

Quest® Enterprise Reporter 3.5.0

What's New



© 2022 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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

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

Refer to our 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, Office 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

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

Contents

What's New in Enterprise Reporter 3.5.0	5
SharePoint Online Discovery	5
Hotfixes Computer Discovery	5
Publishing Reports to SQL Server Reporting Services (SSRS)	5
Performance Enhancements	6
Active Directory Collector	6
New Reports	6
New Active Directory Reports	6
New Azure Active Directory Reports	8
New Computer Reports	8
New Office 365 Reports	9
New Security Explorer Remediation Reports	10
New Report Types	10
Updated Reports	12
Updated Azure Resource Reports	12
Updated Computer Reports	12
Updated Office 365 Reports	12
New Reporting Options	12
New Discovery Options and Changes	13
All Discoveries	13
Cloud Discoveries	13
Active Directory Discovery	13
Azure Active Directory Discovery	14
Computer Discovery	14
Exchange Online Discovery	14
Microsoft Teams Discovery	14
NTFS Discovery	15
Enhanced Data Collection	15
New Active Directory Discovery Attributes	15
New Azure Active Directory Discovery Attributes	15
New Computer Discovery Attributes	16
New Microsoft Teams Discovery Attributes	16
New SharePoint Discovery Attributes	16
Expanded Support for Windows Servers	16
Expanded Support for SQL Servers	17
Other General Enhancements	17
New required software	17

New SharePoint Online Application	17
Import a report to a category	17
Support setting security group location	17
New PowerShell cmdlets	17
Support moving nodes between discovery clusters	18
DevExpress upgrade	18
Option to deploy nodes using alternate credential	18
IT Security Search Integration	18
Support suppressing the login page	18
Improved extended attribute error messages	18
Export log feature enhancement	19
About us	20
Technical support resources	20

What's New in Enterprise Reporter

3.5.0

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.

SharePoint Online Discovery

As part of the Enterprise Reporter for Office 365 solution, Enterprise Reporter 3.5.0 now provides a new discovery type and new report library to support SharePoint Online Discovery and Reporting. With the SharePoint Administrator role, you can collect and report on SharePoint Online sites, site members, site owners, site groups, site permissions, configuration settings, and policies. Basic information from the tenant and sites is always collected.

For a list of SharePoint Online reports in the Enterprise Reporter library, see [New Office 365 Reports](#) on page 9.

Hotfixes Computer Discovery

You can monitor Windows patch compliance by choosing the **Hotfixes** option when defining a computer discovery. You can collect the following information on Windows update history for each computer:

- source of update information
- title of an update
- client application that processed an update
- operation performed on an update
- result of an operation on an update
- server that provided an update

Publishing Reports to SQL Server Reporting Services (SSRS)

You can configure Enterprise Reporter for publishing reports to SQL Server Reporting Services (SSRS). Reports can then be published allowing users to generate reports using a web browser instead of the Report Manager.

The ability to publish reports to Quest Knowledge Portal and the integration with Quest Knowledge Portal has been removed from the product. After upgrade to Enterprise Reporter 3.5, all reports will have to be published to SSRS, as previously published reports to Quest Knowledge Portal will no longer be available and cannot be updated.

Performance Enhancements

Active Directory Collector

When multiple domain controllers are specified for and Active Directory discovery, the workload is now spread among those domain controllers to improve performance.

Collection times have been greatly improved by changes made to how information is received once it is gathered during Active Directory discoveries.

New Reports

New Active Directory Reports

The following new Active Directory reports are added to the Report Library.

Table 1. New Active Directory Reports

Report name	Report description
Resultant Domain Kerberos Configuration	Shows the resultant Kerberos GPO configuration for selected domains. Includes a parameter to select the domains to be included in the report.

The following new Active Directory health check reports are added to the Report Library.

