Quest® Enterprise Reporter 3.2.1

Release Notes

October 2019

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

About Quest Enterprise Reporter 3.2.1

Enterprise Reporter provides a unified solution for data discovery and report generation. Using Enterprise Reporter's 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 3.2.1 is a minor release, with enhanced features and functionality. See New features and Resolved issues.

New features

New features in Enterprise Reporter 3.2.1:

- NTFS discovery scopes page improvements
- Performance enhancements for Exchange Online discoveries
- Active Directory discovery and reporting for managed service accounts
- Active Directory discovery and reporting of user attributes related to usage and requirement for Kerberos
- Active Directory discovery and reporting of service principal names for domain users

- Active Directory discovery and reporting for fine grain password properties
- Azure Active Directory discovery and reporting for users flagged as risky
- Computer discovery and reporting for Microsoft Store Applications
- SQL Server discovery and reporting of additional SQL server attributes including SQL Server Service Pack, case sensitivity, and service account
- SQL Server discovery and reporting of SQL Server jobs including information about job run type, status, and job schedule
- Configuration Manager What's New dialog and notification displays discoveries that need review and reconfiguration based on new features
- Discovery Manager **Duplicate Discovery** option creates new discoveries with similar configuration
- Schedule discovery **View Calendar** option displays what is scheduled to run on each day of the month
- Scheduled discoveries and reports now observe daylight saving time
- Report Manager **Show Preview** option controls the preview of a report while editing
- Report Manager **Import Layout** option imports the report layout from an existing report

See also:

- Enhancements
- Resolved issues
- Known issues

Enhancements

The following is a list of enhancements implemented in Enterprise Reporter 3.2.1.

Table 1. Customer requested enhancements

Enhancement	ID	Issue ID
Collect additional attributes for SQL Database users	753	
Collect if a drive is encrypted (Win32_EncryptableVolume)	935	3373582
Export the errors from the results of a discovery	1794	2454722
Set CC and BCC e-mail addresses for scheduled reports	1803	2528918
Improve Layout tab: suppress automatic display of report preview; add ShowPreview button	1808	2536729
Add option to suppress warning notifying the user that the ER server has been restarted	1851	2611869
Export all objects in the discovery results	1870	2701430
Exclude a list of objects from discovery using an import option	1880	2714742
Sort jobs on the Manage Discoveries page	1982	
Collect Managed Service Accounts and Group Managed Service Accounts	2765	
Collect new Microsoft Store Applications when collecting installed software	10529	
Collect Fine Grain Password Policy attributes for domain users	120143	4413877
Collect additional attributes for SQL Servers	121919	4434492
Exclude a list of objects from discovery using an import option	130682	2714742
Collect service principal name for users	131232	
Select UTC or local time zone when scheduling	131674	504863
Collect Managed Service Accounts and related membership	131877	

Table 1. Customer requested enhancements

Enhancement	ID	Issue ID
As a reporting user I can run the Managed Service Accounts report	131878	
Collect SQL Server information on database jobs	152362	4434492
As a reporting user I can report on user fine grain password policies	155372	
Collect Kerberos related attributes from Active Directory	155377	
Collect Is Trusted for Delegation and Is Trusted to Authenticate for Delegation attributes	159582	4506999
As a reporting user I can run a report *Bitlocker Information*	162547	

Resolved issues

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

Table 2. Resolved issues

Resolved issue	New ID	Issue ID
Add the ability to select fields for raw CSV output	3500	3774541
Local groups in a cluster are recorded incorrectly	41916	4287008
Getting the error System.Exception: CalculatedAceExtension: NTFSComputer.NTFSShare.NTFS.ACL.ACE entity not found for extension with 2.6 reports	120179	
Re-arranging selected fields bug	128028	4465907
Log Viewer: A user cannot delete zip file when added directly	129085	
Error: "Unable to connect to the report server" if security Groups are not in the Users OU	155365	
Enterprise Reporter Account Lockout Duration Reported as -1	157448	4514583
Unable to continue upgrading to 3.2.1 - 'Server Port Failed' message	160409	
Node deployment logs service account password in plain text	160849	4495990
OneDrive: Collection may not exit cleanly as expected when more than three repeated throttling errors occur on same folder or file	160851	
Error during AD discovery for permissions: "The Control is Critical."	162177	4483576
Report Client fails to load with error when using SQL Server Authentication and selecting the **Remember Credentials** option	162298	4509532
Options for CSV in the Report Manager scheduler are greyed out	164896	
Report schedule time is displayed in 12hr format and does not show AM/PM	164902	
Report Manager not opened if user in "Reporter_Exploring_Operators" group	168006	
Exchange Online public folder discovery RunspaceSessionController error	162522	
Reduce amount of logging during SQL discoveries	167126	4556245
Discovery node settings: the settings "separate SQL Server Authentication credential" cannot be saved correctly	168939	
Allow email addresses with the character "_" at the beginning of the email	168955	

