.
- Run pre-defined Security Assessments to identify vulnerabilities in Active Directory and Entra ID and create your own Assessments.
- Investigate Findings for Tier Zero and Privileged objects, vulnerabilities identified through Assessments, and Critical Activity from On Demand Audit.
- Have Findings forwarded to a SIEM tool and alerts sent to selected email recipients.

[New Features](#)

[Resolved issues](#)

[Known issues](#)

[Release History](#)

[Incident response management](#)

[System requirements](#)

[Product licensing](#)

[Third-party contributions](#)

[About us](#)

[Technical support resources](#)

## New Features

The following Active Directory Assessments have been added to Discoveries:

- Credential Access:
  - Microsoft Entra seamless single sign-on (AzureADSSOACC) account password has not changed recently
- Persistence:
  - Tier Zero Group policy contains a scheduled task
  - Non-Tier Zero Group policy contains a scheduled task

## Resolved issues

The following is a list of issues addressed in this release.

### Tier Zero resolved issue

Resolved Issue	Issue ID
The issue "Tier Zero enumeration does not properly handle Domain Users group being member of a Tier Zero group" has been resolved.	542953

## Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

### Assessment known issues

Known Issue	Issue ID
Due to the complexity of the query, an Assessment can evaluate a maximum of 10,000 Tier Zero objects for a vulnerability. If this limit is surpassed, results will be marked as Inconclusive with the following message: <i>Syntax error: Query length (2162372) too large (max: 2097152)</i>	497529

## Release History

The following lists the new features, enhancements and resolved issues by deployment.

## Current Deployment

### March 10, 2025

#### New Features

The following Active Directory Assessments have been added to Discoveries:

- Credential Access:
  - Microsoft Entra seamless single sign-on (AzureADSSOACC) account password has not changed recently
- Persistence:
  - Tier Zero Group policy contains a scheduled task
  - Non-Tier Zero Group policy contains a scheduled task

### Resolved Issues

Resolved Issue	Issue ID
The issue "Tier Zero enumeration does not properly handle Domain Users group being member of a Tier Zero group" has been resolved.	542953

## Previous Deployments

### December 17, 2024

#### New Features

Security Guardian has added support for Entra ID objects in Microsoft 365 tenants, which includes Privileged object identification and certification. Security Assessments, and indicators for Findings in Security Guardian and On Demand Audit.

### December 10, 2024

#### New Features

The following Active Directory Assessments have been added to Discoveries:

- Credential Access
  - Group Policy does not enforce built-in Administrator account lockout
- Lateral Movement
  - Tier Zero Group Policy allows Authenticated Users to add computers to the domain
  - Non-Tier Zero account can request an overly permissive certificate with privileged EKU (ESC2)
- Privilege Escalation
  - Non-Tier Zero account can use a misconfigured certificate template to impersonate any user

### Resolved Issues

Resolved Issue	Issue ID
A performance improvement has been implemented for environments with a large volume of Tier Zero objects.	530317

## October 10, 2024

### New Features

The following Active Directory vulnerabilities have been added to Discoveries:

- Credential Access:
  - Domain trust without Kerberos AES encryption enabled
  - Kerberos KRBTGT account password has not changed recently
- Privilege Escalation:
  - Suspicious ESX Admins group detected in domain

### Enhancements

Enhancement	Issue ID
MITRE ATT&CK TTPs have been added to Hygiene and Detected Indicators Findings Investigation pages.	494070
The reason(s) why an object is considered Tier Zero is displayed in object details and the Findings Investigation page for the object.	479695
In Assessment results for vulnerable computer and user objects, a column has been added to indicate whether the object is enabled or disabled.	481991

## August 15, 2024

### Enhancements

Enhancement	Issue ID
To prevent system overload from exceptionally large data sets, a maximum of 100,000 objects will be displayed in the Assessment Results Vulnerable Objects list.	502873

## August 1, 2024

### New Features

You can export the complete Tier Zero objects list to a csv file, for sharing with stakeholder and security assessment engagements.

### Enhancements

Enhancement	Issue ID
To simplify the user experience, Am I Exposed? no longer displays on the Findings Investigation page.	465773

## July 02, 2024

## New Features

The terminology for Indicator and Finding types has changed to better align with industry standards.

## March 26, 2024

## New Features

A Data Collections page has been added to Security Settings, which allows you to monitor Active Directory data collections within your organization. You can also:

- manually run a data collection
- disable data collections that you no longer want to run.

# 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:

- Microsoft Edge
- Google Chrome (latest version)
- Mozilla Firefox (latest version)

# Additional component requirements

Component	Purpose
Hybrid Agent	Gives Security Guardian access to the Active Directory domain(s) that you want to keep secure.
Quest Change Auditor (via On Demand Audit)	Sends Active Directory events to On Demand Audit for reporting in Security Guardian Findings and allows you to protect Tier Zero objects.  <b>i</b> <b>NOTE:</b> A minimum of version 7.3 is required to send critical activity events to On Demand Audit, and a minimum of version 7.4 is required to protect Tier Zero objects.