Report name	Report description
Health Check Active Directory	
Active Directory Permissions - Dangerous permissions delegated	Shows all Active Directory permissions for the selected domains and Active Directory objects. These permissions can be used to attack Active Directory. For information about attack types, see https://attack.mitre.org/mitigations/M1015/
Active Directory Permissions - Domain Controller Owners	Shows all Active Directory permissions for the selected domains and Active Directory objects. The Domain Administrators group or the Enterprise Administrators group are set as owners for domain controllers. For details, see Privileged Account Management at https://attack.mitre.org/mitigations/M1026/
Active Directory Permissions for Account (Everyone)	Shows the Active Directory permissions for an account, including permissions derived through group membership. (Excluding Deny Permissions and Change Password permissions).
AdminSDHolder Permissions	Shows all Active Directory permissions for the selected domains and Active Directory objects. For more information see Protected Accounts and Groups in Active Directory at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c-protected-accounts-and-groups-in-active-directory and Active Directory Configuration at https://attack.mitre.org/mitigations/M1015/

Report name	Report description
Domain Accounts (Users and Groups) with SID History Attribute not empty	Shows all the domain accounts for the selected domains which can leave accounts open to Access Token Manipulation: SID-History Injection attacks. Adversaries can use SID-History Injection to escalate privileges and bypass access controls. For details, see https://attack.mitre.org/techniques/T1134/005/
Domain Groups and Members (Pre-Windows 2000 Compatible Access)	Shows the group memberships for the selected domains and groups. If you include nested groups, the membership of the groups is displayed. For details, see https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/7a76a403-ed8d-4c39-adb7-a3255cab82c5?redirectedfrom=MSDN and Exploitation of Remote Services https://attack.mitre.org/techniques/T1210/
Health Check Computer	
Computer Services on Domain Controllers (Print Spooler)	Shows information about the services for the selected computers. (Enterprise Reporter Windows Server License must be available). More details at https://adsecurity.org/?p=4056
Domain Computers Having Constrained Delegation	Shows domain computers for selected domains that have constrained delegation.
Domain Computers Having SID History	Shows domain computers for selected domains that have some value specified in SID History attribute.
Domain Computers Having Unconstrained Delegation	Shows domain computers for selected domains having unconstrained delegation.
Domain Computers whose sAMAccountName Does Not End In a Dollar Sign	Shows domain computers for selected domains whose sAMAccountName does not end in a Dollar Sign.
Health Check Group	
Privileged Domain Groups and Members	Shows the group memberships for the selected domains and groups. These privileged groups should have as few members as possible. DNSAdmins should have no members. If you include nested groups, the membership of the groups is displayed. For details, see Privileged Account Management https://attack.mitre.org/mitigations/M1026/
SID History Auditing Group available in Domain (Migration in Progress)	Shows if a SID History auditing group has been created in the domain.
Health Check User	
Active Directory Permissions - Delegations for Accounts that cannot be resolved	Shows all active directory permissions for the selected domains and active directory objects. These permissions can be used for attacks. For details, see Active Directory Configuration https://attack.mitre.org/mitigations/M1015/
Built-in AD Administrator Account Usage	Shows native Administrator account in selected domains who have logged in selected timeframe.
Domain User Accounts that are Sensitive and Cannot be Delegated	Shows all domain user accounts for selected domains that cannot be delegated.
Domain Users who do not require a password	Shows all domain users for selected domains who do not require a password.
Domain Users who do not require Kerberos Pre-Authentication	Shows all domain users for selected domains where the account is configured with the "Do not require Kerberos pre-authentication" option. Kerberos pre-authentication is a security feature which offers protection against password-guessing attacks. When you do not enforce pre-authentication, a malicious attacker can directly send a dummy request for authentication.
Domain Users with weak DES encryption enabled	Shows all domain users for selected domains that have weak DES encryption enabled. DES is considered weak cryptography and is no longer enabled by default in Kerberos authentication.