Known issues

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

Table 3. Known issues

Known issue	New ID	Issue ID
OneDrive discoveries: Groups are not being properly collected on edits of the group properties/permissions	4009	
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 4. Installation known issues

Known issue	New ID	Issue ID
Installing the Enterprise Reporter Server using the Change functionality of the installer fails when UAC is enabled WORKAROUND: Disable UAC before using the Change function to install the server	371	215300
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 5. Configuration Manager known issues

Known issue	New 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
Office 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 6. Report Manager known issues

Known issue	New ID	Issue ID
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
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 7. Knowledge Portal known issues

Known issue	New ID	Issue ID
Special characters not handled correctly in Knowledge Portal 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 Knowledge Portal	373	224951
Scripts are not supported in Knowledge Portal reports	374	224953
When a report is published to Knowledge Portal, charts are not published and sometimes a blank space will appear in the Knowledge Portal report	409	398868
Links in reports are not supported in Knowledge Portal. 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 Knowledge Portal	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 Office365 reports do not publish correctly to Knowledge Portal - errors related to Raw Azure ID and unsupported data types	10819	

Table 7. Knowledge Portal known issues

Known issue	New ID	Issue ID
Advanced calculated field used in reports not supported in Knowledge Portal - reports not published	10889	
Custom images do not export from Report Manager reports to Knowledge Portal	18362	4156245
Parameters used in report layout as binded values are not supported when a report is exported to Knowledge Portal.	18363	4156245
Operator *EqualswithGroupExpansion* is not supported in Knowledge Portal. An error will occur when report is published.	85754	

Table 8. Documentation known issues

Known issue	New ID	Issue ID
Some of the PDF cross references do not link to their destination pages	380	348264

System requirements

Before installing Enterprise Reporter 3.2.1, ensure that your system meets the following minimum hardware and software requirements.

See also:

- Hardware Requirements
- New Required Hardware
- Supported Operating Systems
- Active Roles Supported Versions
- IT Security Search Supported Versions
- SQL Server Supported Versions
- New Required Software
- 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 2cores) • 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 more detailed recommendations for node requirements, see *Optimize Node Setup* in the Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation.

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 3.2.1 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

	ER Server	Consoles	Nodes
Operating Systems	Enterprise Reporter		
Windows Server® 1903	X		X
Windows Server® 2019	X	X	X
Windows Server® 1809	X		X
Windows Server® 2016	X	X	X
Windows Server® 1803	X		X
Windows Server® 2012 R2	X	X	X
Windows Server® 2012	X	X	X
Windows Server® Core 2012 R2	X		X
Windows Server® Core 2012 R2 Cluster	X		X
Windows Server® Core 2012	X		X
Windows Server® Core 2012 Cluster	X		X
Windows Server® 2008 R2 with Service Pack 1	X	X	X
Windows Server® Core 2008 R2 with Service Pack 1	X		X
Windows Server® Core 2008 R2 with Service Pack 1 (64-bit) Cluster	X		X
Windows Server® 2008 with Service Pack 2 (64-bit)	X	X	X
Windows® 10		X	
Windows® 8.1		X	
Windows® 8 (64-bit)		X	
Windows® 7 with Service Pack 1 (64-bit)		X	
Windows Vista® with Service Pack 2 (64-bit)		X	

