Quest® Enterprise Reporter 3.5.1

Release Notes

April 2024

These release notes provide information about the Quest® Enterprise Reporter release.

- About Quest Enterprise Reporter 3.5.1
- New features
- Enhancements
- Deprecated features
- Resolved issues
- Known issues
- System requirements
- Overview of Enterprise Reporter communications and required credentials
- Product licensing
- Getting started with Enterprise Reporter 3.5.1
- Globalization
- About Us

About Quest 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 discovery jobs to collect and store data. Once the data has been collected, the Report Manager allows users to produce reports that help organizations ensure they comply with industry regulations and standards, internal security policies, monitor hardware and software requirements, and many other reporting requirements.

Enterprise Reporter 3.5.1 is a maintenance release, with enhanced features and functionality. See New features and Resolved issues.

New features

New features in Enterprise Reporter 3.5.1:

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

NOTE: Due updates to libraries, after upgrade to Enterprise Reporter 3.5.1, you must reconfigure all tenant applications and authenticate all existing Azure credentials. See Upgrade and compatibility.

- 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. See Deprecated features.
- Remote PowerShell (RPS) Protocol in Exchange Online PowerShell has been deprecated by Microsoft. Enterprise Reporter is now using ExchangeOnlineManager 3.4 library.
- AzureRM PowerShell module has been deprecated by Microsoft and replace with MSAL (Microsoft.Identity.Client version 4.49.1).

AD discovery enhancements

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

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.)

See also:

- Enhancements
- Deprecated features
- Resolved issues
- Known issues

Enhancements

The following is a list of enhancements that are implemented in Enterprise Reporter 3.5.1.

Table 2. Customer requested enhancements

Enhancement	ID	Issue ID
Password protection settings are now collected by the Azure Active Directory discovery and are included in the Azure | Active Directory | Azure Tenant Information report. The fields include the following information • Lockout duration • Lockout threshold • Custom banned password list enforced • Banned passwords • On-premises password protection mode • Enable on-premises password protection The fields are also visible in the list of available fields in Edit Report if you are creating a custom report.	399284	
User activity information can be collected in Azure Active Directory discoveries. 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.	187947	

Table 2. Customer requested enhancements

Enhancement	ID	Issue ID
The following new field is collected by the Azure Active Directory discovery and is available in the fields list when editing a report: Field Name - Is Assignable To Role Field Description - Indicates whether this group can be assigned to a role in Azure Active Directory.	170099	
File locks on remote share are released after NTFS discovery completes.	383605	42074
Support for LDAPS for Active Directory data discovery.	393352	
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.)	462559	

Deprecated features

- 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 which has resulted in the following information no longer collected by Azure Active Directory discoveries:
  - MFARememberDevicesNotIssuedBefore -- Description: Any devices issued before this date do not require MFA
  - MFAProofupTime -- Description: Last MFA Enrollment Date
  - MFANotificationType -- Description: Phone app notification type
  - MFAPhoneAppVersion -- Description: Phone app version
  - MFAAuthenticationType -- Description: Types of phone authentication enabled (notification, OTP, etc.)

NOTE:
- The Azure Active Directory Users with Multi-Factor Authentication Information default report has been amended to exclude the MFADefautMethodType field.
- Ensure that you have also excluded these fields from your custom reports.

Resolved issues

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

Table 3. Resolved issues

Resolved issue	ID
AD Discovery: Group Managed Service Account Members that do not exist cause all members to be lost.	482236
AD Discovery - With the "Create multiple tasks for each domain" option selected, collection tasks may get locked and others tasks stuck waiting.	482104
AD Discovery - Remove Domain Controller information at the end of the discovery process.	482102
AD Discovery - Generating 'Domain Cache not Initialized' when cache is cleared.	482101
Licensing issues.	407740

Table 3. Resolved issues

Resolved issue	ID
Unable to run NTFS discovery on NetApp devices.	416025
Group memberships not reflecting deleted groups in Recursive Group Membership by Domain Account report.	416162
Unable to supply credentials in UPN format for non Azure accounts. Support added and now able to specify credentials in UPN format and select if account is an Azure credential.	438083
Active Directory discovery failing and generating a null reference error.	438355
Reports are only displaying the first service principal name when multiple service principal names are set in Active Directory.	438807
Active Directory discovery fails to generate multiple tasks for domain and discovery processing does not proceed.	438811
Database Utility dialog does not provide adequate information on the requirement of an empty database for the restore and transfer tasks.	439790
Reversible Encryption Password is not collected and does not appear in reports.	445224
Group Membership reports are missing group membership data.	447703
Database disk image is malformed.	453576
Azure credentials with different domain names from Tenant App domain name fail to create cloud discoveries.	455074
Parent/child domain group members are not expanded in the Domain Groups and Members report.	456143
When running LDAP queries, DirectoryOperationException is thrown and ending the discovery.	458288
Unable to save tokens to database due to date time incompatibility.	470127
Failed discovery scan for OneDrive, Azure Resource, and Team.	473662
Computer discovery runs showing “Object reference not set to an instance of an object” error.	474155
AD discovery for Active Roles extended attributes is not functioning properly.	474157

Known issues

The following is a list of issues known to exist at the time of release.