Report name	Report description
Golden Ticket Mitigation - Last Password Change for krbtgt account	Shows user password information for the krbtgt account. Attackers who have the krbtgt account password hash can forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket. Golden tickets enable adversaries to generate authentication material for any account in Active Directory.
Privileged Accounts that are Sensitive and Cannot be Delegated	Shows all privileged accounts for selected domains that are configured with the "Account is sensitive and cannot be delegated" option.
Privileged Accounts that have Not Logged In	Shows privileged accounts in selected domains having unchanged passwords and have not logged in.
Privileged Accounts Vulnerable to the Kerberoast Attack	Shows all privileged user accounts that are vulnerable to the Kerberoast attack. Kerberoasting is an attack technique that attempts to crack the password of a service account within the Active Directory.
Privileged Accounts with Unchanged Passwords that Logged In	Shows privileged accounts in selected domains having unchanged passwords and have logged in.
User Account(s) that have Constrained Delegation	Shows all the domain users for the selected domains that have TRUSTED_FOR_AUTH_DELEGATION enabled. For details, see https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties
User Account(s) that have Unconstrained Delegation	Shows all the domain users for the selected domains that have TRUSTED_FOR_DELEGATION enabled. For details, see https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties

New Azure Active Directory Reports

The following new Azure Active Directory reports have been added to the Report Library.

Table 2. New Azure Active Directory Reports

Report name	Report description
Azure Active Directory Deleted Users	Shows deleted users for the selected tenants. Contains a parameter to select the tenants to be included in the report.
Azure Managers with Direct Reports	Shows all the direct reports for the selected managers. Contains parameters to select the tenants and Azure managers to be included in the report.

New Computer Reports

The following new Computer reports have been added to the Report Library.

Table 3. New Computer Reports

Report name	Report description
Scheduled Tasks	Shows the scheduled tasks for the selected computers. Contains parameters to select the domains, computers, and locations to be included in the report.
Server Features	Shows all the Windows Server Features for the selected computers.

New Office 365 Reports

The following new Office 365 reports have been added to the Report Library.

Table 4. New Office 365 Reports

Report name	Report description
Microsoft Dysfunctional Teams	Shows Microsoft Teams with No Owners or Less Than Two Members. Contains parameters to select the tenants and teams to be included in the report.
Microsoft Teams Application Permission Policies	Shows the Microsoft Teams Application Permission Policies for the selected tenants. Contains parameters to select the tenants and policies to be included in the report.
Microsoft Teams Calling Policies	Shows the Microsoft Teams Calling Policies for the selected tenants. Contains parameters to select the tenants and policies to be included in the report.
Microsoft Teams Meeting Policies	Shows the Microsoft Teams Meeting Policies for the selected tenants. Contains parameters to select the tenants and policies to be included in the report.
Microsoft Teams Messaging Policies	Shows the Microsoft Teams Messaging Policies for the selected tenants. Contains parameters to select the tenants and policies to be included in the report.
Microsoft Teams Organization Settings	Shows the Microsoft Teams Organization Settings for the selected tenants. Contains a parameter to select the tenant to be included in the report.
Microsoft Teams Tabs	Shows the Microsoft Teams tabs for the selected channels, teams, and tenants. Contains parameters to select tenants, teams, channels, and tabs to be included in the report.
Microsoft Teams Team and Channel Policies	Shows the Microsoft Teams Team and Channel Policies for the selected tenants. Contains parameters to select the tenants and policies to be included in the report.
Microsoft Teams User Policies	Shows some Microsoft Teams User Policies for the selected users. Contains parameters to select the tenants and users to be included in the report.
SharePoint Online Access Control Settings	Shows the access control settings for the selected tenants. Contains a parameter to select the tenants to be included in the report.
SharePoint Online Configuration Settings	Shows the configuration settings for the selected tenants. Contains a parameter to select the tenants to be included in the report.
SharePoint Online Office 365 Group Sites	Shows all Office 365 group sites for the selected SharePoint Online Tenants. Contains parameters to select the tenants and sites to be included in the report.
SharePoint Online Permissions for Identity	Shows the SharePoint Online permissions for the selected identity in the selected tenants and sites. Contains parameters to select the identity, tenants, sites, and roles to be included in the report.
SharePoint Online Sharing Policies	Shows the sharing policies for the selected tenants. Contains parameters to select the tenants to be included in the report.
SharePoint Online Site Administrators	Shows all site administrators for the selected SharePoint Online Tenants and sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Site Group Information with Members	Shows all site groups and their members for the selected SharePoint Online Tenants and sites. Contains parameters to select the tenants, site collections, sites, and site groups to be included in the report.