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

Table 14. Supported Operating Systems for Discovery Targets

	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
Supported Operating Systems for Discovery Targets	Licences				
Domain Functional Levels					
Windows Server® 2019 Functional Level	X				
Windows Server® 2016 Functional Level	X				
Windows Server® 2012 R2 Functional Level	X				
Windows Server® 2012 Functional Level	X				
Windows Server® 2008 R2 Functional Level	X				
Windows Server® 2008 Functional Level	X				
Windows Server® 2003 Functional Level	X				
Computers					
Windows Server® 1903		X	X		
Windows Server® 2019 and 1809		X	X		
Windows Server® 2016 and 1803		X	X		
Windows Server® 2012 R2		X	X		
Windows Server® 2012		X	X		
Windows Server® Core 2012		X	X		
Windows Server® 2008 R2 with Service Pack 1		X	X		
Windows Server® Core 2008 R2 with Service Pack 1		X	X		
Windows Server® 2008 with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows Server® 2003 R2 with Service Pack 2 (64-bit)		X	X		
Windows Server® 2003 with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows® 10		X	X		
Windows® 8.1		X	X		
Windows® 8 (64-bit and 32 bit)		X	X		
Windows® 7 with Service Pack 1 (64-bit and 32 bit)		X	X		
Windows Vista® with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows® XP Professional with Service Pack 3 (64-bit and 32 bit)		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		

	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
Supported Operating Systems for Discovery Targets	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		
SQL Server Instances					
SQL Server® 2017				X	
SQL Server® Clusters				X	
SQL Server® 2016				X	
SQL Server® 2014				X	
SQL Server® 2012				X	
SQL Server® 2008 R2				X	
SQL Server® 2008 with Service Pack 2				X	
SQL Server® 2005 with Express Service Pack 3				X	
SQL Server® 2005 with Service Pack 3				X	
Exchange Servers					
Exchange® 2019					X
Exchange® 2016					X
Exchange® 2013					X
Exchange® 2010					X
Exchange® 2007					X
Exchange® Mixed Modes (2007-2010, 2010-2013, 2007-2013)					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 7.3
- Active Roles 7.2.1
- Active Roles 7.1.2
- Active Roles 7.0.4
- Active Roles 7.0.2

- Active Roles 6.9.0

IT Security Search Supported Versions

Enterprise Reporter can be configures 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
- IT Security Search 11.3

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® 2017
- SQL Server® 2016
- SQL Server® 2014
- SQL Server® 2012
- SQL Server® 2008 R2
- SQL Server® 2008 with Service Pack 2
- SQL clusters and database mirroring are supported for your deployment, including
  - SQL Server® 2016 Always On
  - SQL Server® 2014 Always On
  - SQL Server® 2012 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 need to communicate with the SQL Server®, such as:
    - 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

New Required Software

The following software is required for Enterprise Reporter 3.2.1 and higher.

- PowerShell™ 3.0
- Microsoft®.NET Framework 4.6
- Microsoft SharePoint Online Management Shell

    > **NOTE:** PowerShell 3.0 and Microsoft SharePoint Online Management Shell are required on the node machines to collect OneDrive configuration settings.
    >
    > **NOTE:** In addition, for OneDrive configuration settings to be collected successfully, an authorized connection must be established to the SharePoint Online service. To allow for credentials to be specified for your tenant, the “LegacyAuthProtocols” setting must be enabled on your tenant. To set this on your tenant, run the following commands using the Microsoft SharePoint Online Management Shell. This action must be performed on any node machine with Microsoft SharePoint Online Management Shell installed.

    ```
    Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned

    Import-Module -Name Microsoft.Online.SharePoint.PowerShell

    Connect-SPOService -Url "https://<tenant>-admin.sharepoint.com"

    Set-SPOTenant -LegacyAuthProtocolsEnabled $True

    Disconnect-SPOService
    ```

- Microsoft Azure Active Directory Module for Windows PowerShell

    > **NOTE:** Microsoft Azure Active Directory Module for Windows PowerShell is required on the node machines to collect multi-factor authentication attributes for Azure Users.

Required Software

The following software is required for Enterprise Reporter.

- Microsoft®.NET Framework 4.6
- Microsoft®.NET Framework 4.0 (Full)
- Microsoft®.NET Framework 3.5 Service Pack 1
- Microsoft® Excel® (required to view reports exported as spreadsheets)
- Microsoft® Excel® 2010
- Microsoft® Excel® 2013
- 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® 2007 information, the following additional considerations are required:

- Exchange® 2007 Management Tools must be installed on the computer where the Enterprise Reporter node is installed and must be in the same forest as the 2007 Exchange Organization.
- It is highly recommended to put the computer where the Enterprise Reporter node is installed within the target Exchange® 2007 domain.

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)

Azure Required Software

To collect Azure information, the following additional software is required:

- Microsoft Azure Active Directory Module for Windows PowerShell

  NOTE: Microsoft Azure Active Directory Module for Windows PowerShell is required on the node machines to collect multi-factor authentication attributes for Azure Users.