Table 4. Known issues

Known issue	ID
Some of the PDF cross references do not link to their destination pages.	380
Deprecated support for collection of OneDrive attribute 'TenantSyncClientRegistration". No longer available in the One Drive Configuration Settings library report.	235861
When using Multi-Factor Authentication, which uses delegated-only Azure application, there may be inconsistencies with the collection of the Exchange Online mailboxes.	236024
Using discovery credentials that are multi-factor authenticated, may result in some objects not being collected.	236031
To reduce the potential load on ARS Server, we are disabling 'Multiple Tasks' option on the AD scope when collecting ARS attributes.	475475
AD Discovery: If only a read-only domain controller is available for Active Directory discovery, collection will fail.	475471
AD Discovery - Unable to Connect to Database When Primary domain controller (PDC) is shutdown	475473
OneDrive discoveries: Groups are not being properly collected on edits of the group properties/permissions	4009

Table 4. Known issues

Known issue	ID
OneDrive discoveries: Returning unexpected results when "Contribute" permission is being assigned	4221
OneDrive discoveries: Custom Permissions are only returning the "name" of the custom permission and no results on actual set permission	4222
NTFS discoveries: NTFS duplicate files calculation may not be looking at whole computer, only share	7839
PowerShell intermittently returns OneDrive configuration settings incorrectly and updating these attributes is slow on native portal	9902
Azure Active Directory discoveries: Group member of itself not being handled properly	11022
Active Directory discoveries: “TTL” Group Member Property: Data may be overwritten and lost with multiple collections from multiple domains using the “Collect nested groups and members” option	18891
Exchange discoveries: Exchange exclusions should be followed in some cases	25018
Active Directory and Exchange discoveries: Duplicate contacts and distribution groups	25023
NAS Configuration UI Option on NTFS and File Storage Analysis Scopes pages causes confusion	27809
Computer discoveries: Windows service(s) are collecting as a failure on discovery when they are access denied.	27907
Exchange discoveries: Error on Exchange 2007 after collecting mailboxes with subfolders and permissions	76507
Exchange Online discoveries: cannot collect mailbox folders permissions with "/" in name	108051
Exchange Online discoveries: cannot collect permissions for some mailbox folders	108052
Computer discovery: Find Computers dialog: incorrect domain hierarchy after select child domain in Available Scopes	125087
Azure discoveries: Azure Licensed User with Service Plans may report incorrect service plans for users if service plan has not be provisioned	128479
Computer discoveries: With some computer discoveries using a shared data location, objects that have been deleted may not be correctly tombstoned in the database	128660
NTFS discovery taking excessive time to complete when metadata selected and encryption enabled on files and folders	170551

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

Table 5. Installation known issues

Known issue	ID	Issue ID
Installing the Enterprise Reporter Server using the Change functionality of the installer fails when UAC is enabled	371	215300
WORKAROUND: Disable UAC before using the Change function to install the server		
Crash upon launch of Configuration Manager console post upgrade installation	423	
Database Wizard does not auto-start after installing Enterprise Reporter on PC with enabled UAC	124827	

Table 6. Configuration Manager known issues

Known issue	ID	Issue ID
If an ACL references an ACE that is unresolved, that ACE remains unresolved even if the underlying issue is fixed	366	179774
For SQL Server 2000, users who have permissions assigned to database objects will not show properly in the Database Object Permissions report. These permissions are not currently being collected.	367	180536
Registry permissions for a 64-bit key are not being collected when using a 32-bit node	368	180545
A refresh issue sometimes causes a node that was manually removed to remain in the Configuration Manager WORKAROUND: Close the Configuration Manager, and open it again	370	203553
Alternate credentials for a discovery will be ignored if the discovery target is the same machine as the node processing the discovery task. The service account for the node is used to perform the discovery.	376	316195
The dollar sign ($) used for hidden shares does not look correct in Trebuchet font	379	347709
NTFS discovery errors on DFSROOT folders that are actually on the machine but collector says they cannot be found	396	384183
SQL Discovery does not enumerate the SQL Server located on the same system as Enterprise Reporter	397	384273
SQL Discovery does not support SQL Server cluster as a target	413	399407
Microsoft 365 distribution group account type may be updated incorrectly in the database when changing discovery options and collecting mailbox delegates with permissions	444	622477
Exchange throttling warning can occur during large Exchange collections: “The server cannot service this request right now. Try again later.” Create and run smaller discoveries or update Exchange throttling policy. For more information, see Knowledge Base article SOL205286.	446	624722
Multiple errors when using multiple nodes and running ARS collection with AD if nodes do not have prerequisites	449	626447
Special characters in collected data can cause a sorting issue in the SQL Lite database. Data may appear to be deleted when it is not.	2123	212195
When running the ER consoles in 4K resolution, they do not scale properly; 1920x1080 or lower works better. Solution article for DPI settings is available.	164903	

Table 7. Report Manager known issues

Known issue	ID	Issue ID
Potential Security Risk Enterprise Reporter sets the PowerShell script execution policy to Unrestricted. This policy is required to allow non-signed scripts to run with reports. The execution policy can be reset if required for security. If set to RemoteSigned or Restricted, some reports will not run.	478387	
If you have made changes to parameter values when scheduling a report, you must click Save to preserve your changes. If you navigate away from the parameters, your changes are lost. If you make a change in parameters, you are not warned that you will lose your changes if you do not click Save.	369	180547
Account credentials for a schedule report share will be ignored if the share is on same machine as the Enterprise Reporter server. The service account for the Server is used to access the share and deliver the reports.	376	316195

