



Quest[®] Enterprise Reporter 3.2.2
Installation and Deployment Guide



© 2021 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.

Contents

Product Overview	6
Introducing Quest™ Enterprise Reporter	6
Key Features of Enterprise Reporter	7
Enterprise Reporter Components	8
.....	8
Enterprise Reporter Architecture	8
Installation Considerations for Enterprise Reporter	10
Before You Install Enterprise Reporter	10
Reporter Server and Database Considerations	10
Failover Recovery using SQL Clusters	11
System Requirements	11
Hardware Requirements	11
New Required Hardware	13
Supported Operating Systems	13
Active Roles Supported Versions	16
IT Security Search Supported Versions	16
SQL Server Supported Versions	16
New Required Software	17
Required Software	18
Required Services	19
An Overview of Enterprise Reporter Communications and Credentials Required	20
Node Credential and Alternate Credential Details for On-Premises Discoveries	21
Detailed Permissions for Enterprise Reporter Discoveries	23
Permissions for Enterprise Reporter Discoveries on NAS Devices	25
Permissions for Enterprise Reporter Tenant Applications	25
.....	27
.....	27
Minimum Permissions for Initially Installing Enterprise Reporter	27
Port Requirements	28
Firewall Requirements	35
Database Requirements	36
Configuring the Database and Security Groups	36
Installing and Configuring Enterprise Reporter	39
Installing Enterprise Reporter	39
Installing the Components	40
Installing and Configuring Individual Components	43
Installing and Configuring the Configuration Manager	43
Installing and Configuring the Report Manager	44
Installing and Configuring the Database Wizard	44
Installing and Configuring the Log Viewer	44
Installing and Configuring the Encryption Key Manager	44
Creating a Database Prior to Enterprise Reporter Server Installation	44

Installing and Configuring IT Security Search	45
Upgrading Enterprise Reporter	45
Preparing to Upgrade Enterprise Reporter	45
Upgrading Enterprise Reporter Components	46
Upgrading Enterprise Reporter Nodes	48
Upgrading Manually-Configured Enterprise Reporter Nodes	49
After Upgrading Enterprise Reporter	49
Licensing Enterprise Reporter	49
Activating or Updating Your License	51
Security Groups in Enterprise Reporter	51
Role Based Security in Enterprise Reporter	52
Managing Your Database Using the Database Wizard	53
Using the Database Wizard to Create or Connect a Database	54
Upgrading a Database	55
Deleting a Database	56
Changing the Security Mode	57
Changing the Connection to the Enterprise Reporter Database	58
Performing Database Maintenance	59
Managing Your Enterprise Reporter Deployment	60
Optimizing Enterprise Reporter	60
Enterprise Reporter Server and Database Considerations	60
Failover Recovery using SQL Clusters	61
Cluster Deployment Considerations	61
Consider the Data to Collect Before Deploying Nodes	61
Fine Tune Each Cluster and Node	61
Optimize Node Setup	62
Plan Credential Use	65
Effectively Deploy Remote Nodes	68
Optimize Data Transfer	69
Discovery Considerations	69
Divide Discovery Targets According to Cluster Structure	69
Collect Only the Data Needed	70
Plan Discovery and Reporting Schedules	75
Optimize Nested Group Membership Collection	75
Optimize Nested Group Membership Collection for Azure and Office 365 Discoveries	76
Troubleshooting Issues with Enterprise Reporter	77
Troubleshooting Installation Issues	77
Connecting to a SQL Server®	77
Issues with Multi-Domain Controller Environments	78
Problems Opening the Consoles	78
Database Configuration Issues	78
Troubleshooting Connectivity Issues	79
Restoring a Connection to the Enterprise Reporter Server	80
Restoring a Connection to the Enterprise Reporter Database	80
Troubleshooting Connection Timeouts	81

Troubleshooting Credential Change Failures	81
Resolving Issues in the Configuration Manager	82
Node Issues	82
Data Collection Issues	83
Troubleshooting Features in Enterprise Reporter	85
Exporting Logs from the Configuration Manager	85
Viewing Information About Your Enterprise Reporter Configuration	86
Viewing Errors and Statistics for Tasks	86
Moving the Enterprise Reporter Database	87
Disaster Recovery	88
Back Up of Enterprise Reporter	88
How to Deploy Enterprise Reporter to Another Computer After a Disaster	88
Checking the Enterprise Reporter Configuration After a Recovery	89
.....	90
Appendix: Database Content Wizard	91
Software Requirements	91
Starting and Configuring the Enterprise Reporter Database Content Wizard	91
Transferring an Enterprise Reporter Database	92
Backing Up an Enterprise Reporter Database	93
Restoring an Enterprise Reporter Database	94
Cleaning an Enterprise Reporter Database	95
Merging Two Enterprise Reporter Databases	96
Running Custom Enterprise Reporter Scripts	97
Appendix: Encryption Key Manager	99
Starting the Encryption Key Manager	99
Generating a Key File	99
Importing a Key File	100
Exporting a Key File	100
Resetting Credentials	101
Appendix: Log Viewer	102
Starting the Enterprise Reporter Log Viewer	102
Finding and Opening Log Files	102
Viewing and Searching Log File Entries	103
Filtering Log File Entries	104
Index	105
About us	108
Technical support resources	108

Product Overview

Topics

- [Introducing Quest™ Enterprise Reporter](#)
- [Key Features of Enterprise Reporter](#)
- [Enterprise Reporter Components](#)
- [Enterprise Reporter Architecture](#)

Introducing Quest™ Enterprise Reporter

Quest Enterprise Reporter provides administrators, security officers, help desk staff, and other stakeholders with insight into their network environment. Reporting on your network environment provides:

- General visibility into the security and configuration of your environment.
- Validation against your security policies to ensure objects are configured as expected. This helps you detect security violations such as identifying users with inappropriate access.
- An easy way to respond to inquiries from internal and external auditors requesting security and configuration information.

Enterprise Reporter provides scalability, security, and customizability by:

- Allowing the use of Multi-Factor Authentication enabled credentials to be used on Cloud discoveries for added security.
- Allowing you to deploy Enterprise Reporter to take advantage of both your network structure and available hardware or virtual computers. You can scale your deployment up or down as your needs change.
- Separating data collection from reporting, allowing less technical users to easily generate the reports they need from stored data.
- Using role-based security to provide and revoke access to your Quest Enterprise Reporter deployment.
- Providing granular credentials management, allowing you to access information using different accounts for performing different tasks and accessing different parts of your environment. Accounts are stored in a central Credential Manager, making it easy for you to see what accounts are in use and to keep them up to date.
- Providing a full featured report designer. You can easily customize the included reports by adding attributes and using advanced filtering, or you can build new reports to satisfy the unique requirements of your organization.
- Automating the collection of data and the generation and delivery of reports.

Key Features of Enterprise Reporter

Organizations worldwide are struggling to keep up with corporate policies, changing government regulations, and industry standards. Generating reports that prove compliance, and deciding what data to include is a time consuming and difficult process. In order to meet compliance requirements or initiate IT best practices, organizations must know exactly what is in the IT infrastructure at any moment in time, how it is configured, and who has access to it. Quest presents Enterprise Reporter as a solution to these problems.

Enterprise Reporter provides a unified solution for data discovery and report generation. Using the Enterprise Reporter Configuration Manager, administrators can easily configure and deploy discoveries to collect and store data. Once the data has been collected, the Report Manager allows users to produce reports that help organizations to ensure that they comply with industry regulations and standards, adhere to internal security policies, monitor hardware and software requirements, and fulfill many other reporting requirements.

Using the Configuration Manager, you can:

- Configure your collection environment to minimize network traffic and optimize performance.
- Create discoveries to collect data that will be made available to the Report Manager:
 - information about your Active Directory® environment
 - information about files and folders from domains, OUs, computers, NetApp® and EMC® filers, shares, and DFS shares
 - information about the computers in your environment
 - data from specified SQL Server® computers, instances, and databases
 - general and registry information from selected computers
 - high-level summary information on file storage
 - high-level summary information and permissions in your Exchange® environment
 - information about your Azure® subscriptions, licenses, and service plans
 - information about your Azure Active Directory® environment
 - information about your Azure® resources
 - information about files and folders in your OneDrive® environment
 - information about your Office 365® Exchange Online environment
 - information about your Microsoft Teams in Office 365®
- Create Cloud discoveries using Azure Active Directory Multi-Factor Authentication (MFA) enabled credentials
- Schedule discoveries to run automatically.
- Track the progress of discoveries, and pinpoint any errors in the collection.

Using the Report Manager, you can:

- Run reports on the data you have collected.
- Make predefined reports available to reporting users by publishing them.
- Create your own customized reports.
- Customize the appearance of your reports.
- Schedule reports to run when you need them.
- Use the File Storage Analysis summary reports, with meaningful charts and graphs and the ability to drill down for more detailed information, to answer challenging administrative questions about file storage.

- Use the Exchange[®] summary reports, with meaningful charts and graphs and the ability to drill down for more detailed information, to answer challenging administrative questions about your Exchange[®] environments.
- Use the Exchange[®] reports to monitor and update the access permissions of accounts in an efficient and timely manner to ensure mailbox information security.
- Use the OneDrive[®] reports to answer questions about file and folder permissions in your OneDrive[®] environment.
- Use the Azure[®] reports to answer questions about your Azure[®] subscriptions, licenses, and settings.
- Use the Azure Active Directory[®] reports to answer questions about your Azure Active Directory[®] environment.
- Use the Azure[®] resource reports to answer questions about your Azure[®] resources.
- Use the Office 365 Exchange[®] Online reports to answer questions about your Exchange[®] Online mailbox, mailbox folders, and public folders and their permissions.
- Use the Microsoft Teams reports to answer questions about your Microsoft Teams in Office 365[®].

Enterprise Reporter Components

An Enterprise Reporter deployment includes (at minimum):

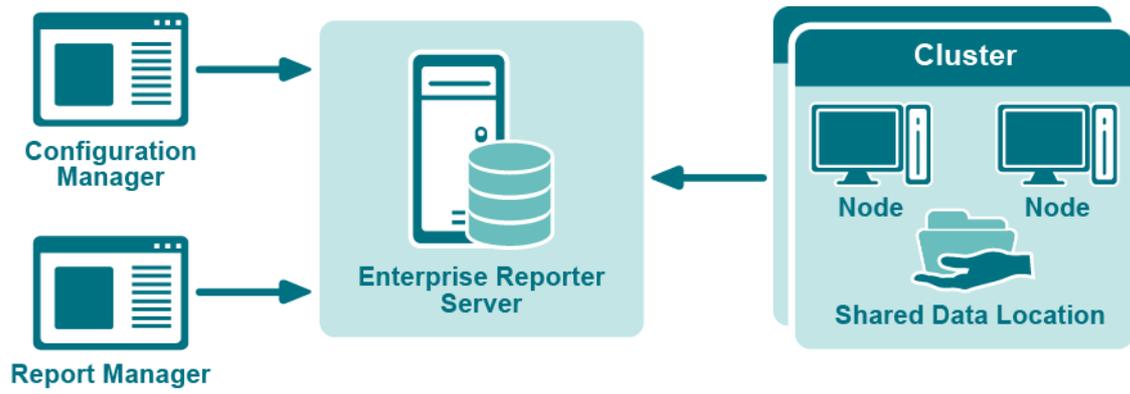
- An Enterprise Reporter server and database
- At least one Configuration Manager installation
- At least one deployed node
- At least one Report Manager installation

- [Enterprise Reporter Architecture](#)

Enterprise Reporter Architecture

[Figure 1](#) outlines the relationship between the components.

Figure 1. Enterprise Reporter Architecture



Installation Considerations for Enterprise Reporter

Topics

- [Before You Install Enterprise Reporter](#)
- [Reporter Server and Database Considerations](#)
- [System Requirements](#)
- [An Overview of Enterprise Reporter Communications and Credentials Required](#)
- [Database Requirements](#)

Before You Install Enterprise Reporter

The system requirements are the same for all components of Enterprise Reporter. Ensure that the minimum requirements are met and all necessary software is installed before installing any of the components.

Topics

- [Reporter Server and Database Considerations](#)
- [System Requirements](#)
- [Minimum Permissions for Initially Installing Enterprise Reporter](#)
- [Port Requirements](#)
- [Firewall Requirements](#)
- [Configuring the Database and Security Groups](#)
- [Database Requirements](#)

Reporter Server and Database Considerations

You need to choose a host computer for Enterprise Reporter server and a SQL Server® to host the Enterprise Reporter database. Your decision will affect the performance of the product.

The Enterprise Reporter server communicates directly with the database frequently. Locate the Enterprise Reporter server physically close to the SQL Server® for best results.

The nodes also regularly connect to the database. The more nodes you have in your deployment, and the more discoveries you run, the greater the impact on the SQL Server®. Choose a SQL Server® with enough power to manage the connections and data transfer from the nodes. Check your Microsoft® SQL Server® documentation for more information on system requirements.

Reporter supports a variety of SQL configurations. You can use a regular SQL instance, a SQL cluster, or a mirrored database. If your SQL deployment supports it, using clusters or mirrors allows for automatic failover recovery in the event that a SQL Server® is down.

Topics

- [Failover Recovery using SQL Clusters](#)

Failover Recovery using SQL Clusters

Using a SQL cluster instead of a single server allows for automatic failover recovery in the event that a SQL Server® is down. Tasks are automatically passed to another SQL Server®. Your cluster can be configured with Always On.

System Requirements

Before installing Enterprise Reporter 3.2.2, ensure that your system meets the following minimum hardware and software requirements.

Topics

- [Hardware Requirements](#)
- [New Required Hardware](#)
- [Supported Operating Systems](#)
- [Active Roles Supported Versions](#)
- [IT Security Search Supported Versions](#)
- [SQL Server Supported Versions](#)
- [New Required Software](#)
- [Required Software](#)
- [Required Services](#)

Hardware Requirements

Enterprise Reporter Server

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

Table 1. Enterprise Reporter Server Hardware Requirements

Component	Recommended specifications
Memory	<ul style="list-style-type: none">• Minimum: 8 GB RAM• Recommended: 16 GB RAM

Table 1. Enterprise Reporter Server Hardware Requirements

Component	Recommended specifications
Processor	<ul style="list-style-type: none">• Intel® or AMD 2 GHz multiprocessor (with at least 2cores)• 64-bit processor
Hard disk space	<ul style="list-style-type: none">• 10 GB• The file share used for the optional Shared Data Location requires space for storage of collected data. Space requirements vary with the amount of data collected.

Configuration Manager and Report Manager

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

Table 2. Configuration Manager and Report Manager Hardware Requirements

Component	Recommended specifications
Memory	<ul style="list-style-type: none">• Minimum: 16 GB RAM• Recommended: 16 GB RAM
Processor	<ul style="list-style-type: none">• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores)• 64-bit processor
Hard disk space	<ul style="list-style-type: none">• Configuration Manager: 2 GB• Report Manager: 20 GB

Enterprise Reporter Nodes

For the Enterprise Reporter Nodes, we recommend the following minimum hardware. For more detailed recommendations for node requirements, see [Optimize Node Setup on page 62. Technical Documentation](#).

Table 3. Node Hardware Requirements

Component	Recommended specifications
Memory	<ul style="list-style-type: none">• Minimum: 16 GB RAM• Recommended: 16 GB RAM
Processor	<ul style="list-style-type: none">• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores - 4 recommended)• 64-bit processor
Hard disk space	<ul style="list-style-type: none">• 10 GB for installed files plus 10-100 GB extra space for processing collections

Enterprise Reporter SQL Server

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

Table 4. SQL Server Hardware Requirements

Component	Recommended specifications
Memory	<ul style="list-style-type: none">• Minimum: 16 GB RAM• Recommended: 24 GB RAM
Processor	<ul style="list-style-type: none">• Intel® or AMD 2 GHz multiprocessor (with at least 4cores)• 64-bit processor
Hard disk space	<ul style="list-style-type: none">• 100 GB or more for larger environments

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

Database Size Estimator

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

Larger Environments

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

- The type of collections being performed.

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

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

- The size of collections being performed.

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

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

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

New Required Hardware

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

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

Supported Operating Systems

The following operating systems are supported for Enterprise Reporter components.

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

Table 5. Supported Operating Systems

Operating Systems	ER Server	Consoles	Nodes
	Enterprise Reporter		
Windows Server® 20H2	X		X
Windows Server® 2004	X		X
Windows Server® 1909	X		X
Windows Server® 1903	X		X
Windows Server® 2019	X	X	X
Windows Server® 1809	X		X
Windows Server® 2016	X	X	X
Windows Server® 1803	X		X
Windows Server® 2012 R2	X	X	X
Windows Server® 2012	X	X	X
Windows Server® Core 2012 R2	X		X
Windows Server® Core 2012 R2 Cluster	X		X
Windows Server® Core 2012	X		X
Windows Server® Core 2012 Cluster	X		X
Windows Server® 2008 R2 with Service Pack 1	X	X	X
Windows Server® Core 2008 R2 with Service Pack 1	X		X
Windows Server® Core 2008 R2 with Service Pack 1 (64-bit) Cluster	X		X
Windows® 10		X	
Windows® 8.1		X	

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

Table 6. 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® 2019 Functional Level	X				
Windows Server® 2016 Functional Level	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 Server® 2012 R2 Functional Level	X				
Windows Server® 2012 Functional Level	X				
Computers					
Windows Server® 20H2		X	X		
Windows Server® 2004		X	X		
Windows Server® 1909		X	X		
Windows Server® 1903		X	X		
Windows Server® 2019 and 1809		X	X		
Windows Server® 2016 and 1803		X	X		
Windows Server® 2012 R2		X	X		
Windows Server® 2012		X	X		
Windows Server® Core 2012		X	X		
Windows® 10		X	X		
Windows® 8.1		X	X		
Network Attached Storage (NAS) Devices					
Dell Fluid File System 6.0		X	X		
Dell Fuilid File System 5.0		X	X		
NetApp® 9.4		X	X		
NetApp® 9.3		X	X		
NetApp® Filer - Data ONTAP® 8..x - 9.x and above (Cluster mode is supported as of version 8.2)		X	X		
EMC Isilon OneFS (Collections require a secure connection to Isilon with a valid certificate.)		X	X		
EMC® VNX 7.1.47.5 X (Supported by collecting as a Windows Server)		X	X		
EMC® VNX 7.0.35.3 X (Supported by collecting as a Windows Server)		X	X		
SQL Server Instances					
SQL Server® 2019				X	
SQL Server® 2017				X	
SQL Server® Clusters				X	
SQL Server® 2016				X	
SQL Server® 2014				X	
SQL Server® 2012				X	
Exchange Servers					

Supported Operating Systems for Discovery Targets	Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
	L i c e n c e s				
Exchange® 2019					X
Exchange® 2016					X
Exchange® 2013					X

Active Roles Supported Versions

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

- Active Roles 7.4.3
- Active Roles 7.3
- Active Roles 7.2.1
- Active Roles 7.1.2
- Active Roles 7.0.4
- Active Roles 7.0.2
- Active Roles 6.9.0

IT Security Search Supported Versions

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

- IT Security Search 11.4
- 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® 2019
- SQL Server® 2017
- SQL Server® 2016
- SQL Server® 2014
- SQL Server® 2012
- SQL clusters and database mirroring are supported for your deployment, including

- SQL Server® 2016 Always On
- SQL Server® 2014 Always On
- SQL Server® 2012 Always On

Using SQL Server Certificates

SSL Encryption of SQL Server Connections using Certificates

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

The steps required to configure this encryption are as follows.