Exchange Online Required Software

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

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

OneDrive Required Software

To collect OneDrive information, the following additional software is required:

- Microsoft SharePoint Online Management Shell

  > **NOTE:** PowerShell 3.0 and Microsoft SharePoint Online Management Shell are required on the node machines to collect OneDrive configuration settings.
  >
  > **NOTE:** In addition, for OneDrive configuration settings to be collected successfully, an authorized connection must be established to the SharePoint Online service. To allow for credentials to be specified for your tenant, the “LegacyAuthProtocols” setting must be enabled on your tenant. To set this on your tenant, run the following commands using the Microsoft SharePoint Online Management Shell. This action must be performed on any node machine with Microsoft SharePoint Online Management Shell installed.
  >
  > ```
  > Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned
  >
  > Import-Module -Name Microsoft.Online.SharePoint.PowerShell
  >
  > Connect-SPOService -Url "<full tenant name>"
  >
  > Set-SPOTenant -LegacyAuthProtocolsEnabled $True
  >
  > Disconnect-SPOService
  > ```

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.

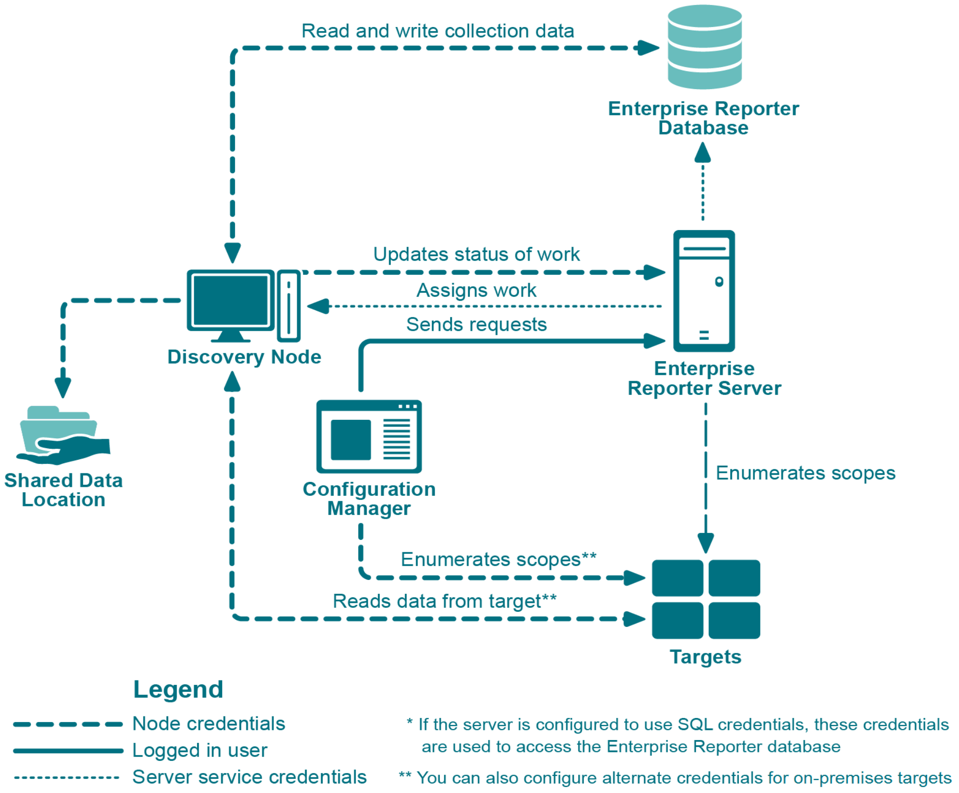
- Remote Registry
- SQL Server Browser service for SQL Discovery
- Windows Management Instrumentation (WMI)

An Overview of Enterprise Reporter Communications and Credentials Required

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 what 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 in the Technical Documentation.

Figure 1. Credentials used to communicate in the Configuration Manager


Read and write collection data
Enterprise Reporter Database
Updates status of work
Assigns work
Sends requests
Discovery Node
Enterprise Reporter Server
Shared Data Location
Configuration Manager
Enumerates scopes
Enumerates scopes**
Reads data from target**
Targets
Legend
Node credentials
Logged in user
Server service credentials
* If the server is configured to use SQL credentials, these credentials are used to access the Enterprise Reporter database
** You can also configure alternate credentials for on-premises targets

See also:

- 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 15. 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 in the Technical Documentation.