Table 7. Report Manager known issues

Known issue	ID	Issue ID
Unicode characters are not displayed correctly when exported (out of box reports) WORKAROUND: Update report layout to font that supports your character	381	358358
Issues may occur when using two Report Manager consoles on the same machine	403	388313
Custom query reports can allow security breach if SQL Server/database is not properly permissioned	438	613837
NullReferenceException occurs in all reports if they were created with parameters named with reserved words	2124	501242
Boolean parameters are shown incorrectly in the Excel files of reports that are created with the auto-layout wizard	2125	588670
Security Explorer cannot take action against 32 registry key from 64 bit machine	10570	
Scheduled reports write to local share using Enterprise Reporter service account instead of account associated with the schedule	11028	
Report layout retains parameters that have been deleted and/or renamed	85849	
Exporting Summary reports to CSV will not work for sub reports or graphs	120306	
The value displayed in the *time last collected* in Custom Query reports is being reported in GMT and not local time	122626	
NTFS: Cannot collect Shares with Cyrillic names in Shares	122634	
When running the ER consoles in 4K resolution, they do not scale properly; 1920x1080 or lower works better. Solution article for DPI settings is available.	164903	

Table 8. SSRS known issues

Known issue	ID	Issue ID
Special characters not handled correctly in SSRS published reports - query fails to run in RDL	372	223723
The option to display nested groups and their members in reports is not supported in SSRS	373	224951
Scripts are not supported in SSRS reports	374	224953
When a report is published to SSRS, charts are not published and sometimes a blank space will appear in the SSRS report	409	398868
Links in reports are not supported in SSRS. Reports that include links to other reports include File Storage Analysis reports and Remediation Reports.	411	398872
Custom report column headers do not appear on first page in a tabular report when exported to SSRS	426	490510
Some Enterprise Reporter Exchange library reports publish with errors due to fields that cannot be converted. Exchange Server Details report is not supported for publishing.	431	509490
Azure and Microsoft 365 reports do not publish correctly to SSRS - errors related to Raw Azure ID and unsupported data types	10819	
Advanced calculated field used in reports not supported in SSRS - reports not published	10889	
Custom images do not export from Report Manager reports to SSRS	18362	4156245
Parameters used in report layout as binded values are not supported when a report is exported to SSRS.	18363	4156245

Table 8. SSRS known issues

Known issue	ID	Issue ID
Operator *EqualswithGroupExpansion* is not supported in SSRS. An error will occur when report is published.	85754	
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.	ADO - 265787	

System requirements

Before installing Enterprise Reporter, ensure that your system meets the following minimum hardware and software requirements.

Topics

- Hardware requirements
- New required hardware
- Supported operating systems
- Active Roles supported versions
- IT Security Search supported versions
- Supported Internet protocols
- SQL Server supported versions
- Required software
- Required services

Hardware requirements

Enterprise Reporter Server

For the Enterprise Reporter Server, we recommend the following minimum hardware.

Table 9. Enterprise Reporter Server Hardware Requirements

Component	Recommended specifications
Memory	• Minimum: 8 GB RAM • Recommended: 16 GB RAM
Processor	• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores) • 64-bit processor
Hard disk space	• 10 GB • The file share used for the optional Shared Data Location requires space for storage of collected data. Space requirements vary with the amount of data collected.

Configuration Manager and Report Manager

For the Configuration Manager and Report Manager, we recommend the following minimum hardware.

Table 10. Configuration Manager and Report Manager Hardware Requirements

Component	Recommended specifications
Memory	• Minimum: 16 GB RAM • Recommended: 16 GB RAM
Processor	• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores) • 64-bit processor
Hard disk space	• Configuration Manager: 2 GB • Report Manager: 20 GB

Enterprise Reporter nodes

For the Enterprise Reporter nodes, we recommend the following minimum hardware. For detailed recommendations for node requirements, see

Table 11. Node Hardware Requirements

Component	Recommended specifications
Memory	• Minimum: 16 GB RAM • Recommended: 16 GB RAM
Processor	• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores - 4 recommended) • 64-bit processor
Hard disk space	• 10 GB for installed files plus 10-100 GB extra space for processing collections

Enterprise Reporter SQL Server

For the Enterprise Reporter SQL Server, we recommend the following minimum hardware.

Table 12. SQL Server Hardware Requirements

Component	Recommended specifications
Memory	• Minimum: 16 GB RAM • Recommended: 24 GB RAM
Processor	• Intel® or AMD 2 GHz multiprocessor (with at least 4cores) • 64-bit processor
Hard disk space	• 100 GB or more for larger environments

NOTE: SQL Server performance is needed to support inserting data into the database tables and to support querying that data for reporting purposes. To improve the performance of data collection or reporting, consider enhancing the SQL Server memory and processor.

Database size estimator

The Enterprise Reporter database is the storage location of all data collected for reporting. As such, the amount of hard disk space required is directly related to the amount of data being collected. The Database Size Estimator tool shipped with Enterprise Reporter can help determine how much space will be required.

Larger environments

Larger environments may have additional requirements for memory, processor, and hard disk space. There are many factors that can affect these requirements.

- The type of collections being performed.

  Some discoveries collect many object types and attributes that require multitudes of inserts into multiple database tables; therefore, they require a more robust SQL Server. Other discoveries collect just a few object types that require minimal inserts into a few database tables; therefore, they require a less robust SQL server.

  For example, A computer discovery collecting 10,000 computers will be inserting into 20+ database tables. An NTFS discovery collecting 10,000 files and folders will only be inserting into 3 database tables. The inserts are more expensive and the computer discovery will require more SQL server resources.

