

Quest™ Enterprise Reporter 3.0

Release Notes

July 2017

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

- [About Quest Enterprise Reporter 3.0](#)
- [New features](#)
- [Enhancements](#)
- [Resolved issues](#)
- [Known issues](#)
- [System requirements](#)
- [An Overview of the Configuration Manager Security](#)
- [Product licensing](#)
- [Getting started with Enterprise Reporter 3.0](#)
- [Globalization](#)
- [About Quest](#)

About Quest Enterprise Reporter 3.0

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 3.0 is a major release, with enhanced features and functionality. See [New features](#) and [Resolved issues](#).

New features

New features in Enterprise Reporter 3.0:

- New Enterprise Reporter for Office 365 licensed module
- OneDrive discovery and reporting for OneDrive files and folders. Please refer to the Enterprise Reporter 3.0 Configuration Manager User Guide for further information on how to set up your first OneDrive discovery.
- Azure and Azure Active Directory discovery and reporting for Azure subscriptions, licenses, and service plans and Azure Active Directory users, groups, roles, and application service principals. Please refer to the Enterprise Reporter 3.0 Configuration Manager User Guide for further information on how to set up your first Azure discovery.

- NTFS Discovery performance enhancements
- New NTFS and File Storage Analysis Discovery options (including NAS configuration and collection of hidden shares)
- Security Explorer Remediation reporting
- IT Security Search configuration and data options
- New Enterprise Reporter Database Content Wizard integrated into existing Database Wizard. The Database Content Wizard allows you to perform various database maintenance tasks such as running backups, merging databases, cleaning discovery data, and running scripts.
- Support for Windows 2016

See also:

- [Enhancements](#)
- [Resolved issues](#)

Enhancements

The following is a list of enhancements implemented in Enterprise Reporter 3.0.

Table 1. Customer requested enhancements

Enhancement	ID	Issue ID
Ability to modify a report to find files older than 7 years, 2555 days	59	
Create a Group Membership by Domain Account report that includes recursive group membership. New Active Directory library report: Recursive Group Membership by Domain Account	471	
Ability for the discovery job system to allow stopping a job run if all remaining tasks are running on a node in faulted state	714	622739
Events are logged when node is in the faulted state	726	476134
Ability to receive an email notification of the status of discovery and nodes	738	370287
Ability to run discoveries against Office 365	744	590682
Ability to report on total folder size including the subfolders	1837	
Ability to turn off the collection of domain contacts	1991	
System validates that the service account has sysadmin and dbowner privileges on SQL server	2130	
Create a report to see who can change group membership and modify user properties. New Active Directory library reports: Users and groups that can change group membership, Users and groups that can change any property of users	2528	
Ability to report on Windows Updates on 2012 R2 Servers (and greater) as hotfixes	2702	
Increase OS Name and OS Version field sizes in the Enterprise Reporter database.	3971	

Resolved issues

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

Table 2. Resolved issues

Resolved issue	New ID	Issue ID
Screen resolution can cause issues with being able to access all controls in Configuration Manager	81	
Deleted Object collection and stats do not show collection of OU	83	
SQL Discoveries stuck in a pending state and do not show as completed	400	387525
Discovery failures when the DNS and domain suffixes do not match	421	454228
Collection groups in AD discovery causing error: "Server does not support the control. The control is critical"	500	
Error during AD resolution task	1987	
WMI calls in Computer collector do not use full username, this treats the user as local user which is wrong	2127	
Report schedules: PDF output w/ password not working	2359	
Password Complexity setting not reported correctly if unset	3806	
Email scroll bar does not work in the email setting for a schedule task in the Report Manager	4146	
Node crashes after running for a about a minute	4307	
Configuration for report timeout need to be changed for the Export to CSV option	4525	
RSOP collected attribute do not show the correct value on non-PDC DCs	5141	