Table 15. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
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). For more information, see Role Based Security in Enterprise Reporter and Configuring the Database in the Quest Enterprise Reporter Release Notes in the Technical Documentation. 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 Office 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 16. 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.
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. For more information, see Using the Tenant Application Manager on page 47.
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. For more information, see Using the Tenant Application Manager on page 47.
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 2007 targets, the credentials must be a member of the Exchange Organization Administrators Group. To collect from Exchange 2010, 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 “ApplicationImpresonation” 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 stated above.

Table 16. 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.
Microsoft Teams	An identity with read permissions for the discovery target tenant. Read permissions are required for collection of Microsoft Teams information including teams, members, channels, applications, and drives. 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. For more information, see Using the Tenant Application Manager on page 47.
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 Azure application required for this discovery. For more information, see the Using the Tenant Application Manager section of the Configuration Manager User Guide in the Technical Documentation.
Registry	An account with local administrator access to the scoped computer is required to collect registry information.

Permissions for Enterprise Reporter Discoveries on NAS Devices

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

Table 17. 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 Office 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 please refer to in the System | Configuration | Application Tenant Management section in the Enterprise Reporter Configuration Manager User Guide.

OneDrive Azure Application Permissions

For the OneDrive discovery, an application with the name Quest Enterprise Reporter One Drive Discovery will be 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 One Drive Discovery application, the following delegated permissions are required:

- Microsoft Graph: Read user files
- Office 365 SharePoint Online: Read user files

- Windows Azure Active Directory: Access the directory as signed-in user
- Windows Azure Active Directory: Read directory data

Azure Active Directory Application Permissions

For the Azure Active Directory discovery, the Exchange Online discovery, and the collection of group members for the OneDrive discovery, an application with the name Quest Enterprise Reporter Azure Discovery will be 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 Azure Discovery application, the following delegated permissions are required:

- Microsoft Graph: Access directory as the signed in user
- Microsoft Graph: Read all groups
- Microsoft Graph: Read all users’ basic profiles
- Microsoft Graph: Read all users’ full profiles
- Microsoft Graph: Read directory data
- Microsoft Graph: Read identity risky user information
- Microsoft Graph: Read your organization’s security events
- Azure Active Directory Graph: Access the directory as signed-in user
- Azure Active Directory Graph: Read all groups

Azure Resource Application Permissions

For the Azure Resource discovery, an application with the name Quest Enterprise Reporter Azure Resource Discovery will be 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 Azure Resource Discovery application, the following delegated permissions are required:

- Windows Azure Service Management API: Access Azure Service Management as organization users
- Windows Azure Active Directory: Access the directory as signed-in user
- Windows Graph: Read all users’ basic profiles

Microsoft Teams Application Permissions

For the Microsoft Teams discovery, an application with the name Quest Enterprise Reporter Microsoft Teams Discovery will be 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 delegated permissions are required:

- Microsoft Graph: Read all users’ basic profiles
- Windows Azure Active Directory: Access the directory as signed-in user
- Windows Azure Active Directory: Read all groups

Upgrade and compatibility

Note the following when upgrading to Enterprise Reporter 3.2.1:

- 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
- During the upgrade to Enterprise Reporter 3.2.1, previously collected Exchange Online information will be removed. After upgrading to Enterprise Reporter 3.2.1, you must run your Exchange Online discoveries to collect the latest information.

Upgrades to Enterprise Reporter 3.2.1 are supported from the following versions of Enterprise Reporter:

- 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 Knowledge Portal 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 3.2.1

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 3.2.1

2 Product Documentation, including:

  - EnterpriseReporter_3.2.1_QuickStartGuide_EN.pdf
  - EnterpriseReporter_3.2.1_InstallationAndDeploymentGuide_EN.pdf
  - EnterpriseReporter_3.2.1_ConfigurationManagerUserGuide_EN.pdf
  - EnterpriseReporter_3.2.1_Report ManagerUserGuide.pdf
  - Report_Designer_User_Guide_(Developer_Express).pdf
  - EnterpriseReporter_3.2.1_WhatsNew_EN.pdf
  - EnterpriseReporter_3.2.1_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:

1. Multibyte Character Product Support: Require .NET 4.5 for Internationalized Domain Names - Service will not start if using .NET 4.0
2. 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.

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. 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.**

i **IMPORTANT NOTE**, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.