Quest® Enterprise Reporter 3.1

Release Notes

July 2018

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

About Quest Enterprise Reporter 3.1

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 3.1 is a minor release, with enhanced features and functionality. See New features and Resolved issues.

New features

New features in Enterprise Reporter 3.1:

- Azure Resource discovery and reporting for resource subscriptions, resource groups, resources, virtual machines, disks, networking, storage accounts and network security groups. Please refer to the Enterprise Reporter 3.1 Configuration Manager User Guide for further information on how to set up your first Azure Resource discovery.
- Performance enhancements for File Storage Analysis
- Detailed Enterprise Reporter System reports showing information about discoveries, discovery clusters, discovery errors, and discovery tasks

- Configurable custom icon for report headers
- Configurable favorite parameter values with the option to load them when running reports
- Options to sort, edit, group, filter, and import parameter values when running reports
- Ability to export and import report category information
- Options to view report schedule history, sort schedule reports, disable schedules, specify custom report filenames, and to select from pre-defined values for pathnames and email addresses
- Support for multiple email notification recipients
- Configurable levels to control how much logging information is collected from Enterprise Reporter
- Option to send all information to IT Security Search

See also:

- Enhancements
- Resolved issues
- Known issues

Enhancements

The following is a list of enhancements implemented in Enterprise Reporter 3.1.

Table 1. Customer requested enhancements

Enhancement	ID	Issue ID
Ability to run a report that shows Domain User Accounts At Risk	33	
Ability to load favorites on a report on a schedule	47	
Ability to add scopes for Computer Discoveries using a query more clearly	61	3219076
Ability to let administrators take ownership of another user's report schedules (and associated reports)	722	2716888
Ability to disable a schedule	724	
Ability to include or exclude volumes from File Storage Analysis discovery scope	725	
Ability to run a report that shows File and Folder Permission Differences (with additional parameters)	733	
Ability to set a global image to be used for report header icon	737	
Ability to collect Exchange mailbox sub-folders and their permissions	751	
Ability to allow reporting administrators to edit reports in Published Reports	754	
Ability to provide a simple report name and to allow scheduled reports to overwrite existing reports	777	2486903
Ability to enter a test address in the SMTP Test Connection dialog and validate that email is sent and received	878	3357637
Ability to set a global image to be used for the icon in report headers	884	3247551
Ability to see more than 25 characters of the OS Version in Computer reports	891	3526787
Ability to look up SQL server requirements for Enterprise Reporter in the guides	896	3514362
Ability to report on the discovery process itself, beyond the usual metrics	900	3566542
Ability to support instance name in Quest Knowledge Portal address	936	
Ability to run a report that shows Folders/Files with ACLs that contain deleted accounts	956	
Ability to view scheduled report history	966	

Table 1. Customer requested enhancements

Enhancement	ID	Issue ID
Ability to filter possible parameters values based on a selected parameter value	1011	
Ability to expand and collapse schedules to see the reports that are listed	1537	
Ability to sort reports by topic (NTFS, Computer, and so on) rather than alphabetically	1539	
Ability to use custom report names for scheduled reports	1775	
Ability to set favorite parameter values	1864	2676705
Ability to order items alphabetically in the NTFS path picker	2185	3650721
Ability to predefine particular fields when creating a new report schedule	2289	3644749
Ability to prevent automatic emailing of blank reports	3177	3746538
Ability to send scheduled email report attachments that are larger than 1MB	3222	3682283
Ability to use "or" entries in parameters	3751	3807877
Ability to filter Local Service, System, and Network Services accounts out of the Services not running as a System account report	3895	3831809
Ability to report on file count per folder to understand unused or frequently used folders	7289	
Ability to edit parameter lists	7467	
Ability to collect multi-factor authentication attributes for users	8935	
Ability to configure the logging level of all Enterprise Reporter components	11024	4073646
Ability to run File Storage Analysis discoveries using multiple tasks/threads when scanning a single host	11591	4069922
Ability to run a report of Probable Group Owners	12835	
Ability to import a file of parameter values for parameters that accept multiple values	14645	
Ability to collect information from EMC VNX storage arrays	16201	4140764
Ability to run a Computer Services report that differentiates between Automatic and Automatic (Delayed Start) startup types	16265	
Ability to run an Azure Active Directory Users with Multi-factor Authentication Information report and an Azure Global Administrators without Multi-factor Authentication Enabled report	16269	
Ability to collect the modifiedTimestamp attribute during the collection of group information	16823	
Ability to reference parent folders for performance enhancement to NTFS	17725	4147152
Ability to add multiple email addresses to the Email Notifications for node and discovery changes	18284	
Ability to import specific folder paths for NTFS discoveries	18347	
Ability to set the NTFS cleanup timeout setting	18672	4168131
Ability to audit users logged in to Enterprise Reporter and the changes made	19909	
Ability to run reports using favorite parameter values	20117	2676705
Ability to refresh the Report Manager Report tab contents	20265	
Ability to resolve the computer domain namespaces in case of disjoint namespaces to improve the performance of Computer discoveries	22350	4218740