- The size of collections being performed.

  The size of the database directly relates to the amount of data being collected and being queried from the SQL Server. In other words, the size of the database directly relates to the number of rows in the database. Each discovery type stores different amounts of data. Use the Database Estimator tool for further information based on the types of collections being performed.

- The location of the SQL Server in relation to the collection targets.

  The power of your SQL Server combined with the performance of your network will dictate how fast data can be sent and retrieved from the database. The further away the SQL server is from collection targets and the slower the network speeds, the more a robust SQL Server will help improve performance.

New required hardware

The following hardware is required for Enterprise Reporter 3.2 and higher.

- Intel® or AMD 2 GHz multiprocessor (with at least 2 cores)

Supported operating systems

The following operating systems are supported for Enterprise Reporter components.

NOTE: It is not recommended that the server or console be installed on a domain controller.

Table 13. Supported Operating Systems

Operating Systems	Enterprise Reporter		
	ER Server	Consoles	Nodes
Windows Server® 2022	X	X	X
Windows Server® 20H2	X		X
Windows Server® 2004	X		X
Windows Server® 1909	X		X
Windows Server® 1903	X		X
Windows Server® 2019	X	X	X

Table 13. Supported Operating Systems

Operating Systems	ER Server (Enterprise Reporter)	Consoles (Enterprise Reporter)	Nodes (Enterprise Reporter)
Windows Server® 1809	X		X
Windows Server® 2016	X	X	X
Windows Server® 1803	X		X
Windows® 11		X	
Windows® 10		X	

The following operating systems are supported for Enterprise Reporter discovery targets.

Table 14. Supported Operating Systems for Discovery Targets

Supported Operating Systems for Discovery Targets	Active Directory Licences	Windows Server Licences	File Storage Analysis Licences	SQL Server Licences	Exchange Licences
Domain Functional Levels					
Windows Server® 2016 Functional Level	X				
Windows Server® 2012 R2 Functional Level	X				
Windows Server® 2012 Functional Level	X				
Computers					
Windows Server® 2022		X	X		
Windows Server® 20H2		X	X		
Windows Server® 2004		X	X		
Windows Server® 1909		X	X		
Windows Server® 1903		X	X		
Windows Server® 2019 and 1809		X	X		
Windows Server® 2016 and 1803		X	X		
Windows Server® 2012, 2012 R2, and 2012 Core		X	X		
Windows® 11		X	X		
Windows® 10		X	X		
Windows® 8.1		X	X		
Network Attached Storage (NAS) Devices					
Dell Fluid File System 6.0		X	X		
Dell Fuild File System 5.0		X	X		
NetApp® 9.4		X	X		

Supported Operating Systems for Discovery Targets	Active Directory Licences	Windows Server Licences	File Storage Analysis Licences	SQL Server Licences	Exchange Licences
NetApp® 9.3		X	X		
NetApp® Filer - Data ONTAP® 8..x - 9.x and above (Cluster mode is supported as of version 8.2)		X	X		
EMC Isilon OneFS (Collections require a secure connection to Isilon with a valid certificate.)		X	X		
EMC® VNX 7.1.47.5 X (Supported by collecting as a Windows Server)		X	X		
EMC® VNX 7.0.35.3 X (Supported by collecting as a Windows Server)		X	X		
Pure Storage FlashBlade Purity//FB 4.3.0 * Note: File Storage Analysis partially supported for Pure Storage Flashblade device. Collection of files, folders and shares is supported. Collection of volumes and computer information is not supported.		X	X*		
SQL Server Instances					
SQL Server® 2022				X	
SQL Server® 2019				X	
SQL Server® 2017				X	
SQL Server® Clusters				X	
SQL Server® 2016				X	
SQL Server® 2014				X	
SQL Server® 2012				X	
Exchange Servers					
Exchange® 2019					X
Exchange® 2016					X
Exchange® 2013					X

Active Roles supported versions

The following versions of Active Roles are supported as targets of Active Directory discoveries. See the Active Roles web site for the hardware and software requirements for your version of Active Roles.

- Active Roles 8.1
- Active Roles 8.0
- Active Roles 7.4.4
- Active Roles 7.3
- Active Roles 7.2.1
- Active Roles 7.1.2
- Active Roles 7.0.4

- Active Roles 7.0.2

IT Security Search supported versions

Enterprise Reporter can be configured to send discovery information to the following versions of IT Security Search. See the IT Security Search web site for the hardware and software requirements for your version of IT Security Search.

- IT Security Search 11.4.1
- IT Security Search 11.3

Supported Internet protocols

Enterprise Reporter can support IPv6 (Internet Protocol version 6) as well as IPv4.

SQL Server supported versions

The following versions of SQL Server® are supported for the Reporter database. See the Microsoft® web site for the hardware and software requirements for your version of SQL Server®:

- SQL Server® 2022
- SQL Server® 2019
- SQL Server® 2017
- SQL Server® 2016
- SQL Server® 2014
- SQL clusters and database mirroring are supported for your deployment, including
    - SQL Server® 2016 Always On
    - SQL Server® 2014 Always On

Using SQL Server certificates

SSL encryption of SQL Server connections using certificates

Enterprise Reporter can be configured to work with a SQL Server® instance. To secure communications while working with Enterprise Reporter, data sent over connections to the SQL Server can be encrypted using an SSL certificate.

The steps required to configure this encryption are as follows.