Component	Purpose
SpecterOps BloodHound Enterprise (Optional)	Identifies Tier Zero assets in your organization's Active Directory domain(s), which you can monitor and assess for security vulnerabilities in Security Guardian.  <b>i</b> <b>NOTE:</b> If BloodHound Enterprise is not configured, Security Guardian will be used as your organization's Tier Zero provider once the Hybrid Agent is configured.
SIEM solution:  • Microsoft Sentinel  • Splunk Cloud or Enterprise  (Optional)	Allows Security Guardian Findings to be forwarded to a configured SIEM tool for further analysis.  <b>i</b> <b>NOTE:</b> Regardless of whether your organization uses a SIEM solution, you can also have Finding alerts sent via email.

## 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](https://quest-on-demand.com).

Use of this software is governed by the Software Transaction Agreement found at [www.quest.com/legal/sta.aspx](https://www.quest.com/legal/sta.aspx) and the SaaS Addendum at [www.quest.com/legal/saas-addendum.aspx](https://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](https://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.

## Third-party contributions

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



#### NOTES:

- For third-party contributions specific to On Demand Audit, refer to the [On Demand Audit Release Notes](#).
- For third-party contributions specific to On Demand Global Settings, refer to the [On Demand Global Settings Release Notes](#).

#### List of Third-Party Contributions

Component	License or Acknowledgement
Azure Core 1.44.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Identity 1.12.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Identity 1.13.0-beta.2	Use of this component is governed by the <a href="#">MIT</a>

Component	License or Acknowledgement
	<a href="#">Template 2020</a> license.
Azure.Identity 1.13.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Messaging.ServiceBus 7.18.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.ResourceManager.Kusto 1.5.1	Use of this component is governed by the <a href="#">MIT N/A</a> license.
Azure.Security.KeyVault.Secrets 4.6.0	Copyright © 2015 Microsoft
Azure.Storage.Blobs 12.22.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Storage.Blobs 12.23.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Storage.Blobs.Batch 12.19.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Storage.Common 12.21.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Azure.Storage.Queues 12.20.1	Use of this component is governed by the <a href="#">MIT 1.0</a> license.
coverlet.collector 6.0.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.Authentication.JwtBearer 8.0.10	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.Mvc.Testing 8.0.10	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.SignalR.Client.Core 8.0.10	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.SignalR.Client.Core 9.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.SignalR.Protocols.MessagePack 8.10.10	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.SignalR.Protocols.MessagePack 9.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.AspNetCore.SignalR.Protocols.MessagePack 9.0.0-rc.2.24474.3	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Azure.AppConfiguration.AspNetCore 8.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Azure.Cosmos 3.44.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Azure.Cosmos 3.45.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.



Component	License or Acknowledgement
Microsoft.Azure.Cosmos 3.45.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Azure.Kusto.Data 12.2.7	Use of this component is governed by the <a href="#">Microsoft Azure Data Explorer SDK N/A</a> license.
Microsoft.Azure.SignalR 1.28.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Data.SqlClient 5.2.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license. Copyright © NET Foundation. All rights reserved.
Microsoft.Extensions.Azure 1.7.6	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Configuration 7.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Configuration 8.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Configuration.AzureAppConfiguration 8.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.DependencyInjection 8.0.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.DependencyInjection.Abstractions 8.0.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Diagnostics.Testing 8.10.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Hosting 8.0.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Logging.Console 9.0.0-rc.2.24473.5	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Extensions.Options 8.0.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Identity.Client 4.65.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.Identity.Client 4.66.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license. Copyright © Microsoft Corporation
Microsoft.IdentityModel.Tokens 8.1.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Microsoft.IdentityModel.Tokens 6.32.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.

Component	License or Acknowledgement
Microsoft.Rest.ClientRuntime 2.3.24	Use of this component is governed by the <a href="#">MIT Template 2020</a> license. Copyright © Microsoft Corporation
Newtonsoft.Json 13.0.3	Use of this component is governed by the <a href="#">MIT Template 2020</a> license. Copyright © James Newton-King 2008
Polly 8.4.2	Use of this component is governed by the <a href="#">BSD 3-Clause Template 2020</a> license.
StackExchange.Redis 2.8.16	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Swashbuckle.AspNetCore 6.8.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
Swashbuckle.AspNetCore.Annotations 6.8.1	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.Drawing.Common 8.0.10	Use of this component is governed by the <a href="#">MIT Template 2020</a> license. Copyright © .NET Foundation and Contributors All rights reserved.
System.Drawing.Common 9.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.IdentityModel.Tokens.Jwt 8.1.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.IdentityModel.Tokens.Jwt 8.2	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.Text.Encodings.Web 8.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.Text.Json 8.0.5	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.Text.Json 9.0.0	Use of this component is governed by the <a href="#">MIT Template 2020</a> license.
System.Text.RegularExpressions 4.3.1	Use of this component is governed by the <a href="#">MIT N/A</a> license. Copyright © .NET Foundation. All rights reserved.

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit [www.quest.com](http://www.quest.com).

## 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

**© 2025 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

20 Enterprise, Suite 100

Aliso Viejo, CA 92656

Refer to our Web site (<https://www.quest.com>) for regional and international office information.



**Patents**

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

**Trademarks**

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

**Legend**

-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Security Guardian Release Notes  
Updated -March 10, 2025