- Using the Microsoft Management Console (MMC):
 - install the Certificates snap-in for the SQL Server® host computer
 - import the certificate to the SQL Server® host computer
- Using SQL Server Configuration manager:
 - configure the SQL Server® to use the certificate
 - configure the SQL Server® to force encryption
- Restart the SQL Server® host computer
- Import the certificate to all Enterprise Reporter computers that will need to communicate with the SQL Server®, such as:
 - Enterprise Reporter server host computer
 - Enterprise Reporter nodes
 - Enterprise Reporter Configuration Manager host computer
 - Enterprise Reporter Report Manager host computer
- Install Enterprise Reporter on a host computer

New Required Software

The following software is required for Enterprise Reporter 3.2.2 and higher.

- PowerShell™ 3.0
- Microsoft® .NET Framework 4.6
- Microsoft Azure Active Directory Module for Windows PowerShell

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

NOTE:

- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

Required Software

The following software is required for Enterprise Reporter.

- Microsoft® .NET Framework 4.6
- Microsoft® .NET Framework 4.0 (Full)
- Microsoft® .NET Framework 3.5 Service Pack 1
- Microsoft® Excel® (required to view reports exported as spreadsheets)
- Microsoft® Excel® 2010
- Microsoft® Excel® 2013
- PowerShell™ 3.0

Active Roles Required Software

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

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

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

The following additional considerations are required:

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

Exchange Required Software

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

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

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

- Impersonation needs to be configured on the Exchange organization. Refer to your Exchange Server documentation or use the following method to set up role assignments.
 - Powershell can be used to add an assignment
New-ManagementRoleAssignment –Name:impersonationAssignmentAdministrator
–Role:ApplicationImpersonation –User:Administrator
 - Alternatively, you can create an administrator role with ApplicationImpersonation role assigned to it and add the required account as a member (or assign ApplicationImpersonation role to an existing administrator role)

Azure Required Software

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

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

- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

Exchange Online Required Software

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

- Ensure the Windows Remote Management (WinRM) service is running.
- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

OneDrive Required Software

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

- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

Azure Active Directory Resource Required Software

- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

Microsoft Teams Required Software

- Microsoft AzureRM PowerShell Module

i | **NOTE:** Microsoft AzureRM PowerShell Module is required to authorize multi-factor authenticated credentials.

Required Services

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

- Net.TCP Port Sharing

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

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

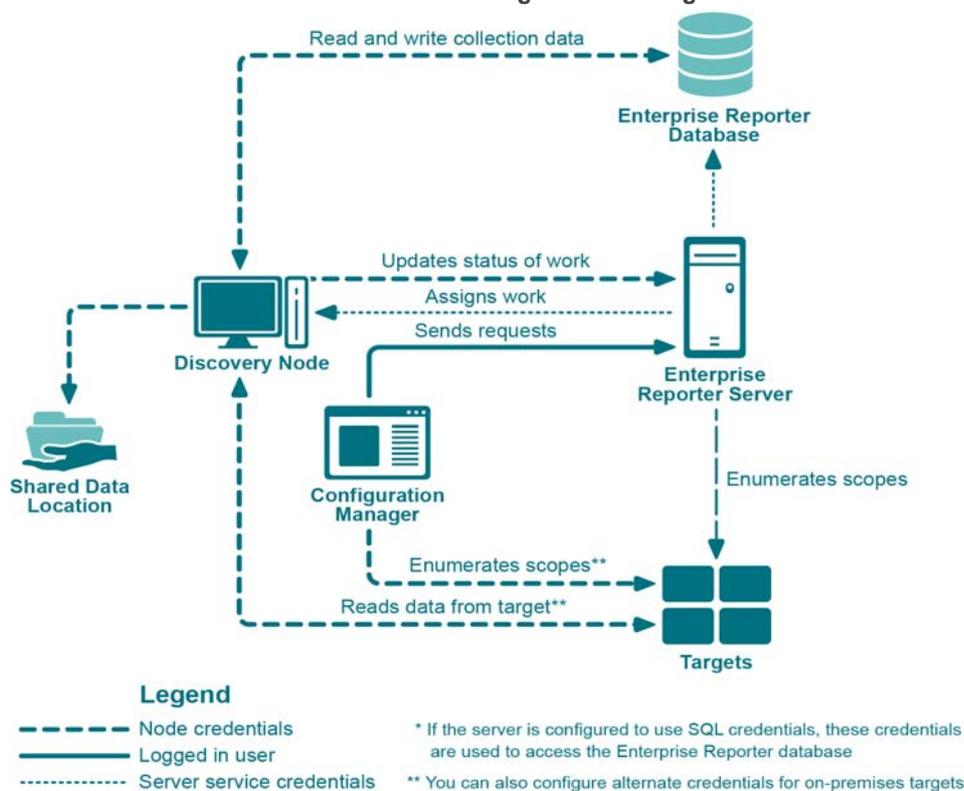
An Overview of Enterprise Reporter Communications and Credentials Required

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

Figure 2 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 2. Credentials used to communicate in the Configuration Manager



Topics

- Node Credential and Alternate Credential Details for On-Premises Discoveries
- Detailed Permissions for Enterprise Reporter Discoveries
- Permissions for Enterprise Reporter Discoveries on NAS Devices
- Permissions for Enterprise Reporter Tenant Applications

Node Credential and Alternate Credential Details for On-Premises Discoveries

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

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

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

Table 7. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Server	Provide server with job status, errors, statistics and logs.	Configured during node creation, or when you edit the node properties to change the credentials. The node credentials must have local administrator access to the host computer and be a member of the group "Reporter_Discovery_Nodes".
Discovery Node	Shared Data Location (if the cluster is configured to use one)	Read and write to the shared data location during data collection.	The shared data location is configured during the creation of a cluster. Ensure the node has read and write access to this file share. For more information, see the Things to Consider Before Creating a Cluster section in the Configuration Manager User Guide in the Technical Documentation .

Table 7. 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_Nodes security group. (Note that if you use the same account as the Enterprise Reporter server it is already permissioned appropriately). Technical Documentation.</p> <p>For more information, see Role Based Security in Enterprise Reporter on page 52.</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 Discovery_Nodes_Role 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 23.</p>

Detailed Permissions for Enterprise Reporter Discoveries

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

Table 8. 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 120.</p>
Azure Resource	<p>An identity with read permissions for the discovery target tenant. Read permissions are required for collection of subscription, Resource groups, and resources.</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 Resource application required for this discovery. For more information, see Using the Tenant Application Manager on page 120.</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 2013, 2016, or Mixed Modes, the credentials must be a member of the Organization Management Group.</p> <p>To collect from Exchange 2016 or Exchange 2019, the credentials must have an administrator role with an assigned "ApplicationImpersonation" role.</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 25.</p>

Table 8. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
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> <p>At a minimum, if not using fixed roles, the following SQL permissions are required on the securable object being used for collection.</p> <ul style="list-style-type: none"> • Grant View Any Definition • Grant View Server State • Grant View Connect Any Database • Grant View Select All Securables
Microsoft Teams	<p>An identity with read permissions for the discovery target tenant. Read permissions are required for collection of Microsoft Teams information including teams, members, channels, applications, and drives.</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 Microsoft Teams application required for this discovery. For more information, see Using the Tenant Application Manager on page 120.</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 25.</p>
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 OneDrive 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 9. Permissions required for Enterprise Reporter discoveries on NAS Devices

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

Permissions for Enterprise Reporter Tenant Applications

Enterprise Reporter requires Azure applications for the collection of Azure and Office 365 objects and attributes. These applications must be registered in the Azure portal and consent must be granted for delegated permissions. To manage tenant applications used by Enterprise Reporter please refer to in the System | Configuration | Application Tenant Management section in the Enterprise Reporter Configuration Manager User Guide.

OneDrive Azure Application Permissions

For the OneDrive discovery, an application with a name that begins with “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
- Microsoft Graph: Have full control of all site collections

Azure Active Directory Application Permissions

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

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

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

Azure Resource Application Permissions

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

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

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

Microsoft Teams Application Permissions

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

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

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

- Windows Azure Active Directory: Read all groups

Minimum Permissions for Initially Installing Enterprise Reporter

During your first installation, when you install the Enterprise Reporter server, there are two sets of credentials that you need to supply, as well as optional SQL credentials. This table outlines what the credentials are used for, and what permissions they require.

Table 10. Credential Use and Required Permissions

Credentials	Used For	Permissions Needed
Logged in user	Installing the components of Enterprise Reporter	Administrator access on the local computer.
	Creating the Enterprise Reporter database, roles and logins on the SQL Server® (unless SQL credentials are provided)	Must have the right to create databases, logins and groups.
	Creating the security groups	Depends on the type of groups that are chosen, but must have the right to create groups in the chosen environment.
	Securing the Configuration Manager and the Report Manager. The logged in user is added to the Reporter_Discovery_Admins, Reporter_Reporting_Admins, Reporter_Reporting_Operators, and Reporter_Discovery_Nodes security groups as an administrator for both consoles when installing the server.	
Service Account Supplied during installation	Installing and running the Enterprise Reporter server	Login as service right is conferred on the service account by the logged in credentials during installation.
	Connecting to the Enterprise Reporter database (unless SQL permissions are provided)	Read and write permissions are automatically granted during database creation.
	Securing the Configuration Manager and Report Manager. The service account is automatically added to the Reporter_Discovery_Admins, Reporter_Reporting_Admins, Reporter_Reporting_Operators, and Reporter_Discovery_Nodes security groups when installing the server.	

Table 10. Credential Use and Required Permissions

Credentials	Used For	Permissions Needed
Optional SQL credentials	Can be used to create the Enterprise Reporter database	Must have the right to create databases, logins and groups.
Supplied during installation	If supplied, are used to connect the database by the Enterprise Reporter server.	Read and write permissions are automatically granted during database creation.

Port Requirements

For the Enterprise Reporter components to communicate, some ports must be open.

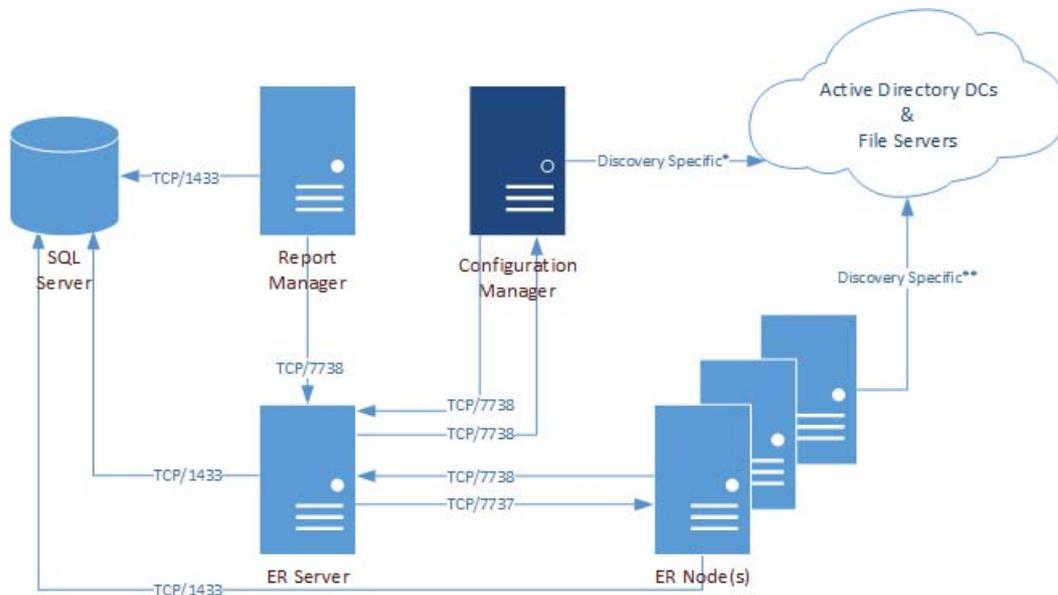
- The default port used for communication between the server and the consoles is 7738. This port is also used by the nodes to access the server. The port is configured during installation of the server, and is required in the connection dialog box for both the Configuration Manager and the Report Manager.

You can view the port currently in use on the System | Information page in the Configuration Manager, and the System Information tab in the Report Manager.

- The default port used for communication from the Enterprise Reporter server to the nodes is port 7737. This port may be configured during installation.

This figure outlines the ports used by the Enterprise Reporter components.

Figure 3. Ports used by Enterprise Reporter components.



*For more information on ports used when creating a discovery, see [Table 11](#).

**For more information on ports used during data collections, see [Table 12](#).

This table outlines the ports used by all of the Enterprise Reporter components.

Table 11. Ports used by Enterprise Reporter components

Application	Port	Type	Components				
			Configuration Manager ^a	Report Manager	SQL Server	ER Server	ER Nodes
FTP	20, 21	TCP		X			
SMTP	25	TCP	X	X		X	
WINS / NetBIOS Name Resolution	42	TCP UDP					X
DNS FQDN Resolution	53	TCP UDP	X	X		X	
Kerberos	88	TCP UDP	X				X
RPC Service & Endpoint Mapper / WMI	135	TCP UDP	X				
NetBIOS Name Service	137	UDP					X
NetBIOS Datagram (browsing)	138	UDP	X				
LDAP	389	TCP UDP	X				
SQL	1433	TCP		X	X	X	X
SQL Server Browser Service	1434	TCP UDP	X	X			
Enterprise Reporter Node	7737	TCP				X	X
Enterprise Reporter Server	7738	TCP	X	X		X	X

a. For the Configuration Manager, also include the ports listed in [Table 12](#).

This table outlines the ports used by all of the Enterprise Reporter discoveries.

Table 12. Ports used by Enterprise Reporter discoveries

Application	Port	Type	Discoveries										
			Active Directory	Azure Active Directory	Azure Resource	Computer	Exchange	Exchange Online	File Storage Analysis	NTFS	OneDrive	Registry	SQL Server
WINS / NetBIOS Name Resolution	42	TCP UDP	X			X	X		X	X		X	X
DNS FQDN Resolution	53	TCP UDP	X			X	X		X	X		X	X
HTTP	80	TCP		X	X		X*	X				X	X
Kerberos	88	TCP UDP	X			X	X*		X	X		X	X
RPC Service & Endpoint Mapper / WMI	135	TCP UDP				X	X**		X	X		X	X
NetBIOS Name Service	137	UDP	X			X	X		X	X		X	X
Remote Registry	139	TCP				X	X		X	X		X	
ICMP						X			X	X		X	X
LDAP	389	TCP UDP	X			X	X		X	X		X	X
HTTPS	443	TCP UDP		X	X							X	X
SMB / Remote Registry	445	TCP	X			X			X	X		X	X
LDAP Secure	636	TCP	X										
DCOM on XP/2003 and below (uses an open port in this range)	1024 - 5000	TCP UDP				X	X		X	X			X
SQL	1433	TCP	X	X	X	X	X	X	X	X	X	X	X
SQL Server Browser Service	1434	UDP											X
LDAP GC	3268	TCP	X				X						
WinRM	5985 5986	TCP UDP						X					X
Exchange PowerShell	12067	TCP					X**						
DCOM on Vista/2008 and above (uses an open port in this range)	49152 - 65535	TCP UDP				X	X		X	X			X

*Exchange 2010 and higher, **Exchange 2007 only

The following figures outline the ports used by the Enterprise Reporter discoveries.