Table 4. New Office 365 Reports

Report name	Report description
SharePoint Online Site Sharing	Shows the sharing settings for the selected tenants and sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Site Permissions	Shows the site permissions for the selected tenants and sites. Contains parameters to select the tenants, site collections, sites, and roles to be included in the report.
SharePoint Online Sites without an Office 365 Group	Shows all sites without an Office 365 group for the selected tenants. The report will not include subsites for the sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Summary	Shows a summary of SharePoint Online for the selected Office 365 tenants. Contains a parameter to select the tenants to be included in the report.

New Security Explorer Remediation Reports

The following new Security Explorer Remediation reports have been added to the Report Library.

Table 5. New Security Explorer Remediation Reports

Report name	Report description
Group Managed Service Accounts and Members with Actions	Shows all the managed service accounts and their members for the selected domains. Contains parameters to select the domains, organizational units, and managed service accounts to be included in the report.
Managed Service Accounts and Members with Actions	Shows all the managed service accounts and their members for the selected domains. If you choose to include nested groups, membership of the group members is displayed. Contains parameters to select the domains, organizational units, and group managed accounts to be included in the report.

New Report Types

The following new report types have been added to the Report Library.

Table 6. New Report Types

Category	Report Type	Report Type description
Microsoft Teams	Teams Organization Settings	Provides information on Microsoft Teams organization-wide settings. Contains fields for Teams Client, External Access, Guest Calling, Guest Meeting, and Guest Messaging settings.
Microsoft Teams Policies	Teams App Permission Policies	Provides information on Microsoft Teams App Permission Policies. Contains fields for Teams Tenant and Teams App Permission Policies.
Microsoft Teams Policies	Teams Calling Policies	Provides information on Microsoft Teams Calling Policies. Contains fields for Teams Tenant and Teams Calling Policies.

Table 6. New Report Types

Category	Report Type	Report Type description
Microsoft Teams Policies	Teams Meeting Policies	Provides information on Microsoft Teams Meeting Policies. Contains fields for Teams Tenant and Teams Meeting Policies.
Microsoft Teams Policies	Teams Messaging Policies	Provides information on Microsoft Teams Messaging Policies. Contains fields for Teams Tenant and Teams Messaging Policies.
Microsoft Teams Policies	Teams Team and Channel Policies	Provides information on Microsoft Teams Team and Channel Policies. Contains fields for Teams Tenant and Teams Team and Channel Policies.
Microsoft Teams Policies	Teams User Policies	Provides information on Microsoft Teams User Policies. Contains fields for Teams Tenant, Teams User Identity, Teams Team and Channel Policies.
Microsoft Teams	Teams Tab	Provides information on Microsoft Teams Tab. Contains fields for Teams Tenant, Teams Identity, Teams Channel, and Teams Tab.
SharePoint Online	SharePoint Online Configuration Settings	Provides information on SharePoint Online configuration settings. Contains fields for SharePoint Online Tenant and SharePoint Online Configuration Setting.
SharePoint Online	SharePoint Online Site Groups	Provides information on SharePoint Online site groups. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, and SharePoint Online Group.
SharePoint Online	SharePoint Online Policies	Provides information on SharePoint Online Policies. Contains fields for SharePoint Online Tenant and SharePoint Online Policy.
SharePoint Online	SharePoint Online Settings and Policies.	Provides information on SharePoint Online Settings and Policies. Contains fields for SharePoint Online Tenant, SharePoint Online Configuration Settings, and SharePoint Online Tenant Policy.
SharePoint Online	SharePoint Online Site Group Members	Provides information on SharePoint Online site group members. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Site Group, and SharePoint Online Site Group Member.
SharePoint Online	SharePoint Online Site Permissions	Provides information on SharePoint Online site permissions. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Role Assignment Set, SharePoint Online Role Assignment, SharePoint Online Permission, and Azure Identity.
SharePoint Online	SharePoint Online Site Users and Azure Group Members	Contains fields for the site and its related Azure Groups as well as the member accounts. Contains fields for the site user information at includes if the user is site administrator or if the user is primary admin. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Site User, Azure Identity, Azure Group, and Azure Group member.
SharePoint Online	SharePoint Online Sites	Provides information on SharePoint Online sites. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, and SharePoint Online Site.