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
The dollar sign used for hidden shares does not look correct in Trebuchet font	379	347709
Groups permissioned on OneDrive files and folders are not being properly collected when edits occur on the group properties/ permissions.	4009	
OneDrive Collection of permissions is returning unexpected results when "Contribute" permission is assigned	4221	
OneDrive Custom Permissions are only returning the "name" of the custom permission and there are no further results available on actual set permission	4222	
Renamed groups may not be processed correctly by OneDrive discovery due to limitations of Microsoft Graph API. If a group is renamed after initial collection, the new name will not be collected by subsequent permission collection and permissions may appear incorrectly.	5486	
Inaccurate NTFS Duplicate files calculations due to not looking at whole computer, only share	7839	
PowerShell intermittently returns OneDrive configuration settings incorrectly and updating these attributes is slow on native portal	9902	
Excluding a shared folder from the NTFS discovery scopes does not work	10744	

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
Multibyte Character Product Support: Require .NET 4.5 for Internationalized Domain Names - Service will not start if using .NET 4.0	378	341608
Mobile IT Licencing Issue (Mobile IT 1.3 + ER 2.5)	402	387936
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
A locked file may prevent the Access Explorer service from stopping during upgrade and the installer will fail. To prevent, ensure that the service is stopped prior to upgrade.	422	458172
Configuration Manager may crash after upgrade due to missing licensing file	423	458949

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
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
Two errors when deploying Agent to a Server 2012 machine	375	315882
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-erroring on DFSROOT folders that are actually on the machine but collector says they cant be found	396	384183
SQL Discovery does not enumerate the SQL Server located on the same system as Enterprise Reporter	397	384273
Reparse 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

Table 5. Configuration Manager known issues

Known issue	New ID	Issue ID
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.	369	180547
If you make a change in parameters, you are not warned that you will lose your changes if you do not click Save.		
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	
Charts are resizing and displaying a message to increase the chart's size instead of displaying the chart.	11149	
Exchange and Exchange Online Mailbox Permissions report does not report on NT Authority/Self and will not display direct permissions assigned to account.	11181	

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: <ul style="list-style-type: none"> • 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

Table 7. Knowledge Portal known issues

Known issue	New ID	Issue ID
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	
Some NTFS reports do not publish correctly to Knowledge Portal and publishing pauses with no error	11319	

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

Hardware Requirements

For each component you need the following minimum hardware:

Table 9. Hardware Requirements

Enterprise Reporter	
Memory	<ul style="list-style-type: none"> • Minimum: 16 GB RAM • Recommended: 16 GB RAM

Table 9. Hardware Requirements

Enterprise Reporter	
Processor	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 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

New Required Hardware

The following hardware is required for Enterprise Reporter 3.0 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.

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

Table 10. 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

Table 10. Supported Operating Systems

Operating Systems	ER Server	Consoles	Nodes
	Enterprise Reporter		
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 11. Supported Operating Systems for Discovery Targets

Supported Operating Systems for Discovery Targets	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
	L i c e n c e s				
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		

	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
	L i c e n c e s				
Supported Operating Systems for Discovery Targets					
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 Fluid File System 5.0		X	X		
Isilon One FS® 7.2 - 8.0 and above (Collections require a secure connection to Isilon with a valid certificate.)		X	X		
NetApp® Filer - Data ONTAP® 8..x - 9.x and above (Cluster mode is supported as of version 8.2)		X	X		
SQL Server Instances					
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 7.1.2

- Active Roles 7.0.4
- Active Roles 7.0.2
- Active Roles 6.9.0

IT Security Search Supported Versions

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

- IT Security Search 11.3

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[®] 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 3.0 and higher.

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

Required Software

To obtain links to the following required software, open the Enterprise Reporter Autorun.

