Quest

Quest® Enterprise Reporter 3.5.1

What's New

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (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. Active Directory, Azure, Microsoft 365, Microsoft Teams, Microsoft 365, OneDrive, PowerShell, SharePoint, SQL Server, Teams, Windows, and Windows Server are trademarks and registered trademarks of the Microsoft Corporation and the Microsoft group of companies.

All other trademarks and registered trademarks 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.

Enterprise Reporter What's New
Updated - February 2024
Software Version - 3.5.1

Contents

What’s New in Enterprise Reporter 3.5.1

Enterprise Reporter provides a unified solution for data discovery and report generation. Using the Enterprise Reporter Configuration Manager, administrators can easily configure and deploy discoveries to collect and store data. Once the data has been collected, the Report Manager allows users to produce reports that help organizations to ensure that they comply with industry regulations and standards, adhere to internal security policies, monitor hardware and software requirements, and fulfill many other reporting requirements.

As a result of ongoing research and development efforts, and in response to customer feedback, the following changes and improvements have been made in this release of Quest Enterprise Reporter.

NOTE: Azure Active Directory is now Microsoft Entra ID.

Support for OAuth2 authentication for email delivery

If you need OAuth2 authentication for sending email, you can use Exchange Online to send email notifications or to email reports. To use Exchange Online accounts to send email, you must register an application for Enterprise Reporter with Azure Active Directory, using certificate-based authentication.

When you configure email settings for the Configuration Manager or the default email server for the Report Manager, you now have the option to select Exchange Online as the service type.

For more information, see the section titled “Configuring Email Notifications” in the *Configuration Manager User Guide* and the section titled “Configuring a Default Email Server” in the *Report Manager User Guide*.

Support for GCC and GCC High tenants for email notifications

When you are configuring email notifications for Exchange Online you can select between Azure Cloud (Default), US Government Cloud L, and US Government Cloud L5 (DoD) as the cloud instance.

Credential Manager improvements

The Credential Manager has added the following enhancements:

- Support for UPN format for user accounts.
- Ability to identify Azure accounts and authenticate through Microsoft.

Ability to collect and report on password protection settings

Users can create passwords that use common words and can be exposed by dictionary-based attacks. To enforce strong passwords, you can use Azure Active Directory Password Protection to enforce a global and custom banned password list. A password change request fails if there is a match in the banned password lists.

Enterprise Reporter now collects and reports the following Azure and on-premises password protection settings fields:

Table 1. Collected Password Protection settings fields

Field Name	Description
Lockout duration	Lockout duration in seconds after the threshold is reached for unsuccessful password attempts.
Lockout threshold	Lockout threshold for how many unsuccessful attempts to enter a password are allowed.
Custom banned password list enforced	Enforcing the custom banned passwords list is enabled.
Banned passwords	List of banned passwords.
On-premises password protection mode	Mode, such as audit or enforce, for checking on-premises banned passwords. For audit, event log messages are generated but passwords are changed. For enforce, a password change request fails if there is a match in the banned password list.
Enable on-premises password protection	Checking for on-premises banned passwords is enabled.

The password protection fields are collected by the Azure Active Directory discovery and are included in the Azure | Active Directory | Azure Tenant Information report. The fields are also visible in the list of available fields in Edit Report if you are creating a custom report.

Ability to collect Azure user activity information

You can select an option in the Scope page for Azure Active Directory discoveries to collect user activity information such as what licenses a user has assigned, when a license was assigned to a user, and the last activity dates for different license services.

New library reports

The following new library reports were added:

Active Directory | Health Check | Active Directory

- Accounts Where SID History Attribute Contains SID From Same Domain

Microsoft 365

- Microsoft 365 Active Users

Updates to libraries

- Upgraded Microsoft Graph for all cloud discoveries. Microsoft Graph version 5.7 is used.
- The Azure Active Directory PowerShell and MSOnline PowerShell modules have been deprecated by Microsoft. As a result, some Azure Active Directory collections have been migrated to use Microsoft Graph.
- Remote PowerShell (RPS) Protocol in Exchange Online PowerShell has been deprecated by Microsoft. Enterprise Reporter is now using ExchangeOnlineManagement 3.4 library.
- AzureRM PowerShell module has been deprecated by Microsoft and replaced with MSAL (Microsoft.Identity.Client v4.49.1).

AD discovery enhancements

Multiple improvement have been made for the Active Directory discovery including improved exception handling and retry logic for large collections.

Updated cryptographic algorithms

Enterprise Reporter Version 3.5.1 has updated and validated all cryptographic algorithms used within each component of the product. Enterprise Reporter 3.5.1 is using FIPS 140-2 validated algorithms and functions. For all encryption, the product uses AES-256 algorithms.

Additional support

- Support for LDAPS for Active Directory data discovery.
- Support for Pure Storage FlashBlade Purity//FB 4.3.0.
  - Support for NTFS discovery.
  - Partial support for File Storage Analysis discovery. (Collection of files, folders and shares supported. Collection of volumes and computer information not supported.)
- Enterprise Reporter can now collect information from computers running the following operating systems.
  - Windows Server 1909
  - Windows Server 2022
  - Windows 11
- Enterprise Reporter can now collect information from computers running the following SQL Server systems:
  - Microsoft SQL Server 2022

Other general enhancements

- File locks on remote share are released after NTFS discovery completes.
- The following new field is collected by the Azure Active Directory discovery and is available in the fields list when editing a report:

- Is Assignable To Role which indicates whether this group can be assigned to a role in Azure Active Directory.

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.

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.