- Using the Microsoft Management Console (MMC):
    - Install the Certificates snap-in for the SQL Server host computer.
    - Import the certificate to the SQL Server host computer.
- Using SQL Server Configuration manager:
    - Configure the SQL Server to use the certificate.
    - Configure the SQL Server to force encryption.
- Restart the SQL Server host computer.

- Import the certificate to all Enterprise Reporter computers that will communicate with the SQL Server, such as the:
  - Enterprise Reporter server host computer
  - Enterprise Reporter nodes
  - Enterprise Reporter Configuration Manager host computer
  - Enterprise Reporter Report Manager host computer
- Install Enterprise Reporter on a host computer.

Required software

The following software is required for Enterprise Reporter.

- Microsoft.NET Framework 4.8
- Microsoft Excel 2010, 2013, 2016, or 2019 (required to view reports exported as spreadsheets)
- Microsoft 365 Excel
- PowerShell 3.0

Active Roles required software

To collect Active Roles information, the following software is required on the computer where the Enterprise Reporter Configuration Manager is installed and on the computer where the Enterprise Reporter node is installed:

- ADSI Provider (the version must match the Active Roles version)

For more information and installation instructions, see the Active Roles Quick Start Guide.

The following additional considerations are required:

- There must be a trust between the Enterprise Reporter domain and the Active Roles domain.
- The credentials used for the Active Roles discovery must have access to the Active Roles domain.

Exchange required software

To collect Exchange information, the following additional considerations are required:

- Ensure the Windows Remote Management (WinRM) service is running.

To collect Exchange mailbox folders, the following additional considerations are required:

- Impersonation needs to be configured on the Exchange organization. Refer to your Exchange Server documentation or use the following method to set up role assignments.
  - PowerShell can be used to add an assignment

    New-ManagementRoleAssignment –Name:impersonationAssignmentAdministrator –Role:ApplicationImpersonation –User:Administrator
  - Alternatively, you can create an administrator role with ApplicationImpersonation role assigned to it and add the required account as a member (or assign ApplicationImpersonation role to an existing administrator role)

Exchange Online required software

To collect Exchange Online information, the following additional considerations are required:

- Ensure the Windows Remote Management (WinRM) service is running.

Multi-Factor Authentication Cloud Discovery Credential Limitations

Cloud discoveries (Azure Active Directory, Azure Resources, Exchange Online, Teams, and SharePoint Online) support both MFA (Multi-Factor Authentication) enabled and disabled credentials. However, using Multi-Factor Authentication enabled credentials on cloud discoveries can result in an incomplete collection that omits one or more of the following objects and attributes.See the following table for details.

Table 15. Cloud discoveries that may be excluded due to Multi-Factor Authentication

Type	Omitted objects and attributes
Azure Active Directory	Risky users and Azure Active Directory extended attributes
Azure Resources	Fails with no data returned
Exchange Online	All Exchange Online Permissions, Mailbox Folders, Mailbox Statistics, Public Folders, Dynamic Groups and Members
Microsoft Teams	No files and folders (drives)
SharePoint Online	Fails with no data returned
One Drive	Fails with no data returned

Required services

The following services are required on the Enterprise Reporter server and nodes.

- Net.TCP Port Sharing

The following services must be enabled on discovery targets for collections.

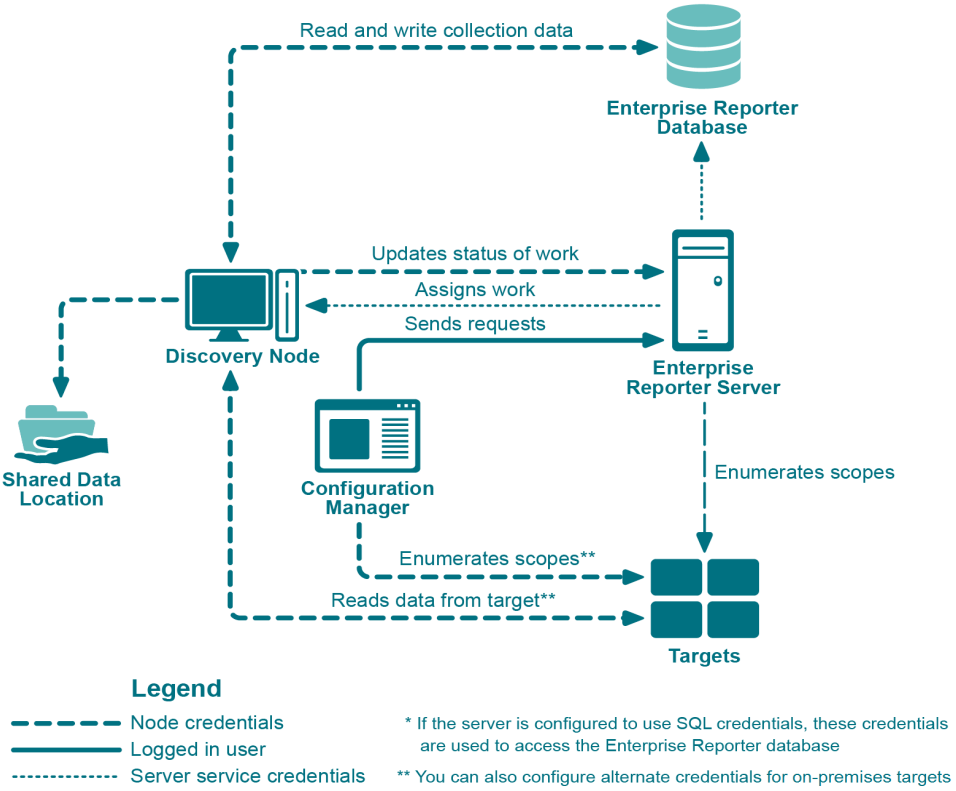
- Remote Registry
- SQL Server Browser service for SQL Discovery
- Windows Management Instrumentation (WMI)

Overview of Enterprise Reporter communications and required credentials

There are many communication channels in Enterprise Reporter, involving different sets of credentials. This allows for controlled access to your environment, but you must understand where each set of credentials are used and the permissions they need.