- Microsoft[®].NET Framework 4.6
- Microsoft[®].NET Framework 4.0 (Full)
- Microsoft[®].NET Framework 3.5 Service Pack 1
- Microsoft[®] Visual C++[®] 2012 Service Pack 1 Redistributable Package (x64) version 11.0.60610.1
- Microsoft[®] Visual C++[®] 2010 Service Pack 1 Redistributable Package (x64) version 10.0.40219
- Microsoft[®] Visual C++[®] 2005 Service Pack 1 Redistributable Package (x64) version 8.0.59192

Other Required Software

- PowerShell 3.0
- Microsoft[®] Excel[®] (required to view reports exported as spreadsheets)
- Microsoft[®] Excel[®] 2013
- Microsoft[®] Excel[®] 2010

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.

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.

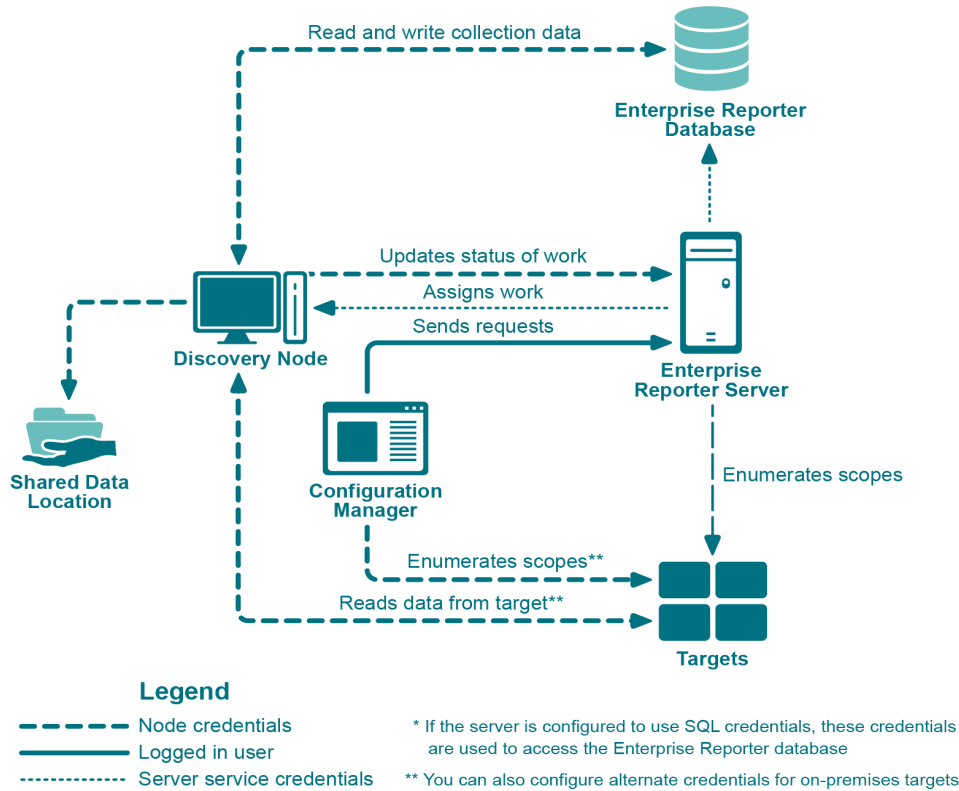
- Remote Registry
- Windows Management Instrumentation (WMI)

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 in 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 12. 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 12. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Database	<p>There are two options for communicating with the database:</p> <ol style="list-style-type: none"> 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. <p>The credentials you choose must be able to read and write to the database.</p>	<p>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 Installation and Deployment Guide in the Technical Documentation.</p> <p>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.</p>
Discovery Node	Targets	<p>Read access on all targets.</p> <p>For on-premises discoveries, all domains with which the credentials have a forest or domain level trust will be enumerated.</p> <p>If required, you can configure alternate credentials for specific discoveries, instead of using the default node credentials.</p>	<p>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.</p> <p>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.</p> <p>For more information on Azure and Office 365 Discoveries, see Detailed Permissions for Enterprise Reporter Discoveries on page 16.</p>