Figure 4. Ports used by Active Directory collections

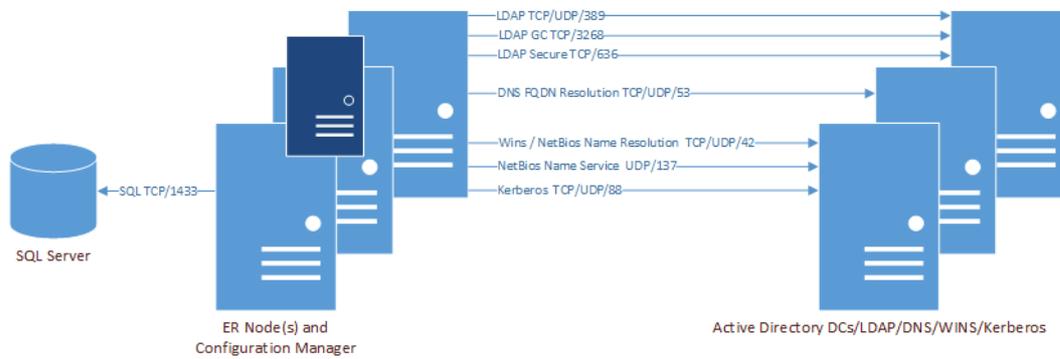


Figure 5. Ports used by Azure and Office 365 collections (Exchange Online, MS Teams, and OneDrive)

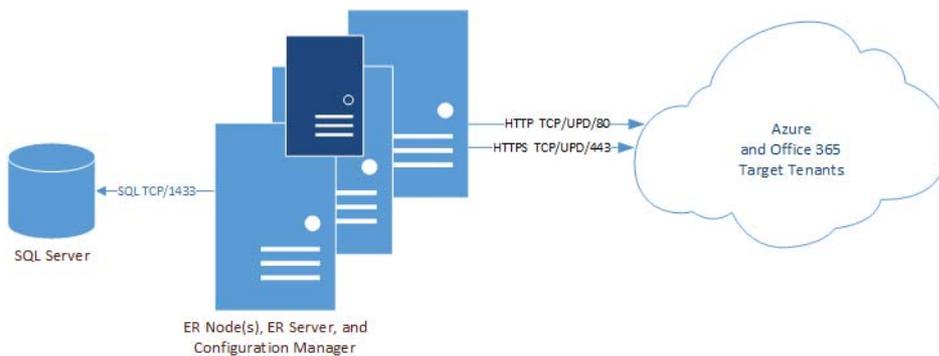


Figure 6. Ports used by Computer collections

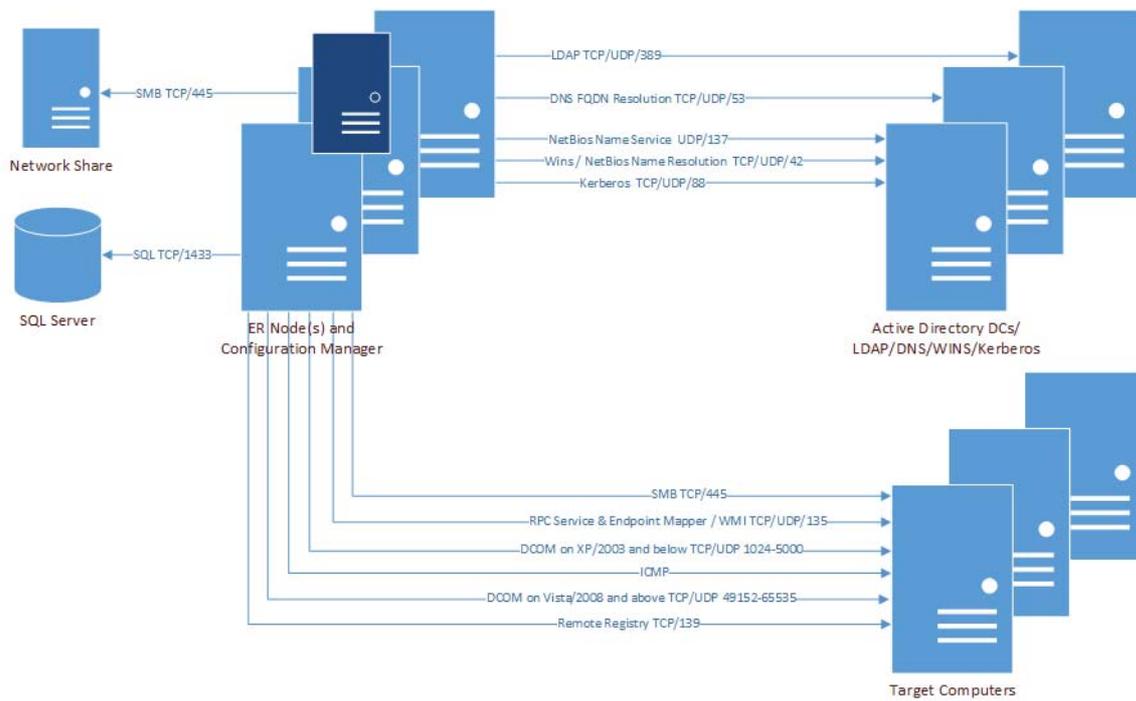


Figure 7. Ports used by Exchange collections

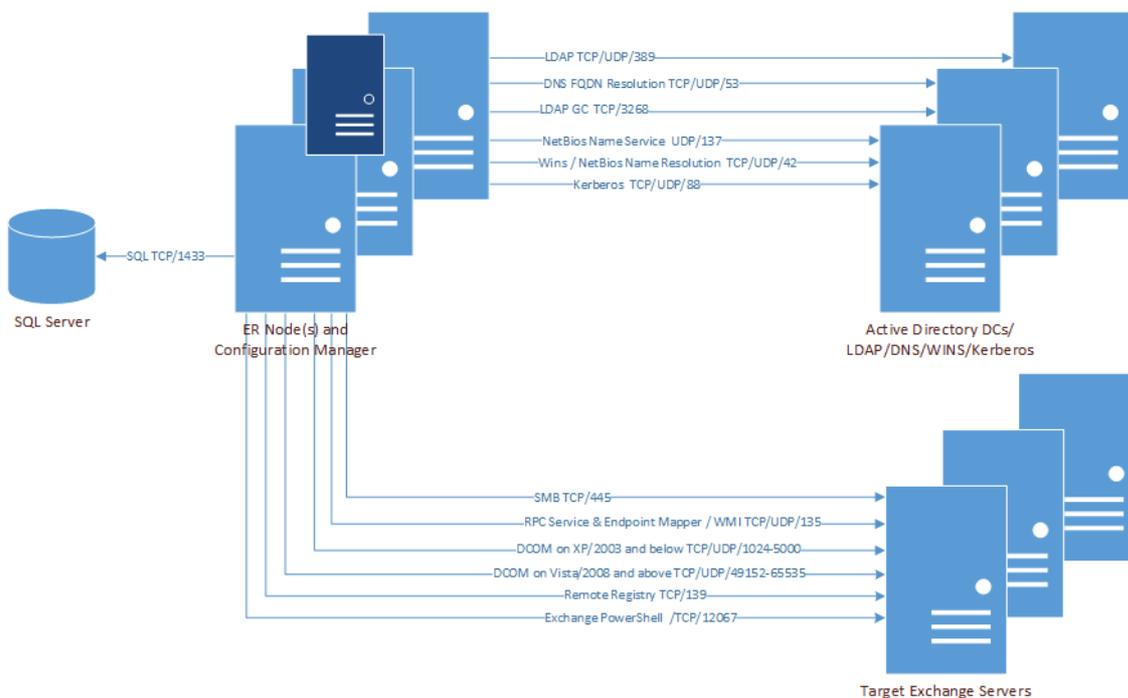


Figure 8. Ports used by File Storage Analysis collections

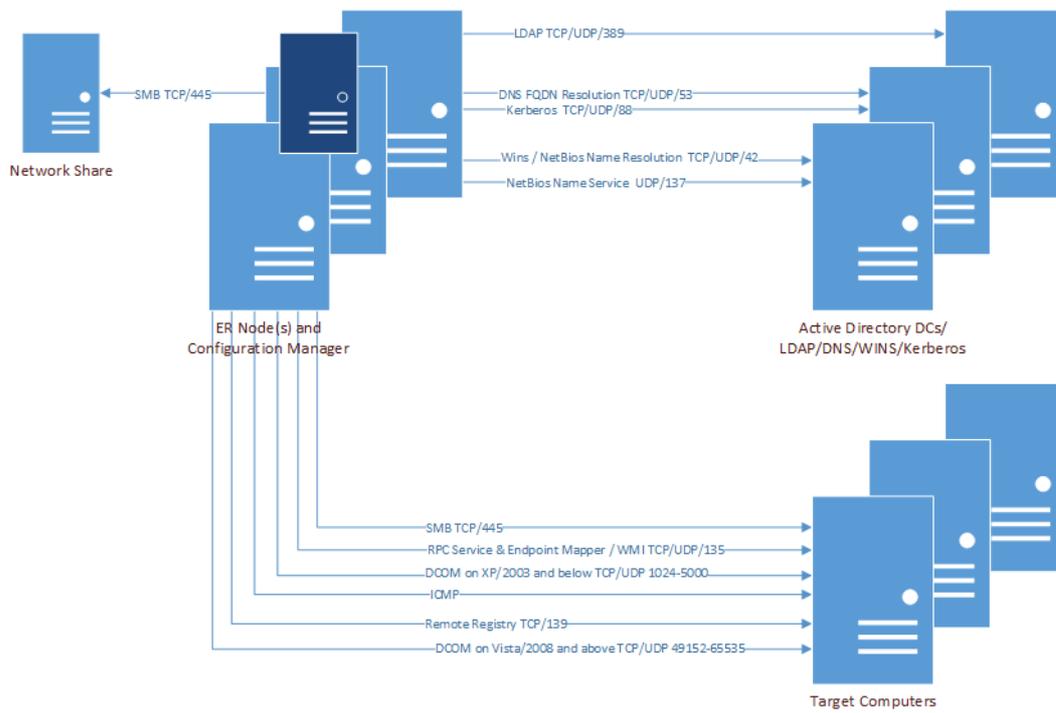


Figure 9. Ports used by NTFS collections

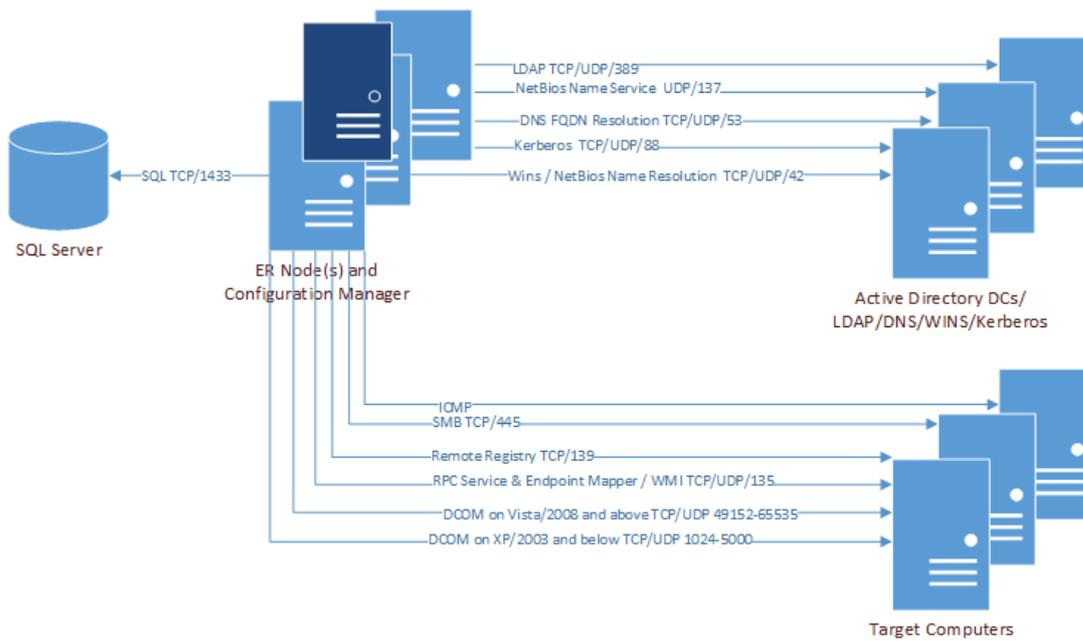


Figure 10. Ports used by Registry collections

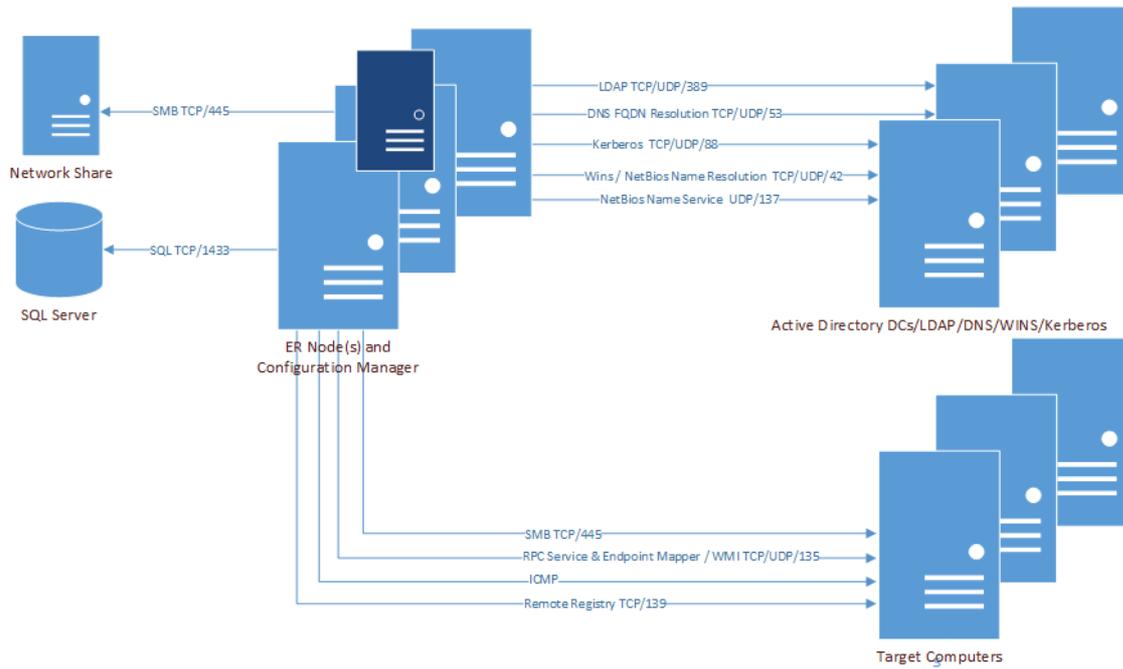
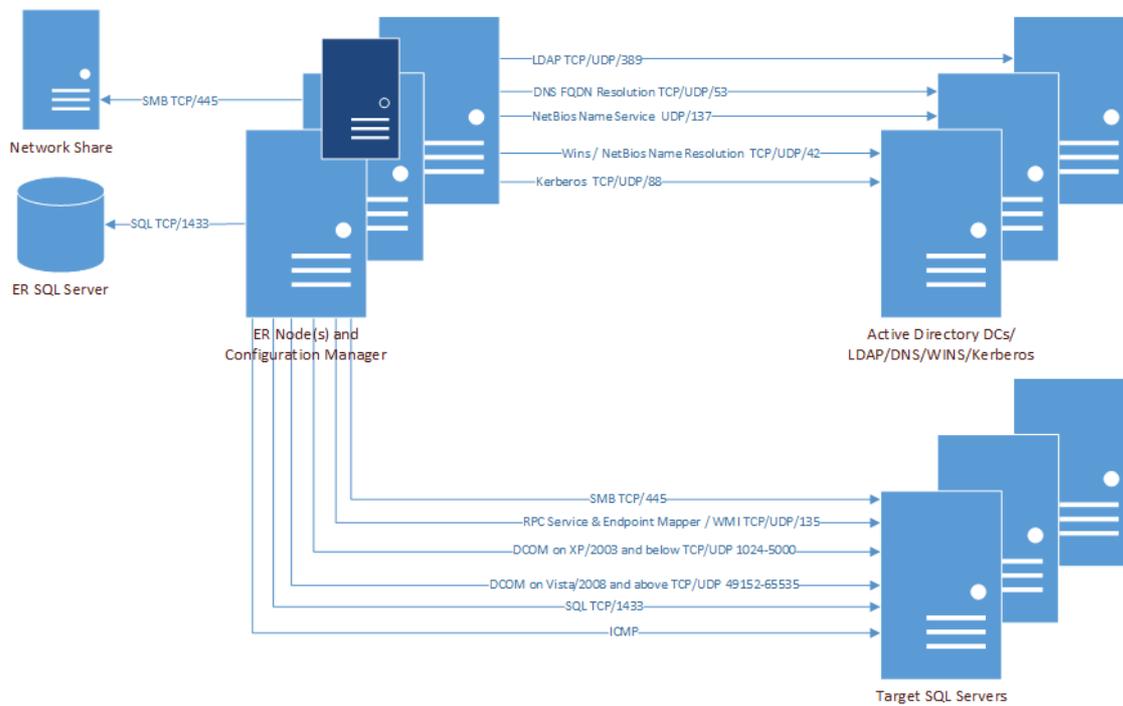


Figure 11. Ports used by SQL collections



Firewall Requirements

The following changes are required to be made to the Windows Firewall settings to allow Enterprise Reporter to return all available data during a discovery. Without these settings, the data returned during a discovery will be limited and the discovery will indicate the following error:

- The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)

Table 13. Firewall requirements for a discovery

Operating System	Firewall Requirement
Windows 2019	<p>Start Settings Network & Internet</p> <p>Select Windows Firewall</p> <p>Scroll down and select Allow an app through firewall</p> <p>Select Windows Management Instrumentation (WMI) and File and Print Sharing (if not already selected)</p> <p>The check box in the Domain column will be selected.</p> <p>Click OK.</p>
Windows 2016	<p>Start Control Panel System Security</p> <p>Select Allow an app through Windows Firewall</p> <p>Select Windows Management Instrumentation (WMI) and File and Print Sharing</p> <p>The check box in the Domain column will be selected.</p> <p>Click OK.</p>
Windows 2012 and Windows 2012 R2	<p>Start Control Panel Windows Firewall.</p> <p>Select Allow an app or feature through Windows Firewall.</p> <p>Select Windows Management Instrumentation (WMI).</p> <p>The check box in the Domain column will be selected.</p> <p>Click OK.</p>
Windows 2008 R2	<p>Start Control Panel System and Security Windows Firewall.</p> <p>Select Allow a program or feature through Windows Firewall.</p> <p>Select Windows Management Instrumentation (WMI).</p> <p>The check box in the Domain column will be selected.</p> <p>Click OK.</p>
Windows 2008	<p>Start Control Panel Windows Firewall.</p> <p>Select Allow a program through Windows Firewall.</p> <p>Select the Exceptions tab.</p> <p>Scroll down and select Windows Management Instrumentation (WMI) and click OK.</p>
Windows 2003 and Windows 2003 R2	<p>Run the following command-line context:</p> <pre>netsh firewall set service type = remotedadmin mode = enable</pre>

Table 13. Firewall requirements for a discovery

Operating System	Firewall Requirement
Windows 8, Windows 8.1, and Windows 10	<p>In the lower left hand corner of the screen right click and select Control Panel.</p> <p>Select System and Security Windows Firewall.</p> <p>Select Allow a program or feature through Windows Firewall.</p> <p>Select File and Printer Sharing and Windows Management Instrumentation (WMI).</p> <p>The checkbox in the Domain column will be selected.</p> <p>Click OK.</p> <p>Start the Remote Registry service and set it to Automatic.</p> <p>This step is required to collect data such as installed software, event logs, and security policies.</p>
Windows 7	<p>Start Control Panel System and Security Windows Firewall.</p> <p>Select Allow a program or feature through Windows Firewall.</p> <p>Select File and Printer Sharing and Windows Management Instrumentation (WMI).</p> <p>The checkbox in the Domain column will be selected.</p> <p>Click OK.</p> <p>Start the Remote Registry service and set it to Automatic.</p> <p>This step is required to collect data such as installed software, event logs, and security policies.</p>
Windows Vista	<p>Start Control Panel Security Windows Firewall.</p> <p>Select Allow a program or feature through Windows Firewall.</p> <p>Select the Exceptions tab.</p> <p>Select File and Printer Sharing and Windows Management Instrumentation (WMI).</p> <p>Click OK.</p>
Windows XP	<p>Start Control Panel Security Center Windows Firewall.</p> <p>Select the Exceptions tab.</p> <p>Select File and Printer Sharing.</p> <p>Click OK.</p>

Database Requirements

The Enterprise Reporter server requires a database to store configuration specifications and the information that will be collected from your network environment. Before you install Enterprise Reporter, determine where you will set up your database. It should reside on a SQL Server® that is accessible from the computer running the Enterprise Reporter server. For more information, see [SQL Server Supported Versions](#) on page 128.

Topics

- [Configuring the Database and Security Groups](#)

Configuring the Database and Security Groups

In order for the server to function, you must have a fully configured Enterprise Reporter database. You can either:

- Create and configure the database automatically during the installation process. Unless you have corporate reasons for not doing so, this is the recommended method. For more information, see [To create a new database during the installation process](#) on page 41.
- Use an existing Enterprise Reporter database. If the database is from a previous version of Enterprise Reporter, it will be upgraded, so ensure you back up your database before beginning. For more information, see [To use an existing Enterprise Reporter database during the initial installation](#) on page 42.