Figure 1 outlines where and for what each of the credentials are used, and the following tables explain the necessary permissions. For information on managing the credentials used in the Configuration Manager, see the *Using the Credential Manager* section in the Quest Enterprise Reporter Configuration Manager User Guide.

Figure 1. Credentials used to communicate in the Configuration Manager



Topics

- Node credential and alternate credential details for on-premises discoveries
- Detailed permissions for Enterprise Reporter discoveries
- Permissions for Enterprise Reporter discoveries on NAS devices
- Permissions for Enterprise Reporter tenant applications

Node credential and alternate credential details for on-premises discoveries

Node credentials are provided when a discovery node is created, and you can modify them as needed. By default, the node's credentials are used to enumerate scopes and access on-premises targets.

If you want to use different credentials for a particular discovery, you can configure them in the Discovery Wizard. By using these alternate credentials, you can target anything on-premises for which you have credentials, in any domain. You can minimize the permissions given to node credentials, and use alternate credentials for scoping and collecting your on-premises discoveries.

The following table outlines the use of the node and alternate credentials, and how to properly configure your environment to ensure successful data collection:

Table 16. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Server	Provide server with job status, errors, statistics and logs.	Configured during node creation, or when you edit the node properties to change the credentials. The node credentials must have local administrator access to the host computer and be a member of the group “Reporter_Discovery_Nodes”.
Discovery Node	Shared Data Location (if the cluster is configured to use one)	Read and write to the shared data location during data collection.	The shared data location is configured during the creation of a cluster. Ensure the node has read and write access to this file share. For more information, see the Things to Consider Before Creating a Cluster section in the Configuration Manager User Guide
Discovery Node	Enterprise Reporter Database	There are two options for communicating with the database: 1. You can use the same service credentials that the node service uses. 2. You can specify SQL credentials only for use when the database is accessed. The credentials you choose must be able to read and write to the database.	The account must be in the Reporter_Discovery_Nodes security group. (Note that if you use the same account as the Enterprise Reporter server it is already permissioned appropriately). If you use SQL authentication to connect with the database, you must manually permission the SQL user, either by adding them to the database role Discovery_Nodes_Role or by permissioning specific tables in the database.
Discovery Node	Targets	Read access on all targets. For on-premises discoveries, all domains with which the credentials have a forest or domain level trust will be enumerated. If required, you can configure alternate credentials for specific discoveries, instead of using the default node credentials.	The targets are defined as part of a discovery. The discovery tasks are assigned to a particular node based on availability, so all nodes in a cluster should have access to all targets defined in all discoveries assigned to the node’s cluster. For on-premises discoveries, ensure the node credentials or alternate credentials have read access to the target. In addition, a trust is required between the node computer and the targets. For more information on Azure and Microsoft 365 Discoveries, see Detailed permissions for Enterprise Reporter discoveries on page 20.

Detailed permissions for Enterprise Reporter discoveries

The following table outlines the permissions required for Enterprise Reporter discoveries.

Table 17. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Active Directory	An account with Active Directory read permissions is required to collect domain information, trusts, sites, domain controllers, and Active Directory computers, users, groups, and organizational units. The account being a member of the Built-in Domain Users group is sufficient to assign read permissions. To collect Fine Grained Password Policy and AD object level permissions, Domain Admin is required.
Azure Active Directory	An identity with read permission for the discovery target tenant. Read permissions are required for collection of tenant information, Azure Active Directory users, groups, group members, roles, and service principals. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Azure application required for this discovery.
Azure Resource	An identity with read permissions for the discovery target tenant. Read permissions are required for collection of subscription, Resource groups, and resources. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Azure Resource application required for this discovery.
Computer	An account with local administrator access on the scope computers to collect computer information, local groups and users, printers, services, policies, and event logs.
Exchange	To collect from Exchange targets, the credential account must have a mailbox on the target organization with access to read the permissions on the targets through EWS. To collect from Exchange 2013, 2016, or Mixed Modes, the credentials must be a member of the Organization Management Group. To collect from Exchange 2016 or Exchange 2019, the credentials must have an administrator role with an assigned “ApplicationImpersonation” role.
Exchange Online	An account with access to the discovery target tenant. Read permission is required for collection of all Exchange Online information including mailboxes, mailbox delegates, public folders, mail-enabled users, mail contacts, distribution groups, group members, and permissions. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as previously stated.

Table 17. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
File Storage Analysis	An account with local administrator access on the scoped computer is required to collect file, folder, share, and home drive analysis data. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 22.
Microsoft SQL	An account with local administrator access on the SQL Server is required. Additionally, the account must have read access to the scoped database to collect database information. At a minimum, if not using fixed roles, the following SQL permissions are required on the securable object being used for collection. • Grant View Any Definition • Grant View Server State • Grant View Connect Any Database • Grant View Select All Securables
Microsoft Teams	The user credentials used to collect Microsoft Teams information must have either the Teams Administrator or Global Administrator permissions. The user must also be a member of each Microsoft Teams group to prevent access denied errors during disk discovery. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Microsoft Teams application required for this discovery.
NTFS	If collecting through the administrator share, an account with local administrator access to the scoped computer is required. If collecting through a network share, an account with read permissions to the scoped shares is required. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 22.
OneDrive	An account with access to the discovery target tenant. Administrator permissions are required for collection of all drives including drive information, configuration settings, files, folders, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each drive that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter OneDrive application required for this discovery.