Detailed Permissions for Enterprise Reporter Discoveries

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

Table 13. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Active Directory	<p>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.</p> <p>The account being a member of the Built-in Domain Users group is sufficient to assign read permissions.</p>
Azure Active Directory	<p>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.</p> <p>If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above.</p> <p>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 42.</p>
Computer	<p>An account with local administrator access on the scope computers to collect computer information, local groups and users, printers, services, policies, and event logs.</p>
Exchange	<p>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.</p> <p>To collect from Exchange 2007 targets, the credentials must be a member of the Exchange Organization Administrators Group.</p> <p>To collect from Exchange 2010, Exchange 2013, 2016, or Mixed Modes, the credentials must be a member of the Organization Management Group.</p>
Exchange Online	<p>An account with access to the discovery target tenant.</p> <p>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.</p> <p>If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above.</p>
File Storage Analysis	<p>An account with local administrator access on the scoped computer is required to collect file, folder, share, and home drive analysis data.</p> <p>For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter Discoveries on NAS Devices on page 17.</p>
Microsoft SQL	<p>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.</p>
NTFS	<p>If collecting through the administrator share, an account with local administrator access to the scoped computer is required.</p> <p>If collecting through a network share, an account with read permissions to the scoped shares is required.</p> <p>For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter Discoveries on NAS Devices on page 17.</p>

Table 13. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
OneDrive	<p>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.</p> <p>Additionally, the discovery credentials must have site collection administrator rights to each drive that is being collected.</p> <p>If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above.</p> <p>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.</p>
Registry	<p>An account with local administrator access to the scoped computer is required to collect registry information.</p>

Permissions for Enterprise Reporter Discoveries on NAS Devices

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

Table 14. Permissions required for Enterprise Reporter discoveries on NAS Devices

Discovery Type	Permissions Required for Discovery Credential
NetApp Cluster Mode	<p>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.</p> <p>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.</p>
NetApp 7 Mode	<p>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.</p>
NetApp Storage Controller	<p>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.</p>
NetApp Filer	<p>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.</p>
Dell Fluid FS	<p>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.</p>
EMC Isilon	<p>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.</p>

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

Upgrade and compatibility

Note the following when upgrading to Enterprise Reporter 3.0:

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

- Upgrade the nodes
- Manually upgrade any manually configured nodes
- Enable any disabled clusters to resume discoveries
- After upgrading to Enterprise Reporter 3.0, if you are collecting against NAS devices, you must manually update your discovery configuration to take advantage of these features.

Upgrades to Enterprise Reporter 3.0 are supported from the following versions of Enterprise Reporter:

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

Product licensing

To activate a trial or purchased commercial license

- 1 Copy the license you received from Dell 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 Dell.
- 9 Click **OK** to exit the licenses tab.

Getting started with Enterprise Reporter 3.0

Upgrade and Installation instructions

Contents of the release package

The Reporter release package contains the following products:

- 1 Quest Enterprise Reporter 3.0
- 2 Product Documentation, including:
 - EnterpriseReporter_3.0.0_QuickStartGuide_EN.pdf
 - EnterpriseReporter_3.0.0_InstallationAndDeploymentGuide_EN.pdf

- EnterpriseReporter_3.0.0_ConfigurationManagerUserGuide_EN.pdf
- EnterpriseReporter_3.0.0_Report ManagerUserGuide.pdf
- Report_Designer_User_Guide_(Developer_Express).pdf
- EnterpriseReporter_3.0.0_WhatsNew_EN.pdf
- EnterpriseReporter_3.0.0_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](#) (hyperlink)
- [Enterprise Reporter Community](#)(hyperlink)

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, Central & Eastern Europe, Far East Asia, Japan, Western Europe & Latin America.

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.

© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

Refer to our website (<https://www.quest.com>) for regional and international office information.


Patents


Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.


Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit <https://www.quest.com/legal/trademark-information.aspx>. All other trademarks and registered trademarks are the property of their respective owners.

Legend

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

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

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