Resolved issues

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

Table 2. Resolved issues

Resolved issue	New ID	Issue ID
Make the “Search within” section of the NTFS object picker in NTFS discoveries, have the “Enter” key as the default	2186	
Database clean up utility times out	5358	
Database Wizard does not check the Data File Path and Log File Path format when creating a new database	10905	
Issues with Health Check and Active Directory reports in Enterprise Reporter 3.0.0.2722 Report Library	11696	
Database Wizard: Configure Security Groups has wording that does not make sense when using service account from external forest	11833	
Getting NTFSShare namespaces error when trying to import custom reports created in Enterprise Reporter 2.6 into Enterprise Reporter 3.0	15297	
Report Manager has items in the configuration file that do not need to be loaded and it slows down launching Report Manager	15712	
Creating a report from a report type with a single entity omits the tombstoned clause from the report query	15986	
When exporting a report to CSV, the text separator defaults to commas even when an override is set	23593	4226052
Improve log entries for Exchange discovery - remove unnecessary logging	25020	
Mailbox Delegates not stored - duplicate IDs	25022	
Exchange public folders not respecting excluded domains when organization is collected	25424	
Collection of mailbox delegates greatly affecting the Exchange collection - need to add caching for account lookups	25816	
No activity reported while collecting Mailbox Delegates or statistics for Mailbox Delegates	25817	
New option in Exchange discovery to exclude collection of specified accounts as delegates	25872	
Computer discovery stuck on one computer	26299	

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	

Table 3. Known issues

Known issue	New ID	Issue ID
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	
NTFS discoveries: Excluding a share folder from the NTFS discovery Scopes doesn't work	10744	
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	

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
After initial upgrade, the Configuration Manager may be slow to launch as the new security descriptor is being created. Configuration Manager will launch after the action is complete.	420	453448
Configuration Manager may crash after upgrade due to missing licensing file	423	458949
The ParentFolderID in the NTFSFolder table will only be populated during the collection that follows an upgrade	17725	4147152

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
The dollar sign ($) used for hidden shares does not look correct in Trebuchet font	379	347709
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
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
Password reset causes discoveries to fail	382	361828
NTFS discovery errors on DFSROOT folders that are actually on the machine but collector says they cannot be found	396	384183

Table 5. Configuration Manager known issues

Known issue	New ID	Issue ID
SQL Discovery does not enumerate the SQL Server located on the same system as Enterprise Reporter	397	384273
Re-parse points and File Storage Analysis storage collections	398	385403
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
Multiple errors when using multiple nodes and running ARS collection with AD if nodes do not have prerequisites	449	626447
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

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
Report Manager slow down when launching	419	450627
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
Custom query reports can allow security breach if SQL Server/database is not properly permissioned	438	613837
Security Explorer cannot take action against 32 registry key from 64 bit machine.	10570	
Exchange and Exchange Online Mailbox Permissions report does not report on NT Authority/Self and will not display direct permissions assigned to account.	11181	
Error in the Report Manager when you copy/paste a report from the library and apply a global report icon	26748	

Table 7. Knowledge Portal known issues

Known issue	New ID	Issue ID
Reports with data that contain special characters will not run in Knowledge Portal	372	223723
The option to display nested groups and their members in the following reports is not supported in Knowledge Portal: • Local Group with Members • Domain Group with Members • Azure Active Directory Groups and Members • Azure Active Directory Application Service Principal Assignments and Members	373	224951
Scripts are not supported in Knowledge Portal reports	374	224953
When a report is published to Knowledge Portal, charts are incorrectly formatted and sometimes a blank space will appear in the Knowledge Portal report	409	398868
There are multiple reports in File Storage Analysis with scripting that cannot be published to Knowledge Portal	410	398871
Links in reports are not supported in Knowledge Portal	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
Advanced calculated field used in OneDrive reports not supported in Knowledge Portal - reports not published	10889	
New special operator for equalswithgroupexpansion for parameter UniqueUserDisplayName in OneDrive not supported in Knowledge Portal - filtering may not work	10890	

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 3.1, ensure that your system meets the following minimum hardware and software requirements.

Hardware Requirements

For each component we recommend the following minimum hardware:

Table 9. 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	Disk space requirements will vary with the Reporter components you install: • Server - 10 GB • Configuration Manager - 2 GB • Discovery Node - 10 GB for installed files, plus extra space (10 GB - 100 GB) for processing discoveries. Space required varies with the amount of data collected. • Report Manager - 10 GB • Database size varies with the amount of data you collect • The file share that you use for the optional Shared Data Location will require space for storage of collected data. Space required varies with the amount of data collected. • Total disk size if all components and databases are on the same system - 100 GB

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

Table 10. SQL Server Hardware Requirements

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

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.

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.