The simplest way to configure the database is to allow Enterprise Reporter to set up the database following installation. You need to know the SQL Server[®] on which you want to create the database, and you can use either Windows[®] or SQL Server[®] credentials to connect to your SQL Server[®].

- i** | **NOTE:** In order to create the database, the currently logged in account must have appropriate rights (including SysAdmin rights) on the SQL Server[®], or you must use appropriate SQL credentials.
- NOTE:** In order to upgrade the database, the currently logged in account must have db-owner rights on the SQL Server, or you must use appropriate SQL credentials.
- NOTE:** In order to create groups, the currently logged in account must be able to add groups to the domain's Users OU, and be able to add members to groups.

- If you use an existing database, you can connect to it during the installation process. You must know the database name and the SQL Server[®] where it resides.

! | **CAUTION:** Any existing database will automatically be upgraded (even if it is new and empty). Ensure you back up the database before beginning.

- If you complete the installation process without a fully functioning database, use the Database Wizard to create a new database. For more information, see [Using the Database Wizard to Create or Connect a Database](#) on page 54.

i | **NOTE:** Enterprise Reporter must have a database to fully function. If there is no database, you will receive an error message when trying to log on with the Configuration Manager.

There are parameters that you can set when creating an Enterprise Reporter database:

- You can adjust the initial size of the database or the database log file. If your database will contain a lot of collected data, increase its size. This will improve performance. Use the Database Estimator Tool for further information based on the types of collections being performed.
- You can choose where to store the database and logs by specifying file paths.

When you allow Enterprise Reporter to create the database, you also have the option to automatically create the following Domain Local security groups:

- Reporter_Discovery_Admins
- Reporter_Reporting_Admins
- Reporter_Reporting_Operators
- Reporter_Discovery_Nodes

You may optionally enter customized group names during setup. Assign names that reflect the purpose of each group to ensure clarity when group names are displayed in various system administration tools.

These groups provide access to the appropriate tables in the Enterprise Reporter database and are used to allow Windows[®] authentication on the SQL Server[®]. For more information, see [Security Groups in Enterprise Reporter](#) on page 51.

i | **NOTE:** If you enter the names of existing security groups, Enterprise Reporter will use the existing groups instead of creating new ones.

i | **NOTE:** If you choose not to allow Enterprise Reporter to create the necessary groups, the database will be created without the necessary security groups and SQL roles for Enterprise Reporter to function.

A corresponding SQL login and role is created for each group.

- For example, for the Reporter_Discovery_Admins group, a Reporter_Discovery_Admins login and a Discovery_Admin_Role are created.
 - In this example, the Reporter_Discovery_Admins will then be given the Discovery_Admin_Role. These roles will define the scope of access to Enterprise Reporter. For more information, see [Role Based Security in Enterprise Reporter](#) on page 52.

Installing and Configuring Enterprise Reporter

Topics

- [Installing Enterprise Reporter](#)
- [Installing and Configuring Individual Components](#)
- [Upgrading Enterprise Reporter](#)
- [Licensing Enterprise Reporter](#)
- [Role Based Security in Enterprise Reporter](#)
- [Managing Your Database Using the Database Wizard](#)

Installing Enterprise Reporter

Once you have determined where you will deploy Enterprise Reporter and have ensured that your computers meet the system requirements, you are ready to install the Enterprise Reporter server and consoles. During the installation process, you can choose whether to install all components on the same computer or on separate computers.

i | **NOTE:** For basic instructions on how to install all of the Enterprise Reporter components onto one server, see the Quest Enterprise Reporter Quick Start Guide in the [Technical Documentation](#).

After this initial installation process is complete, you will need to create the Enterprise Reporter database. The Enterprise Reporter database can be created and configured automatically during the installation, or can be set up later using the Enterprise Reporter Database Wizard utility.

If you have an existing Enterprise Reporter installation and are creating another database with the same version, you can transfer your Enterprise Reporter configuration information (clusters and nodes, discoveries, and reports) using the Database Content Wizard. For more information, see [Appendix: Database Content Wizard](#) on page 91.

If necessary, you can install additional consoles for other users.

- Install the Configuration Manager for all Enterprise Reporter administrators. Ensure that each administrator is added to the Reporter_Discovery_Admins group.
- Install the Report Manager for each user who is required to produce reports. Ensure that for each installation, the user is added to the Reporter_Reporting_Admins group, or the Reporter_Reporting_Operators group as appropriate.

Topics

- [Installing the Components](#)
- [Installing and Configuring the Configuration Manager](#)
- [Installing and Configuring the Report Manager](#)

Installing the Components

There are five components that you can install:

- Enterprise Reporter server
 - When this option is selected, the Database Wizard and the Encryption Key Manager will also automatically be installed.
- Configuration Manager
- Report Manager
- Database Wizard
- Log Viewer

These components can be installed as needed using a single installer.



NOTE: Installations must be done locally. You must be logged in with credentials that allow you to install software.

NOTE: If you are creating the database when you install your server, as recommended, you must have rights to create database on the SQL Server®.

NOTE: If the IE Enhanced Security Configuration setting is enabled in the Server Manager, open the MSI installer instead of the Autorun in the following procedure.

To install Enterprise Reporter components

- 1 Open the self-extracting file **Enterprise Reporter <version number>.exe**.
- 2 Select a location for the extracted files.
- 3 Open the **Autorun** file.

You can access all product documentation on the Documentation tab of the Autorun.

- 4 On the Home page, click the **Enterprise Reporter Setup** tab.
- 5 Click **Open** next to the edition of **Quest Enterprise Reporter** for your operating system (64 bit).
- 6 On the Welcome screen of the Setup Wizard, click **Next**.
- 7 Click **View License Agreement** and scroll to review the entire license agreement.
Optionally, click **Print** to send a copy of the agreement to the printer.
- 8 Select **I accept these terms to accept the agreement**, click **OK** to close the agreement, and click **Next** to continue the installation.

- OR -

Select **I do not accept these terms to reject the agreement**, click **OK** to close the agreement, and click **Cancel** to exit the installation.

- 9 To install all components, click **Next**.

- OR -

To install individual components, click the drive icon for each component, select the desired option, and click **Next**.

Clicking **Reset** restores the default setting of installing all components.

- 10 If you select the Reporter Server component without the Database Wizard component, a warning that the Database Wizard will be installed automatically is displayed. Click **Next** to continue.
- 11 If you are installing the Enterprise Reporter server, specify the credentials that will be used by the Enterprise Reporter server service, and click **Next**.

This service account must be able to access the SQL Server® where the Enterprise Reporter database resides.

12 If you are installing the Enterprise Reporter server, verify the default port of 7738 to be used for the Enterprise Reporter server, and click **Next**.

- OR -

If the default port 7738 is in use, specify an alternate port for the server, and click **Next**.

13 Click **Install**.

14 Click **Close**.

If errors were encountered during installation they are listed on this page.

15 If you have installed the server, you need to configure the database.

- OR -

If you have installed the Configuration Manager or Report Manager without the server, you must add the required user to the proper security group, or they will not be able to open the console.

For more information, see [Role Based Security in Enterprise Reporter](#) on page 52.

Technical Documentation.

Next, the Database Wizard displays automatically after you close the Enterprise Reporter server installation window. If the Quest Enterprise Reporter Database Wizard does not open automatically, you may start it manually from the Windows **Start** menu.

You may either create or connect a new database (see [To create a new database during the installation process](#) on page 41) or use an existing database (see [To use an existing Enterprise Reporter database during the initial installation](#) on page 42).

To create a new database during the installation process

1 Choose **Create New Database**, and click **Next**.

2 Enter the target SQL Server® instance.

You can either type the instance name or browse to it. If you browse, you will see all SQL Servers® in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

3 Type a name for your database.

- OR -

Type the name of the existing empty database to be connected, or browse to it.

4 Select the preferred type of authentication to use to connect to the SQL Server®, and click **Next**.

Enterprise Reporter connects to the SQL Server® using Windows® authentication by default. If you want to connect using SQL credentials, enter them before clicking **Next**.

Enterprise Reporter validates the SQL Server® and your right to create a database on the instance before you can proceed to the next step.

5 If necessary, adjust the initial database size or file paths, and click **Next**.

Use the Database Estimator tool for further information based on the types of collections being performed.

6 If required, enter the domain of the Enterprise Reporter server's service account.

7 Enter the names for the security groups, and click **Next**.

Using the default group names is recommended.

Technical Documentation.

For more information, see [Security Groups in Enterprise Reporter](#) on page 51.

8 Review the message box, and click **OK** to continue.

- OR -

Click **Cancel** to further modify the Security Group Names.

- 9 Optionally, accept the default to open Configuration Manager.

Once the database is created, you will use the Configuration Manager to enter the Enterprise Reporter licences and configure the collection of network information.

- 10 Click **Finish** to create the database.

A task progress dialog will be displayed as the database is created.

- 11 When creation is complete and successful, a notice to backup the encryption key is displayed. Click **OK** to accept the message and start the Encryption Key Manager.

i | **IMPORTANT:** It is important to backup the encryption key. The Encryption Key Manager will automatically start on the Enterprise Reporter Server. Use the **Export Key** option to create a back up file of the encryption key. For more information, see [Appendix: Encryption Key Manager](#) on page 99.

- OR -

If errors were encountered during database creation, an error dialog box displays.

[Technical Documentation.](#)

For help troubleshooting errors, see [Database Configuration Issues](#) on page 78.

To use an existing Enterprise Reporter database during the initial installation

i | **CAUTION:** If the database is from a previous version of Enterprise Reporter, it will automatically be upgraded. Ensure you back up the database and the encryption key before beginning.

- 1 Select **Select/Upgrade Existing Database** and choose **Next**.

- 2 Enter the target SQL Server®.

You can either type the SQL Server® name or browse to it. If you browse, you will see all SQL servers in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

- 3 Confirm database name.

You can type a database name, or browse to find one. Enterprise Reporter validates that the database exists, and is a valid Enterprise Reporter database. If the Browse dialog box is empty, ensure the SQL Server® is correct. Or, try using different credentials, as only databases to which the current credentials have access are shown.

- 4 Confirm which type of authentication to use to connect to the SQL Server and click **Next**.

Enterprise Reporter connects to the SQL Server® using Windows® authentication by default. If you want to connect using SQL credentials, enter them.

- 5 Confirm that you backed up the encryption key using the Encryption Key Manager, and then click **Next**.

If the database is from a previous version of Enterprise Reporter, the database automatically upgrades.

- 6 Confirm that you have created a backup of your database by selecting **I understand and wish to continue**, then click **Next**.

- 7 If required, enter or browse to the domain of the Enterprise Reporter server's service account.

- 8 Confirm or edit the names for the security groups and click **Next**.

- 9 Review the warning message and click **OK** to continue.

- OR -

Click **Cancel** to further modify the Security Group Types or the Security Group Names.

- 10 To complete the database upgrade, click **Finish**.

A task progress dialog is displayed as the database is created.

- 11 When creation is complete and successful, a notice to back up the encryption key is displayed. Click **OK** to accept the message and start the Encryption Key Manager.

i | **IMPORTANT:** It is important to back up the encryption key. The Encryption Key Manager will automatically start on the Enterprise Reporter Server. Use the **Export Key** option to create a backup file of the encryption key. For more information, see [Appendix: Encryption Key Manager](#) on page 99.

- OR -

If errors occur during an upgrade, they are detailed at the end of the process. For more information, see [Database Configuration Issues](#) on page 78.

To launch the Database Content Wizard

- 1 Click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard** and click **Next**.

- OR -

- 2 If the Database Wizard is already running, click **Launch Database Content Wizard**.

Installing and Configuring Individual Components

- [Installing and Configuring the Configuration Manager](#)
- [Installing and Configuring the Report Manager](#)
- [Installing and Configuring the Database Wizard](#)
- [Installing and Configuring the Log Viewer](#)
- [Creating a Database Prior to Enterprise Reporter Server Installation](#)
- [Installing and Configuring IT Security Search](#)
- [Installing and Configuring IT Security Search](#)

Installing and Configuring the Configuration Manager

If you only need to install the Configuration Manager, you can follow the installation steps outlined in [Installing the Components on page 40](#), and ensure that only the Configuration Manager is selected. In order to collect data with the Configuration Manager, you must first set up clusters and discoveries. For more information, see [Configuring the Configuration Manager and Creating and Managing Discoveries in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation](#).

i | **NOTE:** In order to use the Configuration Manager, the user must be in the Reporter_Discovery_Admins security group. For more information, see [Role Based Security in Enterprise Reporter](#) on page 52.

Installing and Configuring the Report Manager

If you only need to install the Report Manager, you can follow the installation steps outlined in [Installing the Components](#) on page 40, and ensure that only the Report Manager is selected.

i | **NOTE:** In order to use the Report Manager, the user must be in the Reporter_Reporting_Admins or Reporter_Reporting_Operators security group.

Installing and Configuring the Database Wizard

If you only need to install the Database Wizard, you can follow the installation steps outlined in [Installing the Components](#) on page 40, and ensure that only the Database Wizard is selected. For more information, see [Managing Your Database Using the Database Wizard](#) on page 53.

Installing and Configuring the Log Viewer

If you only need to install the Log Viewer, you can follow the installation steps outlined in [Installing the Components](#) on page 40, and ensure that only the Log Viewer is selected.

Installing and Configuring the Encryption Key Manager

The Encryption Key Manager requires no separate installation option as it is automatically installed with the Enterprise Reporter server. The Encryption Key Manager must reside on and be used on the same computer as the Enterprise Reporter server component.

Creating a Database Prior to Enterprise Reporter Server Installation

If you need to create a database prior to installing the Enterprise Reporter server, the following steps are required:

- Install the database wizard.
- Create a database using the wizard.
- Install the server and select the existing database during installation.

i | **NOTE:** Read through the following sections before beginning to determine what information you will require during setup.

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.

To create a database and then install a server utilizing that database

- 1 Install the database wizard following the steps in [Installing the Components](#) on page 40.
Ensure that only the Database Wizard component is selected.
- 2 Create the database or connect to an existing database using the wizard. For detailed steps, see [Using the Database Wizard to Create or Connect a Database](#) on page 54

- 3 On the computer where the Enterprise Reporter server will reside, install the Enterprise Reporter server using the existing database. For detailed instructions, see [To use an existing Enterprise Reporter database during the initial installation](#) on page 42

Ensure that only the Enterprise Reporter Server component is selected as outlined in [Installing the Components](#) on page 40.

Installing and Configuring IT Security Search

IT Security Search is a cross-product searching platform. Once it is configured in your environment, you set up System Configuration to push collected data from Enterprise Reporter to the IT Security Search repository. To be able to push collected data to the repository, the database account must have db-owner rights to the Enterprise Reporter database. For information on installing and configuring IT Security Search, see the [IT Security Search documentation](#) in your download package or CD.

Upgrading Enterprise Reporter

The following sections outline how to upgrade Enterprise Reporter.

- [Preparing to Upgrade Enterprise Reporter](#)
- [Upgrading Enterprise Reporter Components](#)
- [Upgrading Enterprise Reporter Nodes](#)
- [Upgrading Manually-Configured Enterprise Reporter Nodes](#)

Preparing to Upgrade Enterprise Reporter

There are four components that you can upgrade: the Enterprise Reporter server, the Configuration Manager, the Report Manager, and the Database Wizard. All components of Enterprise Reporter must be upgraded before it can function correctly and can be upgraded using a single installer.

Prior to upgrading the components, all Enterprise Reporter components must be shut down. While the upgrade is in progress, data collection will stop and no reports will run. Be sure to plan the timing of the upgrade accordingly and inform your users that they will be able to resume reporting once the upgrade is complete.

The system, permission, and port requirements for an upgrade are the same as those for installing Enterprise Reporter. For more information, see [Before You Install Enterprise Reporter](#) on page 10

! **CAUTION:** It is strongly recommended that you back up your database. You can restore the backup if there are issues with the upgrade.

! **CAUTION:** If upgrading from Enterprise Reporter 3.2 or greater, it is strongly recommended to have your encryption key backup file and user-supplied password available prior to upgrading. The encryption key and password are required to decrypt credentials in the Enterprise Reporter Credential Manager during the upgrade. If the encryption key backup file and user-supplied password are unavailable, all passwords must be re-entered in the Enterprise Reporter Credential manager.

i **NOTE:** During the upgrade to version 3.2.2, all Exchange Online data that was stored prior to the upgrade will be removed.

In summary, to upgrade Enterprise Reporter, you must:

- Shut down the Enterprise Reporter server, the Configuration Manager, the Report Manager, and the Database Wizard.
- 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.
- Cancel any report jobs running or scheduled to prevent Report Manager from accessing the database.
- Create a backup of the database.

! **CAUTION:** It is strongly recommended that you back up your database and the encryption key. You can restore the backup if there are issues with the upgrade.

- Note the port number being used by the Enterprise Reporter server.
 - Upgrade the Enterprise Reporter components.
 - Upgrade the nodes.
 - If there are any manually configured nodes, upgrade them manually.
- i** **NOTE:** When upgrading to version 3.2.2, the person performing the upgrade must have permissions to update group membership. A new security role for Reporter_Discovery_Nodes will be created and all node service accounts will be added as members of this group. For nodes to be installed and upgraded the service account must be a member of the group Reporter_Discovery_Nodes.
- Enable any disabled clusters to resume discoveries.

Upgrading Enterprise Reporter Components

There are four components that you can upgrade: the Enterprise Reporter server, the Configuration Manager, the Report Manager, and the Database Wizard. These can be upgraded using a single installer. Prior to upgrading the components, all Enterprise Reporter components must be shut down.

i **NOTE:** Upgrades must be done locally. You must be logged in with credentials that allow you to install software.

i **NOTE:** When you are upgrading the Enterprise Reporter database, you must have db_owner rights to modify the database on the SQL Server. For more information, see [To create a new database during the installation process](#) on page 41.

To prepare to upgrade all Enterprise Reporter components

- 1 Open Configuration Manager.
- 2 Under Discovery Management, click **Manage Discoveries** and stop any running Discoveries.
- 3 Under Discovery Management, click **Manage Discovery Clusters**.
- 4 Disable any Clusters.
The Nodes associated with the Clusters will also be disabled when you disable the Clusters.
- 5 Select the **Discovery Nodes** tab, then select all nodes and click **Stop Node** and wait for the nodes to stop.
- 6 Open Report Manager and confirm that there are no scheduled reports running.
If any reports are running, either cancel them or wait until they complete.
- 7 Close the Configuration Manager and the Report Manager.
- 8 Shut down the Enterprise Reporter server.