Table 17. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Registry	An account with local administrator access to the scoped computer is required to collect registry information.
SharePoint Online	An account with access to the discovery target tenant. Administrator permissions are required for collection of all SharePoint Online site collections, including tenant settings and policies, site information, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each site collection that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter SharePoint Online application required for this discovery.

Permissions for Enterprise Reporter discoveries on NAS devices

The following table outlines the permissions required for Enterprise Reporter discoveries.

Table 18. Permissions required for Enterprise Reporter discoveries on NAS Devices

Discovery Type	Permissions Required for Discovery Credential
NetApp Cluster Mode	Multiple virtual machines belong to a single cluster. All of these virtual machines can be specified as discovery targets. These virtual machines must be part of a domain. The NAS configuration must point to the cluster (name or IP address) with credentials that have read access to the cluster. These would typically be administrator credentials.
NetApp 7 Mode	In NetApp 7 mode, data can be collected on the storage controller or vFilers that are derived from the storage controller. Credentials with read access to the controller and vFiler are required.
NetApp Storage Controller	In NetApp 7 mode, data can be collected on the storage controller or vFilers that are derived from the storage controller. Credentials with read access to the controller and vFiler are required.
NetApp Filer	The vFiler can be a discovery target. In this case, the NAS configuration must point to the storage controller from which the vFilers are derived and the credentials must have read access to the storage controller.
Dell Fluid FS	The discovery target can be any Fluid FS VM. The NAS configuration must be the machine name or IP where Dell Enterprise Manager is installed and credentials must have access to Dell Enterprise Manager.
EMC Isilon	The discovery target can be any Isilon virtual machine. The NAS configuration must be the machine or IP that hosts the OneFS administration site and the credentials must have read access to it. By default, the connection is established using https and, if the connection is not deemed to be secure, the discovery will fail.

Permissions for Enterprise Reporter tenant applications

Enterprise Reporter requires Azure applications for the collection of Azure and Microsoft 365 objects and attributes. These applications must be registered in the Azure portal and consent must be granted for delegated permissions. To manage tenant applications used by Enterprise Reporter, you use the Configuration | Application Tenant Management option.

Azure Active Directory application permissions

For the Azure Active Directory discovery, the Exchange Online discovery, and the collection of nested group members for the OneDrive, Exchange Online, and Azure Resource discovery, an application with a name that begins with “Quest Enterprise Reporter Azure Discovery” is created. To create this application in your tenant, you must specify an account with administrative access to create applications. The account must have the Global Administrator role to be able to create and consent to the application.

Once created, the application must also be delegated permissions and an administrator must consent to the application’s permissions using the Microsoft consent wizard. For the Enterprise Reporter Azure discovery application, the following permissions are required:

Table 19. Required permissions

API Name	Permission	Permission Description	Type
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	Group.Read.All	Read all groups	
Microsoft Graph	IdentityRiskyUser.Read.All	Read identity risky user information	Delegated
Microsoft Graph	SecurityEvents.Read.All	Read your organization's security events	Delegated
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated
Microsoft Graph	Reports.Read.All	Read all usage reports	Delegated
Microsoft Graph	UserAuthenticationMethod.Read.All	Read all users' authentication methods	Delegated

Collecting user activity information

If you want to collect details about Microsoft 365 user activity, such as which licenses are assigned to a user and dates when a user last used a licensed service, the following delegated permission is required:

- Microsoft Graph: Read all usage reports

Also, you must clear the Microsoft default setting that anonymizes the user-level data. To include user activity data in the Enterprise Reporter reports, do the following steps:

1. Open the Microsoft 365 admin center.
2. Navigate to **Settings | Org Settings | Services**.
3. Select **Reports**.
4. Clear the **Display concealed user, group, and site names in all reports** check box.

For more information, see https://learn.microsoft.com/en-US/microsoft-365/troubleshoot/miscellaneous/reports-show-anonymous-user-name

OneDrive application permissions

For the OneDrive discovery, an application with a name that begins with “Quest Enterprise Reporter OneDrive Discovery” is created. To create this application in your tenant, you must specify an account with administrative access to create applications. The account must have the Global Administrator role to be able to create and consent to the application.

Once created, the application must also be delegated permissions and an administrator must consent to the application’s permissions using the Microsoft consent wizard. For the Quest Enterprise Reporter OneDrive Discovery application, the following permissions are required:

Table 20. Required permissions

API Name	Permission	Permission Description	Type
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	Files.Read.All	Read all files that user can access	Delegated
Microsoft Graph	Sites.FullControl.All	Have full control of all site collections	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated
Office 365 SharePoint Online	MyFiles.Read	Read user files	Delegated

Azure Resource application permissions

For the Azure Resource discovery, an application with a name that begins with “Quest Enterprise Reporter Azure Resource Discovery” is created. To create this application in your tenant, you must specify an account with administrative access to create applications. The account must have the Global Administrator role to be able to create and consent to the application.