Updated Reports

Updated Azure Resource Reports

The following Azure Resource reports have been updated in the Report Library.

Table 7. New Azure Resource Reports

Category	Report name	Updates
Azure Virtual Network Resource	Azure Virtual Network Information	New field showing whether the virtual machine protection flag has changed or not.

Updated Computer Reports

The following Computer reports have been updated in the Report Library.

Table 8. New Computer Reports

Category	Report name	Updates
Computer	User Profile Information	New field showing the size of the profile folder.
Hotfixes	Hotfixes And Updates	The following new fields were added: <ul style="list-style-type: none">• Source: source of update information• Title: title of an update• Client Application: client application that processed an update• Operation: operation performed on an update• Operation result: result of an operation on an update• Server: server that provided an update

Updated Office 365 Reports

The following Office 365 reports have been updated in the Report Library.

Table 9. New Office 365 Reports

Category	Report name	Updates
Office 365	Office 365 Overview	Now includes SharePoint Online information.

New Reporting Options

New options have been added to improve the flexibility of the reporting features.

New Discovery Options and Changes

Several discoveries have new collection options to improve the ability to fine tune the information being collected.

All Discoveries

The following new options have been added to all discoveries.

Table 10. New Discovery Options

Option	Description
Save discovery errors	A Save button has been added to the discovery errors page allowing errors to be saved in a CSV or text file.

Cloud Discoveries

The following changes are made to cloud discoveries.

Table 11. Changes to Cloud Discoveries

Option	Description
Change to workflow for creating discoveries for cloud discoveries (Azure Active Directory, Azure Resource, Exchange Online, Microsoft Teams, OneDrive, and SharePoint Online).	Changed the workflow for creating cloud discoveries so you must configure the tenant app before specifying credentials. This change allows Enterprise Reporter to ensure that the credentials are authorized for the specified tenant, eliminating discovery failures due to credentials being used that are not authorized for the tenant.

After you upgrade to Enterprise Reporter 3.5, you must reconfigure the tenant app for the existing cloud discovery types with the exception of Exchange Online.

Active Directory Discovery

The following options have been added to Active Directory discoveries.

Table 12. New Active Directory Discovery Options

Option	Description
Select available domain controllers	Select multiple domain controllers to be used to enumerate the selected domain.

Azure Active Directory Discovery

The following options have been added to Azure Active Directory discoveries.

Table 13. New Azure Active Directory Discovery Options

Option	Description
--------	-------------

Computer Discovery

The following options have been added to Computer discoveries.

Table 14. New Computer Discovery Options

Option	Description
Tasks	Select this option to collect scheduled task information.

Exchange Online Discovery

The following options have been added to Exchange Online discoveries.

Table 15. New Exchange Online Discovery Options

Option	Description
Select available domain controller	Select a domain controller to be used to enumerate the selected domain.

Microsoft Teams Discovery

The following options have been added to Microsoft Teams discoveries.

Table 16. New Microsoft Teams Discovery Options

Option	Description
Policies and Settings	Optionally collect information about Microsoft Team and Channel policies.
Tabs	Optionally collect information about Microsoft Teams Tabs.

NTFS Discovery

The following options have been added to NTFS discoveries.

Table 17. New NTFS Discovery Options

Option	Description
Advanced global exclude filtering	Wildcards can now be used when specifying paths to exclude from collection.

Enhanced Data Collection

A number of discovery types have had new attributes added to them as part of the default collection. These attributes have been added in order to support commonly requested reports. In some cases, report types have been added. To create reports using these new attributes, you need to know the associated report type.

New Active Directory Discovery Attributes

The following data collection has been added to the Active Directory discovery.