To upgrade all Enterprise Reporter components except Nodes

- 1 Run **Autorun.exe**.
- OR -
If necessary, right-click on Autorun.exe and select **Run as administrator**.
- 2 On the Home page, click the **Enterprise Reporter Setup** tab.
- 3 Start the Enterprise Reporter installer for your operating system (64 bit).

- 4 On the Welcome screen of the Setup Wizard, click **Next**.
- 5 Accept the license agreement and click **Next**.
- 6 To upgrade all components, click **Next**.
- OR -
To upgrade select components, click the drive icon for each component, and select the desired option, then click **Next**.
Clicking Reset restores the default setting of installing all components.
- 7 If you are upgrading the Enterprise Reporter server, specify the credentials and the port number to be used by the Enterprise Reporter Server service, then click **Next**.

This service account must be able to access the SQL Server® where the Enterprise Reporter database resides.
- 8 Select your country to determine your customer feedback program status, and click **Next**.
- 9 If you are not currently participating in the customer feedback program and would like to, click **Yes** and then click **Next**.
- OR -
Click **Next**.
- 10 Click **Install**.
- 11 Click **Close** and the Database Wizard will start.
For the next steps, see [To upgrade an Enterprise Reporter database on page 47](#).

The Enterprise Reporter database must be the same version as the Enterprise Reporter server before data collection and reporting can resume. If you decide you do not want to upgrade the database right now, you can use the Database Wizard at any time. For more information, see [Upgrading a Database on page 55](#).

To upgrade an Enterprise Reporter database

! **CAUTION:** It is recommended that you back up your Enterprise Reporter database and encryption key before beginning this process. You cannot undo this operation once it has started.

i **NOTE:** Once an upgrade has started, all connections to the database will be closed and the database will be unavailable until the upgrade completes successfully.

- 1 If you are starting the Database Wizard from the Start menu, click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard** and click **Next**.
- OR -
If the Database Wizard is already running, skip this step.
- 2 Choose **Select/Upgrade Existing Database** and click **Next**.
- 3 Enter the target SQL Server®.

You can either type the SQL Server® name or browse to it. If you browse, you will see all SQL Servers® in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.
- 4 Confirm database name.

You can type a database name, or browse to find one. Enterprise Reporter validates that the database exists, and is a valid Enterprise Reporter database. If the Browse dialog box is empty, ensure the SQL Server® is correct. Or, try using different credentials, as only databases to which the current credentials have access are shown.
- 5 Confirm which type of authentication to use to connect to the SQL Server® and click **Next**.

Enterprise Reporter connects to the SQL Server® using Windows® authentication by default. If you want to connect using SQL credentials, enter them.

- 6 Confirm that you backed up the encryption key using the Encryption Key Manager, and then click **Next**.
If the database is from a previous version of Enterprise Reporter, the database automatically upgrades.
- 7 Confirm that you have created a backup of your database by selecting **I understand and wish to continue**, then click **Next**.
- 8 If the Domain Local security group type was not selected during the creation of the existing Enterprise Reporter Database, you will be asked to confirm that you wish to continue with the original security group type.

Using the Domain Local group type is recommended. For more information on security groups, see [Security Groups in Enterprise Reporter](#) on page 51.
- 9 If required, enter or browse to the domain of the Enterprise Reporter server's service account.
- 10 Confirm or edit the names for the security groups and click **Next**.
- 11 Review the warning message and click **OK** to continue.
- OR -
Click **Cancel** to further modify the Security Group Types or the Security Group Names.
- 12 To complete the database upgrade, click **Finish**.

If errors occur during an upgrade, they are detailed at the end of the process. For more information, see [Database Configuration Issues](#) on page 78.

A task progress dialog is displayed during the upgrade process.
- 13 When the upgrade completes successfully, click **OK** to open the Encryption Key manager.
- 14 Select the **Export Key** option to create an encryption key backup file. For more information, see [Exporting a Key File](#) on page 100.
- OR -
Select the **Import Key** option to import an encryption key backup file. For more information, see [Importing a Key File](#) on page 100.

Upgrading Enterprise Reporter Nodes

Enterprise Reporter nodes must be the same version as the Enterprise Reporter server. Nodes can be upgraded in groups or individually.

i | **NOTE:** Nodes that were configured manually must have credentials updated manually before they can be upgraded. For more information, see [Upgrading Manually-Configured Enterprise Reporter Nodes](#) on page 49.

To upgrade Enterprise Reporter nodes

- 1 Open the Configuration Manager.
- 2 To display the nodes, select **Manage Discovery Clusters** and click the **Discovery Nodes** tab.

All nodes with versions that are out of sync with the Enterprise Reporter server will display a status of Incompatible Version.

i | **NOTE:** Nodes may only be upgraded if the node service account is a member of the group Reporter_Discovery_Nodes. The upgrade process will attempt to add all node service accounts to this group. If this attempt is unsuccessful, the account must be added manually for a successful node upgrade.
- 3 If nodes are stopped, click **Restart node**.

- 4 Select the nodes you want to upgrade and click the **Upgrade Node** icon.

The status of the node will change to Upgrading. Once the Nodes have been updated, their statuses will change to Enabled and any Cluster associated with the Nodes will also become enabled.

Upgrading Manually-Configured Enterprise Reporter Nodes

Nodes that were configured manually must have credentials updated manually before they can be upgraded.

To upgrade Enterprise Reporter manually-configured nodes

- 1 Open the Configuration Manager.
- 2 To display the nodes, select **Manage Discovery Clusters** and click the **Discovery Nodes** tab.
Nodes requiring the manual entry of credentials before upgrade will display 'Manually configured' in the Service Account column and will display 'Incompatible Version' in the Status column.
- 3 Select the manually-configured node you want to upgrade and click the **Node Properties** icon.
- 4 To open the Credentials Manager, click the ellipsis.

For detailed instructions Modifying Node Credentials in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

- 5 To accept the updated credentials, click **OK**.
- 6 Select this node and click the **Upgrade Node** icon.

The status of the node will change to Upgrading.

If the node upgrade does not complete successfully, see Node Deployment Issues the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

After Upgrading Enterprise Reporter

After upgrading Enterprise Reporter, open the Configuration Manager to see an overview of What's New and any new discovery configuration features that may need to be updated manually. Validate your current cluster, node, and discovery configurations.

Licensing Enterprise Reporter

You need either a trial or full license to use Enterprise Reporter. You must have a valid license to use the Configuration Manager; no license is required for the Report Manager. If you have questions about your license, contact your sales representative.

Topics

- [Activating or Updating Your License](#)

Table 14. Enterprise Reporter Licenses

Enterprise Reporter License	Discovery Types Available with License	Report Libraries Available with License
Enterprise Reporter for Windows Servers	<ul style="list-style-type: none"> • NTFS • Computer • Registry • OneDrive • Azure Resource 	<ul style="list-style-type: none"> • NTFS • Computer • Registry • Office 365 OneDrive • Change History • Hybrid • Azure Resources
Enterprise Reporter for Active Directory	<ul style="list-style-type: none"> • Active Directory • Azure Active Directory 	<ul style="list-style-type: none"> • Active Directory • Azure • Change History • Hybrid
Enterprise Reporter for SQL Server	<ul style="list-style-type: none"> • MS SQL 	<ul style="list-style-type: none"> • Microsoft SQL Server • Change History
Enterprise Reporter for File Storage Analysis	<ul style="list-style-type: none"> • File Storage Analysis 	<ul style="list-style-type: none"> • File Storage Analysis
Enterprise Reporter for Exchange	<ul style="list-style-type: none"> • Exchange • Exchange Online 	<ul style="list-style-type: none"> • Exchange • Office 365 Exchange Online • Hybrid
Enterprise Reporter for Office 365	<ul style="list-style-type: none"> • Exchange Online • Azure Active Directory • Azure Resource • OneDrive • Microsoft Teams 	<ul style="list-style-type: none"> • Office 365 Exchange Online • Azure • Office 365 OneDrive • Office 365 Microsoft Teams
Enterprise Reporter Suite	<ul style="list-style-type: none"> • Active Directory • Azure Active Directory • Azure Resource • Computer • File Storage Analysis • Exchange • Exchange Online • Microsoft Teams • MS SQL • NTFS • OneDrive • Registry 	<ul style="list-style-type: none"> • Active Directory • Azure • Change History • Computer • Exchange • File Storage Analysis • Hybrid • Microsoft SQL Server • NTFS • Office 365 Exchange Online • Office 365 Microsoft Teams • Office 365 OneDrive • Registry • Security Explorer Remediation

Activating or Updating Your License

Activate or update your license in the Configuration Manager on the System | Information page.

To activate your license

- 1 Install and open the Configuration Manager.
- 2 Connect to your Enterprise Reporter server.
If no license has been installed, the licensing dialog box appears.
- 3 Click **Update License** and navigate to your license file.
- 4 Click **Open**.
- 5 In the licensing dialog box, click **OK**.

To view or update your license

- 1 Open the Configuration Manager.
- 2 Select **System | Information** and click **View licensing information**.
- OR -
Click the **Information** icon on the right-hand side of the Quest header and select the **Licenses** tab.
- 3 To view the license details of a feature, select a feature and click **Details**, then click **OK** to close the license details window.
- 4 Optionally, to update the license of a feature, select the feature, click **Update License**, locate the license file, select it, and click **Open**.
- 5 Click **OK** to close the About Quest Enterprise Reporter dialog box.

Security Groups in Enterprise Reporter

When installing Enterprise Reporter 3.2.2 for the first time, if you let Enterprise Reporter create the database and security groups, the security group type is automatically set to Domain Local.

If an earlier version of Enterprise Reporter was previously installed, or if the security groups were created manually, the existing security groups may not be Domain Local groups. You can determine the security group type chosen when Enterprise Reporter was originally deployed on the System | Information page.

If the existing groups are not Domain Local groups, during install or upgrade, you will be given the option to keep them or to configure new security group types (recommended).

The following table outlines each supported choice:

Table 15. Security Group Types

Security type	Location of group	Who you can add to the group
Domain Local (recommended)	Added to the domain Users OU The groups are given the appropriate SQL roles	A domain local group can have the following members: user accounts, groups with universal scope, and groups with global scope — all from any domain. If users are in multiple domains, this type of group is required.
Global	Added to the domain Users OU The groups are given the appropriate SQL roles	A domain global group can have the following members: accounts from the same domain and other groups with global scope from the same domain. If all users are in the same domain, this type of group may be used.

Your choice will impact the following options:

- Determine where the groups will be created, and what type of groups they are — Active Directory® objects (Domain Local and Global groups).
- Determine who in your environment can be added to the groups (and therefore who can access Enterprise Reporter).
- The account being used to create the database will be added to the security groups, thus giving this account full access to Enterprise Reporter.

i | **NOTE:** In order to create groups, the currently logged in account must have appropriate rights for the type of groups you are creating. If you are creating Domain Local or Global groups, you must be able to add users to the domain Users OU, and add members to groups.

Role Based Security in Enterprise Reporter

The data collected and reported on by Enterprise Reporter can contain sensitive information about your environment. To ensure that only appropriate users can access this information, each console has role based security.

i | **NOTE:** During installation, the logged in user is added to the Reporter_Discovery_Admins group, the Reporter_Discovery_Nodes group, and the Reporter_Reporting_Admins group. The Enterprise Reporter server service account is added to the Reporter_Discovery_Admins group and Reporter_Discovery_Nodes group.

i | **NOTE:** Each security group name may be customized during installation. The security group names for your system are displayed on the Configuration Manager System | Information page.

In order to be able to open a console, the user must be assigned to one of the security groups. Four security groups are created when the Enterprise Reporter server is installed, and four are associated with SQL roles:

Table 16. Security Group and SQL Role Permissions

Security Group	SQL Role	Permissions
Reporter_Discovery_Admins	Discovery_Admin_Role (also known as discovery administrator)	<ul style="list-style-type: none">• Access to all functionality in the Configuration Manager
Reporter_Reporting_Operators	Reporting_Operator_Role (also known as reporting user)	<ul style="list-style-type: none">• Run published reports• Copy published reports to My Reports.• Create and edit reports in My Reports container• Export report definitions from Published Reports and My Reports• Import report definitions into My Reports• Manage the My Reports container (move, copy, create categories)

Table 16. Security Group and SQL Role Permissions

Security Group	SQL Role	Permissions
Reporter_Reporting_Admins	Reporting_Admin_Role (also known as reporting administrator)	<ul style="list-style-type: none"> • All reporting user functionality • Paste or import reports into the Published Reports container • Publish to Knowledge Portal • Run reports from the Report Library • Export report definitions and copy from the Report Library • View all reporting users' schedules, edit the properties of the schedule, or delete it
Reporter_Discovery_Nodes	Discovery_Nodes_Role	<ul style="list-style-type: none"> • Deployment of node • Upgrade of node • Access to all functionality on the Enterprise Reporter Node

To add a user or group to a security role

- Determine if your security groups are domain groups by checking the System | Information page.
 - To add an account to the discovery administrator role, use system-provided tools to add the user to the Reporter_Discovery_Admins group.
 - To add an account to the reporting administrator role, use system-provided tools to add the user to the Reporter_Reporting_Admins group.
 - To add an account to the reporting user role, use system-provided tools to add the user to the Reporter_Reporting_Operators group.
 - To add an account to the discovery node role, use system-provided tools to add the user to the Reporter_Discovery_Nodes group.

For more information, see the Microsoft® documentation for your operating system.

Managing Your Database Using the Database Wizard

By default, the Database Wizard is installed on the same computer where the server is installed. You can also install it on a separate computer if needed. For more information, see [Installing the Components](#) on page 40. Using the Database Wizard, you can:

- Create a new database. This gives you the option to create a new database or to connect to an existing empty database. You may then select this database during subsequent server installations.
- Select or Upgrade an Enterprise Reporter database. You can use this to change the database or server that you want to use, to change the type of authentication you are using, or to change the SQL credentials.

When you select a database, it is automatically upgraded if it is not the same version as the server.

CAUTION: It is recommended that you back up your database and encryption key before upgrading it, or before changing to a different database, as this may trigger an upgrade. You cannot undo an upgrade once it has started.

- Remove an Enterprise Reporter database. You can use this to remove an unused database from the SQL Server®.

- Change the SQL Server® security mode. You can choose to change the acceptable method of authentication for the SQL Server®.
- Perform database maintenance. You can use this to perform consistency checks, reset identity columns or rebuild database indexes.

Topics

- [Using the Database Wizard to Create or Connect a Database](#)
- [Upgrading a Database](#)
- [Deleting a Database](#)
- [Changing the Security Mode](#)
- [Changing the Connection to the Enterprise Reporter Database](#)

Using the Database Wizard to Create or Connect a Database

The Database Wizard is used to create or connect an Enterprise Reporter database. You can either create the database when the wizard is automatically launched after installing the Enterprise Reporter server, or launch the wizard as a stand-alone application.

i | **NOTE:** The Database Wizard is installed with the Enterprise Reporter server by default.

To create a database using the Database Wizard

i | **NOTE:** If you use the Database Wizard on the same computer as the Enterprise Reporter server, when the database creation is complete, the Enterprise Reporter server service is restarted, and the server will be connected to the new database. If you create the database on a different computer, you must change the database to which you are connected. See [Changing the Connection to the Enterprise Reporter Database](#) on page 58.

- Click the **Start** menu, and select **All Programs|Quest|Enterprise Reporter|Database Wizard** and click **Next**.
- 1 Choose **Create New Database**, and click **Next**.
- 2 Enter the target SQL Server® instance.

You can either type the instance name or browse to it. If you browse, you will see all SQL Servers® in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.
- 3 Type a name for your database.

- OR -

Type the name of the existing empty database to be connected, or browse to it.
- 4 Select the preferred type of authentication to use to connect to the SQL Server®, and click **Next**.

Enterprise Reporter connects to the SQL Server® using Windows® authentication by default. If you want to connect using SQL credentials, enter them before clicking **Next**.

Enterprise Reporter validates the SQL Server® and your right to create a database on the instance before you can proceed to the next step.
- 5 If necessary, adjust the initial database size or file paths, and click **Next**.

Use the Database Estimator tool for further information based on the types of collections being performed.
- 6 If required, enter the domain of the Enterprise Reporter server's service account.

- 7 Enter the names for the security groups, and click **Next**.

Using the default group names is recommended.

[Technical Documentation](#).

For more information, see [Security Groups in Enterprise Reporter](#) on page 51.

- 8 Review the message box, and click **OK** to continue.

- OR -

Click **Cancel** to further modify the Security Group Names.

- 9 Optionally, accept the default to open Configuration Manager.

Once the database is created, you will use the Configuration Manager to enter the Enterprise Reporter licences and configure the collection of network information.

- 10 Click **Finish** to create the database.

A task progress dialog will be displayed as the database is created.

- 11 When creation is complete and successful, a notice to backup the encryption key is displayed. Click **OK** to accept the message and start the Encryption Key Manager.

i | **IMPORTANT:** It is important to backup the encryption key. The Encryption Key Manager will automatically start on the Enterprise Reporter Server. Use the **Export Key** option to create a back up file of the encryption key. For more information, see [Appendix: Encryption Key Manager](#) on page 99.

- OR -

If errors were encountered during database creation, an error dialog box displays.

[Technical Documentation](#).

For help troubleshooting errors, see [Database Configuration Issues](#) on page 78.

- 12 Click **Cancel**.

Upgrading a Database

The Enterprise Reporter database must be the same version as the Enterprise Reporter server. You can use the Database Wizard to upgrade your database outside of the installation process.

To upgrade an Enterprise Reporter database

i | **CAUTION:** It is recommended that you back up your Enterprise Reporter database and encryption key before beginning this process. You cannot undo this operation once it has started.

i | **NOTE:** Once an upgrade has started, all connections to the database will be closed and the database will be unavailable until the upgrade completes successfully.

- 1 If you are starting the Database Wizard from the Start menu, click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard** and click **Next**.

- OR -

If the Database Wizard is already running, skip this step.

- 2 Choose **Select/Upgrade Existing Database** and click **Next**.

- 3 Enter the target SQL Server®.

You can either type the SQL Server® name or browse to it. If you browse, you will see all SQL Servers® in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

4 Confirm database name.

You can type a database name, or browse to find one. Enterprise Reporter validates that the database exists, and is a valid Enterprise Reporter database. If the Browse dialog box is empty, ensure the SQL Server® is correct. Or, try using different credentials, as only databases to which the current credentials have access are shown.

5 Confirm which type of authentication to use to connect to the SQL Server® and click **Next**.

Enterprise Reporter connects to the SQL Server® using Windows® authentication by default. If you want to connect using SQL credentials, enter them.

6 Confirm that you backed up the encryption key using the Encryption Key Manager, and then click **Next**.

If the database is from a previous version of Enterprise Reporter, the database automatically upgrades.