Once created, the application must also be delegated permissions and an administrator must consent to the application’s permissions using the Microsoft consent wizard. For the Enterprise Reporter Azure Resource discovery application, the following permissions are required:

Table 21. Required permissions

API Name	Permission	Permission Description	Type
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated
Windows Azure Service Management API	user_impersonation	Access Azure Service Management as organization users	Delegated

Microsoft Teams application permissions

For the Microsoft Teams discovery, an application with a name that begins with “Quest Enterprise Reporter Microsoft Teams Discovery” is created. To create this application in your tenant, you must specify an account with administrative access to create applications. The account must have the Global Administrator role to be able to create and consent to the application.

Once created, the application must also be delegated permissions and an administrator must consent to the application’s permissions using the Microsoft consent wizard. For the Quest Enterprise Reporter Microsoft Teams Discovery application, the following permissions are required:

Table 22. Required permissions

API Name	Permission	Permission Description	Type
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	Files.Read	Read user files	Delegated
Microsoft Graph	Sites.FullControl.All	Have full control of all site collections	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed in user	Delegated
Microsoft Graph	Group.Read.All	Read all groups	Delegated
Office 365 SharePoint Online	MyFiles.Read	Read user files	Delegated

SharePoint Online application permissions

For the SharePoint Online discovery, an application with a name that begins with “Quest Enterprise Reporter SharePoint Online Discovery” is created. To create this application in your tenant, you must specify an account with administrative access to create applications. The account must have the Global Administrator role to be able to create and consent to the application.

Once created, the application must also be delegated permissions and an administrator must consent to the application’s permissions using the Microsoft consent wizard. For the Quest Enterprise Reporter SharePoint Online Discovery application, the following permissions are required:

Table 23. Required permissions

API Name	Permission	Permission Description	Type
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	Sites.FullControl.All	Have full control of all site collections	Delegated

Upgrade and compatibility

Note the following when upgrading to Enterprise Reporter:

- Disable clusters to stop discoveries from being sent to the nodes
- Cancel any jobs running on the nodes to stop data from writing to the Enterprise Reporter database
- Create a backup of the database
- Note the port number being used by the Enterprise Reporter server
- Upgrade the Enterprise Reporter components

- Upgrade the database
- Upgrade the nodes
- Manually upgrade any manually configured nodes
- Enable any disabled clusters to resume discoveries
- After upgrade to Enterprise Reporter 3.5.1, you must reconfigure all tenant applications. Open the Tenant Application Manager. For each tenant, click Reconfigure beside each application. Complete the wizard to register the application and reconsent to application permissions.
- After upgrade, you must authenticate all Azure credentials. Open the Credential Manager, select Azure credential, click Edit and Click Authenticate.

Upgrades to Enterprise Reporter are supported from the following versions:

- Enterprise Reporter 3.5 HF1
- Enterprise Reporter 3.5 HF2
- Enterprise Reporter 3.5
- Enterprise Reporter 3.2.2 H1
- Enterprise Reporter 3.2.2
- Enterprise Reporter 3.2.1 H1
- Enterprise Reporter 3.2.1
- Enterprise Reporter 3.2 H1
- Enterprise Reporter 3.2
- Enterprise Reporter 3.1
- Enterprise Reporter 3.0

IMPORTANT: After upgrading, it is recommended that you re-publish any reports previously in Quest SSRS to receive all updates and fixes.

Product licensing

To activate a trial or purchased commercial license

1. Copy the license you received from Quest to your Desktop, or another convenient location.
2. Ensure that the Enterprise Reporter Configuration Manager is installed.
3. Launch the Configuration Manager from the Start Menu and connect to the Enterprise Reporter server.
4. For first-time installations, the Licensing dialog box is displayed.

   - OR -

   Navigate to **System | Information** and click the **View licensing information** link.
5. Click **Update License** in the Licenses dialog box.
6. Navigate to the location of your license file and select it.
7. Click **Open** to apply the license.
8. Repeat steps 6-7 for each license file supplied by Quest.
9. Click **OK** to exit the licenses tab.

Getting started with Enterprise Reporter 3.5.1

The following section outlines how to get started with Enterprise Reporter and includes links to the technical documentation and Enterprise Reporter community for additional resources.

See also:

- Upgrade and Installation instructions
- Additional resources

Upgrade and Installation instructions

Contents of the release package

The Reporter release package contains the following products:

1. Quest Enterprise Reporter 3.5.1
2. Product Documentation, including:
    - EnterpriseReporter_3.5.1_QuickStartGuide_EN.pdf
    - EnterpriseReporter_3.5.1_InstallationAndDeploymentGuide_EN.pdf
    - EnterpriseReporter_3.5.1_ConfigurationManagerUserGuide_EN.pdf
    - EnterpriseReporter_3.5.1_Report ManagerUserGuide.pdf
    - Report_Designer_User_Guide_(Developer_Express).pdf
    - EnterpriseReporter_3.5.1_WhatsNew_EN.pdf
    - EnterpriseReporter_3.5.1_ReleaseNotes_EN.pdf
    - Online Help

Installation instructions

For upgrade and installation instructions, refer to the Enterprise Reporter Installation and Deployment User Guide in the Technical Documentation.

Additional resources

Additional information is available from the following:

- Online technical documentation
- Enterprise Reporter Community

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

This release has the following known capabilities or limitations: Known Issues:

- Unicode characters are not displayed correctly in the exported reports. Customers are advised to change report fonts that would work with multi-byte character sets.

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.

© 2024 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, 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.