Table 18. New Active Directory Discovery Attributes

Data Being Collected	Associated Report Type
Kerberos information	Domain
IsTrustedForDelegation	Users
IsTrustedToAuthenticateForDelegation	

New Azure Active Directory Discovery Attributes

The following data collection has been added to the Azure Active Directory discovery.

Table 19. New Azure Active Directory Discovery Attributes

Data Being Collected	Associated Report Type
Deleted Date and Time	Azure Users
Fax Number	Azure Users
Manager Information	Azure Users
Additional Microsoft Teams Channels Attributes	Teams Channels
Device information	Azure Devices Azure Device Members

New Computer Discovery Attributes

The following data collection has been added to the Computer discovery.

Table 20. New Computer Discovery Attributes

Data Being Collected	Associated Report Type
Task Information	Scheduled Tasks

New Microsoft Teams Discovery Attributes

The following data collection has been added to the Microsoft Teams discovery.

Table 21. New Microsoft Teams Discovery Attributes

Data Being Collected	Associated Report Type
Policy and setting information	Teams App Permission Policies
	Teams Calling Policies
	Teams Meeting Policies
	Teams Messaging Policies
	Teams Team and Channel Policies
	Teams User Policies
Teams organization information	Teams Organization Settings
Microsoft Teams Tab information	Teams Tab

New SharePoint Discovery Attributes

The following data collection has been added to the SharePoint discovery.

Table 22. New SharePoint Discovery Attributes

Data Being Collected	Associated Report Type
Site sharing information	SharePoint Online Sites

Expanded Support for Windows Servers

Enterprise Reporter can now collect information from computers running the following operating systems.

- Windows Server® 1909
- Windows Server® 2022
- Windows® 11

Expanded Support for SQL Servers

Enterprise Reporter can now collect information from computers running the following SQL Server systems:

- Microsoft SQL Server® 2022

Other General Enhancements

New required software

The following software is required for Enterprise Reporter 3.5.0.

- Microsoft® .NET Framework 4.8

New SharePoint Online Application

A new Quest Enterprise Reporter SharePoint Online Discovery application can now be configured for use with your Microsoft Azure Tenants in the Enterprise Reporter Tenant Application Manager.

Import a report to a category

The **Import-ERReport** PowerShell cmdlet can be used to import report definitions into a new or existing category within the report library.

Support setting security group location

During the installation of Enterprise Reporter, you can now specify where to create Enterprise Reporter security groups.

New PowerShell cmdlets

The following Enterprise Reporter tasks can now be performed using PowerShell cmdlets:

- database backup
- database clean
- database merge
- database restore
- database transfer
- publish report to SSRS

Support moving nodes between discovery clusters

When a node is selected, disabled, and stopped in the Configuration Manager, the new **Change Cluster** option can be used to move the node to a different cluster.

DevExpress upgrade

DevExpress has been upgraded to v19.2.5. All Enterprise Reporter library reports have been converted to use expression binding instead of standard data binding as part of this upgrade. Any report in the My Reports folder of the Report Manager will only be converted to use expression binding if the report is edited with the Report Manager.

i | **IMPORTANT:** It is recommended to back up My Reports before editing them with Report Manager as the automatic upgrade that occurs with editing is irreversible.

Option to deploy nodes using alternate credential

When installing a node on a new computer, there is now an option to **Specify an alternate credential for Node service deployment**. The account must have permissions to copy files in the Admin\$ share folder and to install and run services.

IT Security Search Integration

New Attribute Supported

Enterprise Reporter will now send the ComputerOwnerID object with the permission owner information sent to the IT Security Search Repository after every computer discovery.

Support suppressing the login page

When logging in to the Enterprise Reporter Configuration Manager or the Enterprise Reporter Report Manager, there is now an option to suppress the login page so that the same server and port is always used. This option can also be managed on the System Configuration page of each console.

Improved extended attribute error messages

When extending attributes, an error message is displayed for any attribute that cannot be collected. Use the error message to troubleshoot any issues with collecting the attribute before attempting to extend the attribute again.

Export log feature enhancement

You have complete visibility of the export log process. A download link is displayed on success/failure of export logs. A confirmation message is displayed if you try to cancel an export log operation.

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.