7 Confirm that you have created a backup of your database by selecting **I understand and wish to continue**, then click **Next**.

8 If the Domain Local security group type was not selected during the creation of the existing Enterprise Reporter Database, you will be asked to confirm that you wish to continue with the original security group type.

Using the Domain Local group type is recommended. For more information on security groups, see [Security Groups in Enterprise Reporter](#) on page 51.

9 If required, enter or browse to the domain of the Enterprise Reporter server's service account.

10 Confirm or edit the names for the security groups and click **Next**.

11 Review the warning message and click **OK** to continue.

- OR -

Click **Cancel** to further modify the Security Group Types or the Security Group Names.

12 To complete the database upgrade, click **Finish**.

If errors occur during an upgrade, they are detailed at the end of the process. For more information, see [Database Configuration Issues](#) on page 78.

A task progress dialog is displayed during the upgrade process.

13 When the upgrade completes successfully, click **OK** to open the Encryption Key manager.

14 Select the **Export Key** option to create an encryption key backup file. For more information, see [Exporting a Key File](#) on page 100.

- OR -

Select the **Import Key** option to import an encryption key backup file. For more information, see [Importing a Key File](#) on page 100.

Deleting a Database

If you no longer want an Enterprise Reporter database, you can use the Database Wizard to remove it from the SQL Server®. You must have rights to remove a database.

i **TIP:** It is recommended that you do not delete the database currently in use by the server. If you delete the current database, the Enterprise Reporter server service cannot start, and you will be unable to open the Configuration Manager or the Report Manager. This option is intended for deletion of Enterprise Reporter databases no longer in use.

To delete a database using the Database Wizard

- 1 Click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard**.
- 2 Click **Next**.
- 3 Select **Remove Database**.
- 4 Enter the SQL Server[®] where the database is stored.

You can either type the SQL Server[®] name or browse to it. If you browse, you will see all SQL servers in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

- 5 Enter or browse to the database to remove and click **Next**.

Enterprise Reporter uses the stored connection settings to connect to the SQL Server[®]. If you want to change the type of authentication or the SQL credentials, enter them before clicking Next.

Enterprise Reporter validates the SQL Server[®] and your right to remove a database on it before you can proceed to the next step.

- 6 Click **Finish** to remove the database.

Changing the Security Mode

You can use the Database Wizard to change the security mode of the SQL Server[®] where your database resides. SQL servers can use either Windows[®] authentication (Integrated mode), or Windows[®] and SQL authentication (Mixed mode). Changing the security mode may grant access to additional groups and revoke access from already configured groups, so you should exercise caution with this option.

- i** | **NOTE:** If you change the security mode, it affects all databases on the SQL Server[®], not just the Enterprise Reporter database. You must have adequate rights on the SQL Server[®] to make this change.
- If you change the security mode to Windows[®], any service configured to connect to the SQL Server[®] using SQL authentication will fail.

To change the security mode of the SQL Server[®]

- 1 Click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard**.
- 2 Click **Next**.
- 3 Select **Change Security Mode** and click **Next**.
- 4 Enter the target SQL Server[®].

You can either type the SQL Server[®] name or browse to it. If you browse, you will see all SQL Servers[®] in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

- 5 Confirm database name.

You can type a database name, or browse to find one. Enterprise Reporter validates that the database exists, and is a valid Enterprise Reporter database. If the Browse dialog box is empty, ensure the SQL Server[®] is correct. Or, try using different credentials, as only databases to which the current credentials have access are shown.

- 6 Confirm which type of authentication to use to connect to the SQL Server[®] and click **Next**.

Enterprise Reporter connects to the SQL Server[®] using Windows[®] authentication by default. If you want to connect using SQL credentials, enter them.

- 7 Change to the desired mode, and click **Next**.

- 8 Click **Finish** to change the security mode.

i | **NOTE:** You must restart the SQL Server® service for this change to take effect.

Changing the Connection to the Enterprise Reporter Database

Using the Select/Upgrade Existing Database option, you can:

- Switch to a different Enterprise Reporter database. The database must be properly configured as outlined in [Configuring the Database and Security Groups](#) on page 36. The database will be automatically upgraded if required, so ensure you back up before using this option.
- Switch to a different server. This is useful if you have moved your database.
 - i** | **NOTE:** If you are moving your database to a different server, you should undeploy your nodes first, move the database, and then redeploy the nodes. For more information, see [To change and save database connection information](#) on page 58.
- Change the credentials you are using to access the database. You can switch between Windows® (which uses the currently logged in credentials) and SQL. You can enter or update the SQL credentials as necessary.
- Upgrade your database to a newer version of Enterprise Reporter. For more information, see [Upgrading a Database](#) on page 55.

i | **NOTE:** It is recommended to complete the above actions on the computer running the Enterprise Reporter Service.

To change and save database connection information

- 1 On the computer hosting the Enterprise Reporter server, click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard**.
- 2 Click **Next**.
- 3 Choose **Select/Upgrade Existing Database**, and click **Next**.
The Establish Connection page is populated with your existing database and server.
- 4 If desired, change the SQL Server® or database name.
- 5 If desired, change the authentication type, and provide a user name and password if necessary.
- 6 If desired, change security groups.
- 7 Click **OK** to accept the message.
- 8 Click **Next**.
- 9 Click **Finish** to close the wizard.
- 10 When the database has been selected successfully, click **OK** to open the Encryption Key manager.
- 11 Select the **Export Key** option to create an encryption key backup file. For more information, see [Exporting a Key File](#) on page 100.

- OR -

Select the **Import Key** option to import an encryption key backup file. For more information, see [Importing a Key File](#) on page 100.

Performing Database Maintenance

Using the Perform Database Maintenance option, you can perform consistency checks, reset identity columns, or rebuild indexes.

Before performing database maintenance

- 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.
- Cancel any report jobs running or scheduled to prevent Report Manager from using the database.
- Create a backup of the database.
 - ! **CAUTION:** It is strongly recommended that you back up your database. You can restore the backup if there are issues with the upgrade.
- Stop the Quest Enterprise Reporter Server service.
- Close the Configuration Manager and Report Manager on all computers.

To perform database maintenance

! **CAUTION:** It is recommended that you backup your Enterprise Reporter database before beginning this process. You cannot undo this operation once it has started.

- 1 Complete all steps in the procedure [Before performing database maintenance](#) on page 59.
- 2 On the computer hosting the Enterprise Reporter server, click the **Start** menu and select **All Programs|Quest|Enterprise Reporter|Database Wizard**.
- 3 Click **Next**.
- 4 Choose **Perform Database Maintenance**, and click **Next**.
The Establish Connection page is populated with your existing database and server.
- 5 If desired, change the SQL Server® or database name.
- 6 If desired, change the authentication type, and provide a user name and password if necessary.
- 7 Click **Next**.
- 8 Select the database maintenance options to perform, and click **Next**.
- 9 Click **Finish** to complete the request and close the wizard.

Managing Your Enterprise Reporter Deployment

Topics

- [Optimizing Enterprise Reporter](#)
- [Enterprise Reporter Server and Database Considerations](#)
- [Cluster Deployment Considerations](#)
- [Discovery Considerations](#)

Optimizing Enterprise Reporter

Enterprise Reporter is very scalable. Properly planning and managing the system is important to ensure that your data is collected as quickly and effectively as possible. There are many ways to improve the performance of your deployment.

Topics

- [Enterprise Reporter Server and Database Considerations](#)
- [Cluster Deployment Considerations](#)
- [Discovery Considerations](#)

Enterprise Reporter Server and Database Considerations

You need to choose a host computer for Enterprise Reporter server and a SQL Server[®] to host the Enterprise Reporter database. Your decision will affect the performance of the product.

The Enterprise Reporter server communicates directly with the database frequently. Locate the Enterprise Reporter server physically close to the SQL Server[®] for best results.

The nodes also regularly connect to the database. The more nodes you have in your deployment, and the more discoveries you run, the greater the impact on the SQL Server[®]. Choose a SQL Server[®] with enough power to manage the connections and data transfer from the nodes. Check your Microsoft[®] SQL Server[®] documentation for more information on system requirements.

Enterprise Reporter supports a variety of SQL configurations. You can use a regular SQL instance, a SQL cluster, or a mirrored database. If your SQL deployment supports it, using clusters or mirrors allows for automatic failover recovery in the event that a SQL Server[®] is down.

Topics

- [Failover Recovery using SQL Clusters](#)

Failover Recovery using SQL Clusters

Using a SQL cluster instead of a single server allows for automatic failover recovery in the event that a SQL Server® is down. Tasks are automatically passed to another SQL Server®. Your cluster can be configured with Always On.

Cluster Deployment Considerations

The following sections can help you get the most out of Enterprise Reporter:

- [Consider the Data to Collect Before Deploying Nodes](#)
- [Fine Tune Each Cluster and Node](#)
- [Optimize Node Setup](#)
- [Plan Credential Use](#)
- [Effectively Deploy Remote Nodes](#)
- [Optimize Data Transfer](#)

Consider the Data to Collect Before Deploying Nodes

There is a relationship between the design of your discoveries and the physical deployment of your clusters and nodes. By understanding what you want to collect, and what network and hardware resources you have available, you can deploy Enterprise Reporter in a way that makes sense for your environment. When you create a discovery, you assign it to a cluster. The actual work of the collection can be done by any node in the cluster, load balanced by the Enterprise Reporter server. This means that each node should:

- Be physically close to the targets in the discoveries you intend to assign to the cluster
- Use credentials that can access most or all of the targets

You may not have this insight before you start using Enterprise Reporter, however you can modify your deployment at any time. If you are creating a discovery with targets that are not near the nodes of any of your clusters, consider creating a new cluster to support this.

Topics

- [Optimize Node Setup](#)

Fine Tune Each Cluster and Node

A discovery is resolved to a number of tasks. Each task is then automatically assigned to a node in the cluster by the server, depending on the node's availability. If you are collecting from many targets at the same time, you can increase performance by adding more nodes to the cluster and by ensuring that each node is configured to allow the node to optimize how many concurrent tasks it can process (by setting the maximum number of concurrent tasks to a value of zero).

You can see the amount of time it took to run each instance of the discovery in the history view. If you drill down, you can see how the time was distributed across the targets, and what node did the processing. This information can aid in your decisions about how to scale up your deployment.

Adding nodes and optimizing concurrent tasks can only speed things up if there are multiple tasks to assign to the node. When a large amount of data is collected from an individual target, only one task will be created. In that case, you can improve performance by increasing the CPU, the available disk space, and the memory of the node host computer, or by looking at other factors, such as network latency.

The discovery type determines what the targets are and helps you decide on your options for speeding up collections. Clusters that handle large targets will benefit from increasing the CPU, available disk space and memory of the node host computers, or being dedicated to a smaller number of discoveries. The following table outlines how each discovery type is broken down into tasks:

Table 17. Discovery Types

Discovery Type	Task Breakdown
Active Directory®	Each domain, or per object type by domain
Azure Active Directory	Each tenant
Azure Resource	Each tenant
Computer	Each computer
Exchange®	The Exchange Organization, or per object type, or per object type per server
Exchange Online™	The Office 365 tenant
File Server Analysis	Each computer
Microsoft SQL	Each computer
Microsoft Teams	Each tenant
NTFS	Each computer or per share by computer
OneDrive	Each tenant
Registry	Each computer

Topics

- [Optimize Node Setup](#)

Optimize Node Setup

Two of the most common questions are, “What nodes do I deploy?” and, “What computer specifications do I need?” To determine the answers to these questions, we typically look at the following criteria.

- 1 What discoveries need to be run? (Active Directory, NTFS, Office 365, and so on)

Each discovery has its own performance influences and setup considerations as outlined by the tables in this section.

- 2 How many objects need to be collected for each discovery?

The number of objects determines whether the setup should accommodate a small, medium, or large collection as outlined by the tables in this section.

- 3 Where are the objects located across the network?

The location of the objects impacts the setup of each type of discovery differently as outlined by the tables in this section.

The following sections outline considerations when optimizing node setup for each type of discovery.

Active Directory Discoveries: Node Setup

Active Directory collections are sequential and create heavy network traffic as they query the domain controller so the network connection to the domain controller is the primary concern. Locating the node close to the domain controller is recommended. Choose a domain controller close to your node when you configure the discovery. For more information, see Choosing your Active Directory® Scopes in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

The CPU benchmarks of the node computer affect the threading capability so it is a secondary concern.

Typically, an organization with one domain only needs one node. Additional nodes usually only help optimize concurrent collection when there are multiple domains.

Table 18. Node Considerations for Active Directory Discoveries

# Objects	Performance Influences				# Nodes Needed	Discovery Settings
	Network Bandwidth	RAM	Disk Speed	CPU		
Small < 100K 1 domain	Primary Concern	No Concern	No Concern	Secondary Concern	1	
Medium 100K - 500K 1 domain	Primary Concern	No Concern	No Concern	Secondary Concern	1	
Large 500K - 1M 1 domain	Primary Concern	No Concern	No Concern	Secondary Concern	1	<ul style="list-style-type: none"> •break single discoveries by object type •use one discovery per object type combined with schedules

Azure Active Directory and Azure Resource Discoveries: Node Setup

Azure Active Directory collections are sequential and create heavy network traffic as they query Azure. Ensuring the node machine has optimal network bandwidth is the primary concern. The CPU benchmarks of the node computer affect the threading capability, so it is a secondary concern. Typically, an organization with one tenant only needs one node.

Table 19. Node Considerations for Azure Active Directory and Azure Resource Discoveries

# Objects	Performance Influences				# Nodes Needed
	Network Bandwidth	RAM	Disk Speed	CPU	
Small < 100K 1 tenant	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1
Medium 100K - 500K 1 tenant	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1
Large 500K - 1M 1 tenant	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1

Computer Discoveries: Node Setup

Computer collections are sequential and create heavy network traffic as they query each local computer. Ensuring the node machine has optimal network bandwidth is the primary concern.

Table 20. Node Considerations for Computer Discoveries

# Objects	Performance Influences				# Nodes Needed
	Network Bandwidth	RAM	Disk Speed	CPU	
Small < 5K	Primary Concern	No Concern	Secondary Concern	Tertiary Concern	1 - 3
Medium 5K - 10K	Primary Concern	No Concern	Secondary Concern	Tertiary Concern	3 - 8
Large > 10K	Primary Concern	No Concern	Secondary Concern	Tertiary Concern	8 - 10

File Storage Analysis Discoveries: Node Setup

Table 21. Node Considerations for File Storage Analysis Discoveries

# Targets	# Files / Computer	Performance Influences				# Nodes Needed
		Network Bandwidth	RAM	Disk Speed	CPU	
Small 1 - 10 Computers	< 2M	Primary Concern	Secondary Concern	No Concern	Secondary Concern	1 - 3
Medium 1 - 10 Computers	< 20M	Primary Concern	Secondary Concern	No Concern	Secondary Concern	3 - 9
Large > 10 Computers	> 20M	Primary Concern	Secondary Concern	No Concern	Secondary Concern	10

Microsoft SQL Discoveries: Node Setup

Table 22. Node Considerations for Microsoft SQL Discoveries

# SQL Servers	Performance Influences				# Nodes Needed
	Network Bandwidth	RAM	Disk Speed	CPU	
Small 1 - 3	Primary Concern	Tertiary Concern	Secondary Concern	No Concern	1
Medium 3 - 5	Secondary Concern	Primary Concern	Tertiary Concern	No Concern	2
Large > 5	Secondary Concern	Primary Concern	Tertiary Concern	No Concern	> 3

NTFS Discoveries: Node Setup

The most important guideline is to collect only the information required. For example, most files have inherited permissions so, typically, collecting folder permissions is sufficient.

By default, NTFS discoveries, will create multiple tasks (one task per share) to improve performance. If disk speed is slow, network bandwidth is low, or there is only one node, disable this performance option.

Table 23. Node Considerations for NTFS Discoveries

# Objects	Performance Influences				# Nodes Needed	Discovery Settings
	Network Bandwidth	RAM	Disk Speed	CPU		
Small 0 - 5M	Secondary Concern	Tertiary Concern	Primary Concern	No Concern	1 - 3	
Medium 5M - 100M	Secondary Concern	Tertiary Concern	Primary Concern	No Concern	3 - 6	
Large 100M - 1B multiple shares	Secondary Concern	Tertiary Concern	Primary Concern	No Concern	6 - 10 ^a	•use multiple tasks option unless slow disk speed, low network bandwidth, or one node

a.It is recommended to deploy 10 nodes or less.

Office 365 Discoveries: Node Setup

These considerations apply to Exchange Online, Microsoft Teams, and OneDrive discoveries.

OneDrive can be divided into multiple discoveries to increase collection speed. If Microsoft throttling is often an issue, the use of multiple credentials can help minimize throttling.

Table 24. Node Considerations for Office 365 Discoveries

# Objects	Performance Influences				# Nodes Needed
	Network Bandwidth	RAM	Disk Speed	CPU	
Small	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1
Medium	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1
Large	Primary Concern	No Concern	Tertiary Concern	Secondary Concern	1

Plan Credential Use

There is granular control over the credentials that are used to perform various functions in Enterprise Reporter. For more information, see [Role Based Security in Enterprise Reporter on page 52](#) and An Overview of the Configuration Manager Security in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

Topics

- [Logged In User Details](#)
- [Understanding Credentials Using Scenarios](#)

Logged In User Details

You can use as many or as few credentials as you need. Many of the credentials used in Enterprise Reporter are stored in the Credential Manager, which makes it easy to replace or update credentials across your environment.

Credentials for the Configuration Manager are stored in a single Credential Manager, shared by all Configuration Manager users. If only certain employees know the passwords or are responsible for certain credentials, such as service credentials, one of those employees can add the credentials to the Credential Manager, and then all Enterprise Reporter administrators can use them.

Credentials in the Credential Manager are used in the following ways in the Configuration Manager:

- Running the node service.
- Accessing the Enterprise Reporter server and database from the node. You can use either a Windows® or a SQL account.
- Accessing the targets of a discovery to collect data.
- Accessing the shared data location of a cluster, if used.

Each Report Manager user has their own Credential Manager. Credentials in the Credential Manager are used in the following ways in the Report Manager:

- Delivering scheduled reports to a share.
- Configuring an SMTP server for email delivery.
- Publishing reports to Knowledge Portal.

The logged in user is used for:

- Logging into both consoles.
- Connecting to the Enterprise Reporter server (Configuration Manager and Report Manager).
- Connecting to the Enterprise Reporter database (Configuration Manager and Report Manager).
- Browsing the targets of a discovery.