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 Reporter3.1 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 11. Supported Operating Systems

Operating Systems	Enterprise Reporter		
	ER Server	Consoles	Nodes
Windows Server® 2016	X	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 12. Supported Operating Systems for Discovery Targets

Supported Operating Systems for Discovery Targets	Licences				
	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
Domain Functional Levels					
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® 2016		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® 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		

Supported Operating Systems for Discovery Targets	Active Directory Licences	Windows Server Licences	File Storage Analysis Licences	SQL Server Licences	Exchange Licences
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 Online™					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 7.2.1
- 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 3.1 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 "<full tenant name>"

  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® 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)

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
```

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.

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.

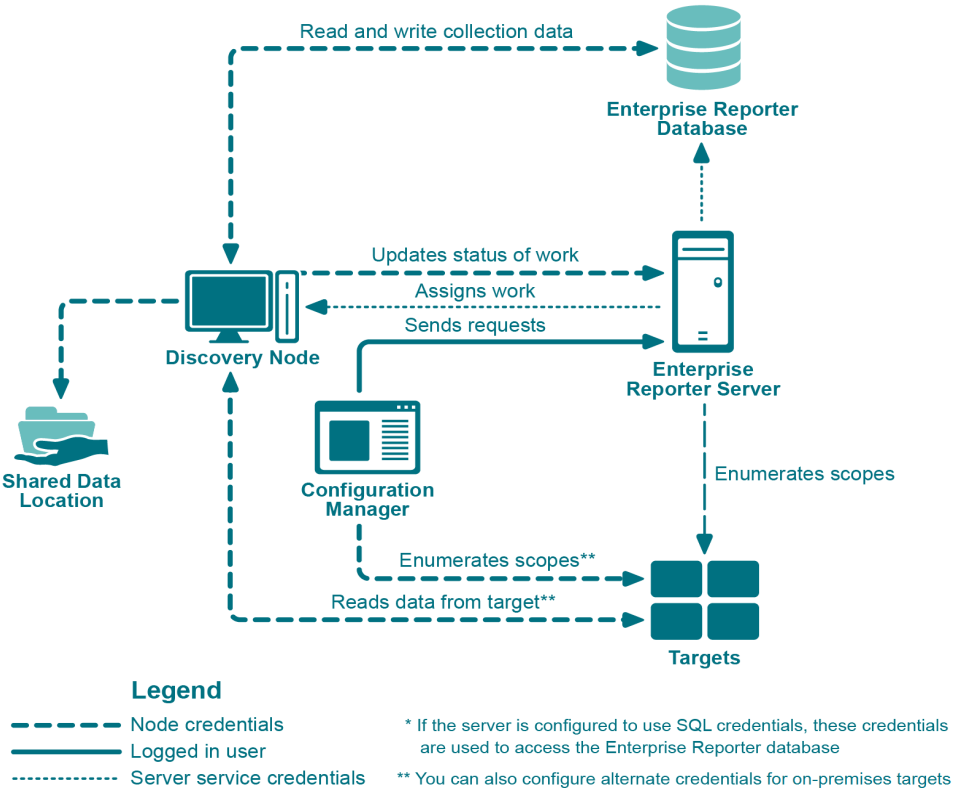
- Remote Registry
- Windows Management Instrumentation (WMI)

An Overview of the Configuration Manager Security

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 n the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

Figure 1. Credentials used to communicate in the Configuration Manager



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 13. 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.
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 13. 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_Admins 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 Reporter_Discovery_Admin_Role (recommended) 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 18.

Detailed Permissions for Enterprise Reporter Discoveries

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

Table 14. 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 43.
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 43.
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.
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.
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 19.

Table 14. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
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.
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 19.
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 15. 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.

Table 15. Permissions required for Enterprise Reporter discoveries on NAS Devices

Discovery Type	Permissions Required for Discovery Credential
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, 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: Read all users' basic profiles
- Windows Azure Active Directory: Access the directory as signed-in user
- Windows Azure Active Directory: 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

Upgrade and compatibility

Note the following when upgrading to Enterprise Reporter 3.1:

- 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

Upgrades to Enterprise Reporter 3.1 are supported from the following versions of Enterprise Reporter:

- Enterprise Reporter 3.0
- Enterprise Reporter 2.6
- Enterprise Reporter 2.5.1
- Enterprise Reporter 2.5

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 3.1

Upgrade and Installation instructions

Contents of the release package

The Reporter release package contains the following products:

1. Quest Enterprise Reporter 3.1
2. Product Documentation, including:
   - EnterpriseReporter_3.1.0_QuickStartGuide_EN.pdf
   - EnterpriseReporter_3.1.0_InstallationAndDeploymentGuide_EN.pdf
   - EnterpriseReporter_3.1.0_ConfigurationManagerUserGuide_EN.pdf
   - EnterpriseReporter_3.1.0_Report ManagerUserGuide.pdf
   - Report_Designer_User_Guide_(Developer_Express).pdf
   - EnterpriseReporter_3.1.0_WhatsNew_EN.pdf
   - EnterpriseReporter_3.1.0_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 Quest

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit https://quest.com/contact.

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.

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

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