Understanding Credentials Using Scenarios

The following scenarios outline how credentials can be used in different environments:

- [Minimizing the Number of Credentials Used by Enterprise Reporter](#)
- [Minimizing the Permissions Required for Credentials Used by Enterprise Reporter](#)

Minimizing the Number of Credentials Used by Enterprise Reporter

If you have a simple deployment, you can permission two sets of credentials to perform all functions. In this scenario, you have a single Enterprise Reporter administrator, who manages installation, discoveries, and reporting. The following table outlines the required permissions:

Table 25. Required Permissions

Account	Use	Permissions
Administrator's user account Use these credentials to log in to the computer, and to schedule reports.	Launch consoles	Be a member of Reporter_Discovery_Admins and Reporter_Reporting_Admins groups
	Enumerate scopes	Read access to all discovery targets
	Deliver reports by email	Access to the SMTP server
	Enumerate report delivery shares and deliver reports	Read and write access to the delivery share
Service credentials Use these credentials for the Enterprise Reporter server and all nodes.	Use the shared data location, if configured for a cluster	Read and write access to the share
	Writing to the database	Be a member of Reporter_Discovery_Nodes group
	Collect data	Be a local administrator on all computer targets, and have read access to targeted domains, SQL servers, NTFS objects

Minimizing the Permissions Required for Credentials Used by Enterprise Reporter

A complex deployment may require some thought to determine what credentials you want to use in different situations. With effort, you can minimize the permissions you must add to accounts to use Enterprise Reporter. Keep in mind that some of the data collected is available only to privileged accounts. In most cases, accounts with inadequate privileges can collect partial data.

For this scenario:

- You have several large domains, each with its own Enterprise Reporter administrator. Trusts exist between all domains.
- There is one report administrator for the whole deployment.
- Each domain has a dedicated cluster with a shared data location.
- Each domain has a set of service credentials for use by the nodes.
- Discoveries use alternate credentials specific to the targets.
- SQL credentials are used to access the Enterprise Reporter database.

For each domain you need:

Table 26. Permissions Required

Account	Use	Permissions
Service credential Use these credentials for the Enterprise Reporter server and all nodes.	Enterprise Reporter server service	Local administrator access to the server host. Use the credentials from the domain in which the server is hosted
	Node service	Local administrator access to the node host
	Shared Data Location for each cluster	Read and write access to the share

Table 26. Permissions Required

Account	Use	Permissions
Administrator's user account Use these credentials to log in to the computer running the Configuration Manager.	Launch console	Be a member of Reporter_Discovery_Admins group

You also need:

Table 27. Additional Permissions Required

Account	Use	Permissions
SQL Account When creating the database or modify using the Database Wizard	Communication between the server and database Logging in to the Report Manager Communication between the node and the database	Read and write access to the database
Report Administrator account	Log in to the Report Manager Deliver reports by email Enumerate report delivery shares and deliver reports	Must be a member of the Reporter_Reporting_Admins group Access to the SMTP server Read and write access to the delivery share

For browsing to your discovery targets and collecting the data you can choose the credentials that make sense for your environment. Set these credentials at the discovery level. For example:

- For Active Directory® discoveries, you could use a domain admin account that has access to the targeted domain.
- For computer accounts, you could either use existing accounts with local administrator access, or set up specific accounts for groups of similar computers.

i | NOTE: The Credential Manager allows the owner of the credentials to enter the password. Other administrators can then use the credentials as appropriate.

- For more information about credentials required to collect data with Enterprise Reporter discoveries, see [Detailed Permissions for Enterprise Reporter Discoveries](#) on page 23.
- For more information about credentials required to collect data from Azure, Azure Active Directory, Azure Resource, Exchange Online, Microsoft Teams, and OneDrive, see [Permissions for Enterprise Reporter Tenant Applications](#) on page 25.

Effectively Deploy Remote Nodes

You can deploy nodes from the Configuration Manager or manually. When you are deploying a node to a remote computer, factors such as firewall configuration and network latency can cause problems. In this case, you can deploy a node manually on the host computer. For more information, see [Node Deployment Issues](#) on page 82.

Deploying a Node to a Trusted Domain

When deploying a node to a trusted domain, the remote domain must trust the domain where the Enterprise Reporter Server is installed because the account that runs the node service has to authenticate to the Enterprise Reporter Server.

We strongly recommend deploying the Enterprise Reporter Node software on a computer that is local to the discovery targets - in this case, in the remote domain.

The Enterprise Reporter Service Account requires Local Administrator access to the remote node computers to deploy the node using the Configuration Manager.

The Enterprise Reporter Node service account has the following requirements.

- It must be from the same domain as the Enterprise Reporter Server service account.
- It requires sufficient rights to the Enterprise Reporter database (member of the Reporter_Discovery_Nodes group is sufficient).
- It requires Local Administrator rights on the node computer.

When deploying a node to a trusted domain, the port requirements are the same as when deploying a node to a local domain. For more information, see [Port Requirements](#) on page 28.

Optimize Data Transfer

When you run a discovery for the first time, all of the data is collected and written to the database. For subsequent runs, only the changes are written. Determining the changes requires some processing, and you can choose the data source against which to compare the new data. You have two choices, and you may need to experiment to find the best setting for each cluster:

- Compare to a local copy of the data

The shared data location is a network share, used by all nodes in the cluster. When data is collected, a copy of the data is stored in the shared data location. Subsequent runs of the discovery are compared to this data, and once the comparison is complete, only changes are sent to the SQL Server®. This reduces traffic across the network and load on your SQL Server®.

i | **NOTE:** Not all discovery types utilize the shared data location. For example, Active Directory®, Exchange™, and NTFS, do not use the shared data location to optimize on the number of collection tasks generated to collect the data in a more efficient manner.

- Compare to the main database

For subsequent runs of a discovery, the comparison can be made directly against the Enterprise Reporter database, instead of the shared data location. This can be faster if the node is physically close to your SQL Server®, or if the SQL Server® is lightly loaded.

Discovery Considerations

The following sections can help you get the most out of Enterprise Reporter:

- [Divide Discovery Targets According to Cluster Structure](#)
- [Collect Only the Data Needed](#)
- [Plan Discovery and Reporting Schedules](#)
- [Optimize Nested Group Membership Collection](#)

Divide Discovery Targets According to Cluster Structure

Clusters contain the nodes that actually collect data from the targets of the discovery. The closer your nodes are to your targets, the faster the collection will be. Because Enterprise Reporter is scalable, you can modify your

deployment at any time to suit your needs. Consider these approaches for ensuring effective target distribution across your deployment:

- If you have a full understanding of your data collection needs, design your clusters and nodes to fit. For example, if the bulk of your collection targets are located in your head office, and you only have small collections in other areas, you could create a large cluster in your head office, and a single node cluster in each of the areas where other collections occur.
- If you know where some of your targets are, but not the amount of data that will be collected, start by creating a single cluster in the major geographical areas and then when creating discoveries, group targets accordingly. For example, create a small cluster in each network branch, and when discoveries are created, group the targets and assign the cluster accordingly. You can scale up your cluster at any time if the nodes cannot keep up to the data collection.
- Grow your deployment on demand. Create a single node cluster for your first collection. As your discoveries grow, scale this cluster up for targets in the same geographical location, or add new clusters when targets become physically removed from your node.

Collect Only the Data Needed

When you configure a discovery, you choose both the scope of the discovery, and what you want to collect from each target. If you know what the data is going to be used for, you can collect only the needed data. If you are not sure, and performance is an issue, consider collecting a minimal set of data, and then wait for requests for more data before extending the discovery.

When scoping your discovery, consider:

- If you add OUs and Domains as your scope in an NTFS, computer or registry discovery, all relevant objects within these containers will be collected. This has the advantage of capturing changes within the containers, but the disadvantage of potentially collecting information that is of little interest. You may want to break up large discoveries into smaller, more focused discoveries.
- Ensure that each target computer is in only one discovery of each type. For example, a computer can be in a Computer discovery and an NTFS discovery, but not in two different NTFS discoveries.
- Collect only the files, folders, and registry keys that you know are required for your reporting users.

Once you have carefully selected your scopes, consider what you need to collect from each target. The following table outlines the collection options for each type of discovery:

Table 28. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
Active Directory®	<ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> ▪ Token groups count ▪ Domain controller last logon ▪ Remote desktop information for domain users ▪ Photographs for domain users • Groups and Members <ul style="list-style-type: none"> ▪ Members from foreign domains ▪ Nested groups and their members from foreign domains • Computers (Active Directory® objects) • Domain Controllers • Permissions • Contacts • Trusts • Sites • Deleted objects • Service Accounts • Active Roles Virtual Attributes
Azure Active Directory	<ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> ▪ Additional attributes from Office 365 ▪ Multi-factor authentication attributes ▪ Users flagged for risk • Contacts • Devices • Groups <ul style="list-style-type: none"> ▪ Additional attributes from Office 365' • Roles • Applications and Service Principals
Azure Resource	<ul style="list-style-type: none"> • Subscriptions (all or specific) • Resources <ul style="list-style-type: none"> ▪ Virtual machines ▪ Disks ▪ Networking ▪ Storage Accounts • Access control <ul style="list-style-type: none"> ▪ Nested group members

Table 28. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
Computer	<ul style="list-style-type: none"> • Printers • Shares • Volumes • Accounts • Installed Software • Microsoft Store Applications • Hotfixes • Policies • Services • Event Log Configuration • Extended WMI Entities • Nested group members
Exchange	<ul style="list-style-type: none"> • Mailboxes <ul style="list-style-type: none"> ▪ Mailbox subfolders ▪ Mailbox delegates <ul style="list-style-type: none"> ▫ Include system delegates • Mail-Enabled Users • Mail Contacts • Public Folders <ul style="list-style-type: none"> ▪ System public folders • Distribution Groups • Permissions <ul style="list-style-type: none"> ▪ Mailbox AD permissions ▪ Mailbox Exchange permissions ▪ Mailbox folder permissions ▪ Public folder permissions ▪ Optionally, only explicit permissions • Nested group members

Table 28. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
Exchange Online	<ul style="list-style-type: none"> • Mailboxes <ul style="list-style-type: none"> ▪ Mailbox delegates ▪ Mailbox statistics ▪ Mailbox folders • Public Folders <ul style="list-style-type: none"> ▪ System Public Folders • Mail-Enabled Users • Mail Contacts • Distribution Groups <ul style="list-style-type: none"> ▪ Group members ▪ Dynamic group members • Permissions <ul style="list-style-type: none"> ▪ Mailbox folder permissions ▪ Optionally, only explicit permissions • Nested group members
File Storage Analysis	<ul style="list-style-type: none"> • Shares <ul style="list-style-type: none"> ▪ Hidden Shares ▪ Home Directories • Collect NAS using Configuration <ul style="list-style-type: none"> ▪ If unable to collect volumes then collect shares as volumes • Files • Folders <ul style="list-style-type: none"> ▪ Follow Directory Symbolic Links • Owners
Microsoft SQL	<ul style="list-style-type: none"> • Group members — either Active Directory® or computer users who are members of any groups discovered in the collection. You can also get this information through Active Directory® and Computer discoveries. For more information, see Optimize Nested Group Membership Collection on page 75.
MS Teams	<ul style="list-style-type: none"> • Channels • Files and Folders • Applications

Table 28. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
NTFS	<ul style="list-style-type: none"> • How to collect the information: <ul style="list-style-type: none"> ▪ Collect all available public shares <ul style="list-style-type: none"> ▫ Include hidden hares ▪ Collect all available volumes <ul style="list-style-type: none"> ▫ Based on your selected scope, if you are collecting against NAS devices, do you want to use specified NAS Configurations? <ul style="list-style-type: none"> - Yes - No ▪ Collect only selected shares, folders and DFS shares. Collection of all public shares or volumes will not occur. • Folder options: <ul style="list-style-type: none"> ▪ All folder levels ▪ Folder depth— determines how far into the folder structure to collect data • File options: <ul style="list-style-type: none"> ▪ Collect files and their basic details like size and attributes ▪ Collect advanced file metadata such as author and title ▪ Calculate duplicate files within the same computer • Permission options: <ul style="list-style-type: none"> ▪ Folder permissions - these should only be collected if needed by your reporting users ▪ File permissions - these should only be collected if needed by your reporting users <ul style="list-style-type: none"> ▫ Only collect and store files which have explicitly granted permissions ▪ Calculate permissions differences between folders, subfolders, and files. ▪ If a group account is found when collecting permissions, recursively collect group members. <p>Note: Group members of any groups discovered in the collection - either Active Directory® or computer users who are members of any groups discovered in the collection. You can also get this information by through Active Directory® and Computer discoveries. For more information, see Optimize Nested Group Membership Collection on page 75.</p> • Advanced options: <ul style="list-style-type: none"> ▪ Create a task per share for each computer - a collection task is created for each computer in the NTFS discovery. You can select this option to enable additional load balancing between nodes.

Table 28. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
OneDrive	<ul style="list-style-type: none">• Drives<ul style="list-style-type: none">▪ All drives▪ Selected drives• Folders<ul style="list-style-type: none">▪ Files• Permissions<ul style="list-style-type: none">▪ Nested group members• Configuration Settings
Registry	<ul style="list-style-type: none">• Registry values• Permissions and group members• Directory or computer users who are members of any groups discovered in the collection. You can also get this information through Active Directory® and Computer discoveries. For more information, see Optimize Nested Group Membership Collection on page 75.• Recursion level — determines how far into the registry structure to collect data.

Plan Discovery and Reporting Schedules

Enterprise Reporter reports on previously collected data. It is important to coordinate the discovery schedules with your reporting schedules, to ensure that the data meets the requirements of the users.

As your deployment grows in complexity, you may find value in coordinating the schedules for your discoveries in a cluster. Things to consider:

- Run your discoveries or scheduled reports at times when network traffic is low.
- Take into account the number of nodes in relation to the number of tasks that will be processed by discoveries. You should only schedule discoveries simultaneously if your deployment is capable of processing them.
- Evaluate the time it takes to run a discovery using the history view for a discovery. This can be very useful when you are trying to get the freshest data possible for a scheduled report—you can schedule to start as late as possible while still providing data for the necessary reports. You can also use this understanding to better coordinate the schedules of your discoveries to avoid overloading your nodes.

Optimize Nested Group Membership Collection

Depending on the reports that will be run, you may need to collect data to show nested group memberships. It is more efficient to collect to group members through Active Directory® discoveries than using the nested group membership options in individual discoveries of other types. This also helps avoid collecting the same accounts in multiple discoveries. The recommended practice for collecting nested group members is to:

- Collect accounts from each domain of interest (one discovery per domain, and be sure to include all other data that you need from that domain). This results in the groups and members in the domain being collected once.
- If a domain has groups with members from other domains for which you do not have separate discoveries, you should collect foreign group members to ensure complete data.

- Do not collect group members in NTFS, Registry, or MS SQL discoveries, if you will have all the information needed for reporting from the Active Directory® or Exchange® discoveries.

i | **NOTE:** If you are not running Active Directory® or Exchange® discoveries, you will need to include the nested group members in NTFS, Registry or MS SQL discoveries.

Optimize Nested Group Membership Collection for Azure and Office 365 Discoveries

Depending on the reports that will be run, you may need to collect data to show nested group memberships. It is more efficient to collect group members through the Azure Active Directory discoveries than using the nested group membership option on the Azure Resource, Exchange Online, or OneDrive discovery. This also helps to avoid collecting the same accounts in multiple discoveries.

Troubleshooting Issues with Enterprise Reporter

Topics

- [Troubleshooting Installation Issues](#)
- [Problems Opening the Consoles](#)
- [Database Configuration Issues](#)
- [Troubleshooting Connectivity Issues](#)
- [Troubleshooting Credential Change Failures](#)
- [Resolving Issues in the Configuration Manager](#)
- [Troubleshooting Features in Enterprise Reporter](#)
- [Moving the Enterprise Reporter Database](#)
- [Disaster Recovery](#)

Troubleshooting Installation Issues

Although the installation should proceed smoothly if proper credentials are used, there are some environmental and security issues to consider.

Topics

- [Connecting to a SQL Server®](#)
- [Issues with Multi-Domain Controller Environments](#)
- [Restoring a Connection to the Enterprise Reporter Server](#)
- [Database Configuration Issues](#)

Connecting to a SQL Server®

You must be able to connect to a SQL Server® in order to complete the installation. If you are attempting to connect to a server, and none appear in the browse list, try these solutions:

- Ensure the Computer Browser service is running on your computer.
- Ensure the SQL Server® is configured to receive remote connections.
- Type the SQL Server® name directly in the text box.

Issues with Multi-Domain Controller Environments

If you have multiple domain controllers, an issue can occur during the database creation. If the security groups are created on one domain controller, and another domain controller to which the roles have not yet replicated is queried, your installation may fail.

In this case, wait until all domain controllers have replicated, and then create a new database and connect to it using the Database Wizard. For more information, see [Using the Database Wizard to Create or Connect a Database](#) on page 54.

Problems Opening the Consoles

If you have UAC enabled, ensure that you have Administrator permission to open the console at an elevated level.

To open a console, you must be assigned one of the Enterprise Reporter roles.

For more information, see [Role Based Security in Enterprise Reporter](#) on page 52.

[Technical Documentation.](#)

If you are unable to log into the Configuration Manager, verify the type of groups you have selected during installation and how you are adding accounts to those groups to give them access to Enterprise Reporter.

For more information, see [Configuring the Database and Security Groups](#) on page 36.

[Technical Documentation.](#)

Database Configuration Issues

When you install the Enterprise Reporter server, you must configure your database. Occasionally, you may get errors when you perform the creation and setup of your database. The source of database configuration error message varies depending on how you attempted to create the database:

- During the installation of the server, these errors appear on the last page of the installation wizard.
- Using the database wizard, these errors appear as the wizard proceeds through the process of creating the database.
- To aid with troubleshooting, errors generated during database configuration are also written to the following log file: `\ProgramData\Quest\Enterprise_Reporter\DatabaseMaintenance.log`

When you are troubleshooting these installation errors, generally the cause is credential related. You can create a database using either Windows® or SQL credentials:

- Windows® credentials are those you logged in as
- SQL credentials are optionally provided when you create the database, either during installation or using the Database Wizard.

One solution is to create a new database using credentials that have the database creation right. Once the database is created, you can use the Save Connection Information option in the Database Wizard to connect to the database using your own credentials. If you have a partially created database that you want to remove from the server, you can use the Database Wizard to do this. See [Deleting a Database](#) on page 56. You may need to have an administrator with the database creation right run the Database Wizard or installer to create the database.

The following table outlines possible solutions to each error.

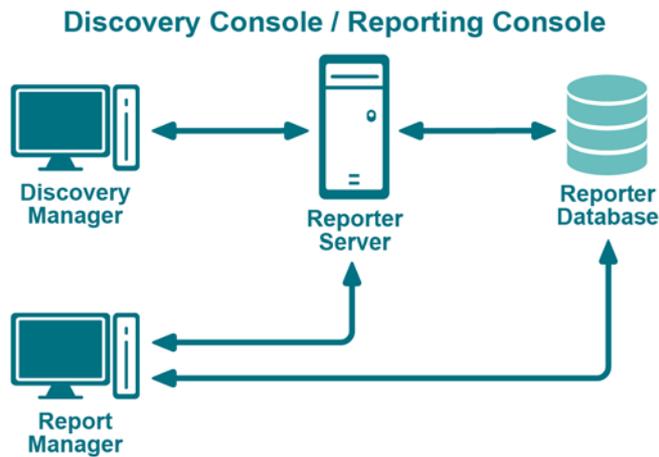
Table 29.

Error	potential causes	potential solutions
Could not create a Database	The credentials you used are not assigned the Database Creator role on the target SQL Server®.	Create a new database using the Database Wizard. For more information, see Using the Database Wizard to Create or Connect a Database on page 54. Ensure that your domain controllers have replicated, and then create a new database using the Database Wizard.
Could not create all groups	The credentials you used do not have permissions to create groups on the domain.	Have an administrator with the group creation permission run the Database wizard to remove the existing database and create a new database. For more information, see Using the Database Wizard to Create or Connect a Database on page 54.
Could not create all logins	The credentials you used do not have permissions to create logins. Groups may not exist on the domain controller to which the SQL Server® is connecting.	Verify that the groups exist on the domain. Have a SQL administrator run the Database wizard to remove the existing database and create a new database. For more information, see Using the Database Wizard to Create or Connect a Database on page 54.
Could not create all SQL roles	The credentials you used may not have SQL role creation permissions on SQL Server®.	Have a SQL administrator run the Database wizard to remove the existing database and create a new database. For more information, see Using the Database Wizard to Create or Connect a Database on page 54.
Could not add Service account to all groups	The groups may not have been created. The service account may not exist on the domain or SQL Server®. The credentials you used may not have permissions to add account to groups.	Verify that the groups and Service account exist. Have an administrator manually add the service account to the appropriate groups.
Could not start NT service	Service cannot connect to database. Problems with account used to run the service.	Verify that the service account or SQL login used by the service has permissions to read and write to the database. Verify that the service account is valid and has permissions to login as service.

Troubleshooting Connectivity Issues

Each console maintains connections to the Enterprise Reporter server and to the SQL Server® database that stores Enterprise Reporter data. A loss of either connection causes problems. [Figure 12](#) outlines the connections between the components and the server and database.

Figure 12. Connections between components and the server and database.



Topics

- [Restoring a Connection to the Enterprise Reporter Server](#)
- [Restoring a Connection to the Enterprise Reporter Database](#)

Restoring a Connection to the Enterprise Reporter Server

There are a number of reasons why a Enterprise Reporter server may be down. When a console loses its connection to the server, it becomes unusable and must be restarted. All users connected to the Enterprise Reporter server are affected. You should check the following connections:

- Ensure that the computer hosting the server is turned on and running properly.
- Ensure that the Enterprise Reporter server service is running. If necessary, restart it using the Services console.
- Ensure that you can reach the host computer over your network.
- Ensure that the server host computer meets the minimum system requirements.

If the server has gone down and been restored since you last logged in, then the next time you connect, you will be informed that the server went down. If you are the main Enterprise Reporter administrator, this allows you to be aware that your server has had issues. Intermittent failures over time may be due to instability in your network, problems on the server's host computer, or your SQL Server[®] deployment.

Restoring a Connection to the Enterprise Reporter Database

If your server has lost its connection to the database, you can still open a console and connect to the server, but functionality will be limited. You will be unable to create discoveries, run reports or modify your configuration.

Ensure that the SQL Server[®] hosting the Enterprise Reporter database is running, and that the server can access it.

The Report Manager maintains a direct connection to the SQL Server[®] database, so ensure that the console's computer can also access the SQL Server[®].

Troubleshooting Connection Timeouts

As Enterprise Reporter processes your requests, constant communication with the database is required. Depending on your network configuration, your Enterprise Reporter deployment, and the power of your SQL Server[®] host, the solution for timeout issues may vary.

You can fix timeout issues by either increasing the timeout in Enterprise Reporter, or by investigating any systemic or deployment issues. For example, perhaps your SQL Server[®] where the database is hosted is underpowered, or you have located your Enterprise Reporter server physically distant from your SQL Server[®].

There are two places in the Configuration Manager where you can control the database timeouts:

- **Server timeout**
You can increase the timeout between the server and the database. If a timeout occurs, you will see a warning dialog box, indicating that this has occurred. For information on changing the server timeout, see [Configuring Global Settings](#) in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).
- **Cluster timeout**
You can increase the timeout between the nodes in the cluster and the database. This is useful when a collection fails due to a timeout, which is indicated by an error on the Errors tab for the discovery. For more information, [Modifying a Cluster](#) in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

There are two settings for each timeout configuration:

- **Connection timeout**
This is the amount of time given to make the initial connection to the database each time communication is needed. This is less likely to need adjustment. Timeouts are more likely due to SQL Server[®] or network issues than Enterprise Reporter specific problems. However, if you continually are seeing timeout errors, try increasing this setting.
- **Command timeout**
This is the amount of time allowed for the database to process requests. If you are getting timeout error messages during data collection, increase this setting.
- **Report command timeout**
This is the amount of time allowed for report generation. If you are getting timeout errors messages during report generation, for interactive or scheduled reports, increase this setting.

Troubleshooting Credential Change Failures

Each credential in the Credential Manager has three parts—an account name, a password and an optional description—and you can change any of them. While most changes should be processed smoothly, occasionally issues in the network environment may prevent changes from being applied. When a change fails, you need to determine the reason, and then manually make the changes.

- If you have to manually change a credential on a node, you should ensure that there are no discoveries running or queued before making the change. Change the credentials using the Services console on the host computer, then restart the service. Verify that the node started in the bottom pane of the Manage Discovery Clusters page. Restart any discoveries you canceled.
- If a node fails to start after changing the credentials, ensure the credentials have local administrator access on the node host computer, and check that the credentials you provided are valid.
- If a discovery fails after changing a credential, ensure that the new credentials have read access on the targets of any discovery. Check the discovery to see if it using the default node credentials or if credentials are specified. Ensure that the credentials you provided are valid.

Resolving Issues in the Configuration Manager

The Configuration Manager is used to configure your data collection. Collecting data involves your network security, which can occasionally cause problems.

- [Node Issues](#)
- [Data Collection Issues](#)

Node Issues

- [Node Deployment Issues](#)
- [Dealing with Unassociated Nodes](#)
- [Problems Deleting a Node](#)
- [Creating a Node Debug Log File](#)

Node Deployment Issues

If something goes wrong with your node deployment, you can manually install and configure the node. When you manually install a node, it appears in the Configuration Manager as an unassociated node.

- **NOTE:** You must have administrative permissions on the node host computer to install the node.
- **NOTE:** the node service account must be a member of the Reporter_Discovery_Nodes group for node deployment.

To manually install a node

- 1 If applicable, remove the node in the Configuration Manager.

For more information, see the "What does the status of a node or cluster indicate?" section in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

If necessary, use the Control Panel to uninstall the node.

- 2 Locate the node installer, Enterprise ReporterNode 3.2.2.xxxxx x64.msi (where xxxxx is a unique 5-digit code), in the Quest\Enterprise Reporter\Server folder in the install location.

- **NOTE:** If you are installing the node on a remote computer, copy the appropriate Enterprise ReporterNode 3.2.2.xxxxx x64.msi file to that computer.

- 3 Run the node installer.

For more information about the service credentials required by the node, see the Discovery Credential(Alternate Credential) Details chapter in the Quest Enterprise Reporter Configuration Manager User Guide in the [Technical Documentation](#).

When the node is installed, associate it with a cluster. For more information, see [Dealing with Unassociated Nodes on page 82](#).

Dealing with Unassociated Nodes

An unassociated node is one that has been either manually installed, or left behind from a previous installation of Reporter. You can either uninstall the node, or associate the node with a cluster.

To uninstall a node

- Use the Control Panel, and uninstall Quest Enterprise Reporter Node.

To associate a node with a cluster

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 In the Unassociated Nodes pane, select the node.
- 3 Click **Associate Node(s) with Selected Cluster**.
- 4 In the confirmation dialog box, click **Yes**.
- 5 If necessary, close the Unassociated Nodes pane.

The node appears associated with the cluster in the Initializing state until it is deployed.

Problems Deleting a Node

If you are deleting a node, you may see an error message indicating that the discovery node installation failed, for example:

"An error occurred copying the discovery node installation program Quest.Reporter.Core.Server.MsiInstaller.exe to \\servername\ADMIN\$\Quest.Reporter.Core.Server.MsiInstaller.exe."

This indicates that there was a problem connecting to the host computer. Check your node credentials, ensure that the firewall is not enabled on the host, and ensure that the computer can be reached on the network. Once you have resolved the connection issue, you can attempt to remove the node again.

Creating a Node Debug Log File

If you are experiencing difficulty, the support staff may ask you to change the logging level for nodes in a cluster. The default setting for node logging is Warning, which also includes Fatal and Error. You can increase the logging level to Information or Debug to help them troubleshoot your issue. You also should increase the size of the node log files temporarily to accommodate the increased data collection.

i | **IMPORTANT:** Use caution when increasing the logging level. We recommend that you do not increase the level permanently, as it may affect node performance. The logging levels are cumulative, so Debug contains debug, information, warnings, errors and fatal errors.

To create a node debug log file

- 1 In the Manage Discovery Clusters pane, select the cluster.
 - i** | **NOTE:** The cluster must be enabled to change the node logging level.
- 2 On the Cluster Details tab in the bottom pane, change the node logging level to Debug.
- 3 Increase the size of the node log files.
- 4 Click **Apply**.

Data Collection Issues

You may run into situations where not all of your data is collected, or even no data at all. The first thing you need to determine is what tasks in the discovery are failing. Once you have located the problem tasks, you can use the errors and statistics generated to pinpoint the problem. There are several other things you can examine:

- The errors generated for a task provide a good starting point for troubleshooting. For more information, see [Viewing Errors and Statistics for Tasks](#) on page 86.

- During an Active Directory discovery, if collection issues are related to overloaded domain controllers, disable Create multiple tasks for each domain and specify multiple domain controllers for the domain instead. For more information, see [AD Discovery: Optionally select one or more domain controllers](#) on page 28.
- If your discovery fails for all tasks, it is possible that your shared data location is the problem. The shared data location may no longer exist, or the node may not have adequate access to it. Check the errors on the discovery task to investigate. For more information, see [Viewing Errors and Error Suppressions](#) on page 79. If this is the issue, ensure the shared data location belonging to the cluster exists and is properly permissioned. Shared data locations are not used for Active Directory, Exchange, or NTFS discoveries.
- If your discovery fails for a particular task:
 - The node may not have access to that server. Check your credentials, and change them if necessary. For more information see [Node Credential and Alternate Credential Details for On-Premises Discoveries](#) on page 86 and [Modifying Node Credentials](#) on page 99.
 - If you have used alternate credentials for the discovery, ensure that they are permissioned properly. For more information, see [Node Credential and Alternate Credential Details for On-Premises Discoveries](#) on page 86 and [Detailed Permissions for Enterprise Reporter Discoveries](#) on page 89.
 - If an Azure or Office 365 discovery fails, indicating that the objects could not be collected using a multi-factor authentication credential, retry the discovery with a non-multi-factor authenticated credential. For more information, see [Multi-Factor Authentication Discovery Credential Limitations](#) on page 16.
 - WMI and the SQL Server Browser service may be disabled or your credentials are inadequate. WMI and the SQL Server Browser service are used to query for SQL instances that are not broadcasting.
 - The task may have been rejected. If a task is rejected, it means that it is currently being collected by another discovery. Due to the way the Enterprise Reporter collects data, collecting from a SQL Server® in more than one discovery can result in data loss. You could only create one discovery for each SQL scope.
 - A discovery can fail if it runs at the same time attributes are being extended for that discovery type. Run the discovery again once the extension has been processed.
 - If a particular task is timing out, you can increase the amount of time allowed to connect to the database or process a command. For more information, see [Troubleshooting Connection Timeouts](#) on page 81.
 - A task may fail because the target computer cannot be pinged. The ping setting is available for computer, Exchange, NTFS and registry discoveries. If a target computer cannot be pinged, for example due to network settings or firewall configurations, or if you know that all computers in the discovery are online and available, you can disable the ping. However, if you have added a domain or OU as your scope, and there is a chance that any computer in the container is not available, setting the ping time ensures that no time is spent preparing to collect from these computers. If a computer unexpectedly fails a ping check, try increasing or disabling the ping for the discovery.
 - If your reporting users are experiencing unexpected data fluctuation, check your discovery configuration. If the same target (computer) is in more than one discovery, the data available for reporting reflects the last configuration that was run. Enterprise Reporter's recommended practice is to include a target in only one discovery of a given type. If you have accidentally included a target in more than one place, remove it from all but the desired discovery, and then run that discovery. If for some reason you choose to leave the target in more than one discovery, you can mitigate this issue by using the same settings in both discoveries.
 - The node may be running an unsupported operating system. Check the system requirements, and if necessary, remove the node from the cluster, then rerun the discovery.
 - If your Enterprise Reporter database is hosted on a SQL cluster which has experienced a node failure, this can occasionally result in a task that cannot finish processing. In this case, you may need to recreate the discovery.
 - Try running the discovery, and monitoring the Activity column in the Processing Tasks view, or looking at the history of the discovery. This may help you identify the specific activity that is causing

performance or data collection issues with the discovery. For more information, see [Viewing the Tasks for a Processing Discovery](#) on page 78, and [Viewing the History of a Discovery](#) on page 77.

- If your scheduled discovery does not run, there may be system issues that prevent the job from being created based on the schedule. In this case there is no error reported in the Configuration Manager. To address this issue check that your Enterprise Reporter server service is running, validate your license and check the state of any nodes on the system.
- If a discovery disappears, it is likely that another administrator deleted it. You will have to recreate the discovery.

Troubleshooting Features in Enterprise Reporter

There are several features in Enterprise Reporter to help you solve problems.

- [Exporting Logs from the Configuration Manager](#)
- [Viewing Information About Your Enterprise Reporter Configuration](#)
- [Viewing Errors and Statistics for Tasks](#)

Exporting Logs from the Configuration Manager

Exporting Discovery Management Logs

Discovery logs can be used to troubleshoot issues with discoveries. Discovery logs are collected from the Reporter server and all of the nodes within a selected cluster, and zipped into files that can be sent to Quest Support to help resolve certain collection problems. The discovery log files are all sent to the Exported Logs folder on the Reporter server. You may have several different .zip files, which may take some time to appear, depending on your configuration:

- A ServerLogs.zip file containing the logs from the server.
- A <Computer Name>_NodeLog.zip file for each node in the cluster.

To export discovery logs

- 1 On the Manage Discoveries pane, select a discovery.
By selecting a discovery first, the correct cluster for the discovery is automatically chosen.
- 2 Click the **Manage Logs** button and select **Export Logs**.
- 3 If necessary, change the selected cluster.
- 4 Click **Export**.
- 5 Click the link to locate your zip files.
Zip files are all located in the \ProgramData\Quest\Enterprise_Reporter\Exported_Logs folder.
You can now email your log files to your Quest Support representative.
- 6 Click **Close**.

NOTE: To help diagnose issues, the ServerLogs.zip contains additional files including the DatabaseMaintenance.log file and a SQLite file containing Enterprise Reporter system configuration information.

Exporting the Configuration Manager Logs

The Configuration Manager logs can be used to troubleshoot issues with the Configuration Manager service. Information is collected from the Configuration Manager service and is zipped into log files that can be sent to Quest Support to help resolve certain Configuration Manager problems. The log files are sent to the desktop on the Configuration Manager computer and may take some time to appear, depending on your configuration:

To export Configuration Manager logs

- 1 Click **System | Information**.
- 2 Under Client Logging Information, click **Export Configuration Manager logs**.
- 3 Click **Export**.
- 4 Click the link to locate your zip file.
You can now email your log files to your Quest Support representative.
- 5 Click **Close**.

Viewing the Configuration Manager Logs

You can unzip and view the Configuration Manager logs using the Log Viewer.

To view the Configuration Manager logs

- 1 Click **System | Information**.
- 2 Under Log Viewer, click **View logs** to open the Log Viewer.

Viewing Information About Your Enterprise Reporter Configuration

Understanding your system setup can be useful when troubleshooting. You can use the System Information page to determine where your console, Reporter server and Reporter database are hosted, what port the server is using to communicate, your software version, and other similar information you may find helpful in resolving issues.

To view system information in the Configuration Manager

- On the Navigation pane, click **System | Information**.

Viewing Errors and Statistics for Tasks

For each task of a discovery, you can view collection options, errors, and statistics. These may be helpful when you experience failed collections, data that does not match your expectations, or when working on performance issues. To display the collection options for a task, hold the mouse over any column of data for that task.

For more information, see the Viewing Errors and Viewing Statistics in the Quest Enterprise Reporter Configuration Manager User Guide [in the Technical Documentation](#).

Moving the Enterprise Reporter Database

The following summary outlines line how to move the Enterprise Reporter Database from one SQL Server® to another SQL Server®.

- Backup the database on SQL Server®
- Restore the database from a backup to the new SQL Server®
- Connect Enterprise Reporter to the new database location
- Verify that the database has been moved successfully

The following procedures assume that you have the following permissions:

- SQL permissions to access SQL Server® Management Studio on both the current and new SQL Server® to backup and restore the SQL database
- Windows account permissions to copy the database file from one server to another, and to stop and start services on the Enterprise Reporter server

To back up the Enterprise Reporter database (dbReporter) on SQL Server

- 1 Open Enterprise Reporter and stop all node services in the Configuration Manager.
- 2 On the Enterprise Reporter Server, stop the Quest Enterprise Reporter Server services (and the Quest Enterprise Reporter Node services if a node was deployed on the Enterprise Reporter server).
- 3 Start SQL Management Studio and connect to the SQL Server® where the dbReporter database resides.
- 4 Expand the database node.
- 5 Right-click on the dbReporter database and select **Tasks | Back up**.
- 6 In the Back Up Database dialog, note the location and name of the dbReporter database backup and click **OK**.

To restore the Enterprise Reporter database (dbReporter) from a backup to the new SQL Server

- 1 Copy the .BAK file(s) to the new SQL Server®.
- 2 Start SQL Management Studio on the new SQL Server®.
- 3 Right-click on the database's node and select **Restore Database**.
- 4 Under Source, select **Device**, click the ellipsis (...).
- 5 Click **Add** and browse to the backup copies.
- 6 Click **Add**, select the .BAK file, and click **OK** twice.
- 7 Under Backup sets to restore, select **Restore** beside the backup name.
- 8 From the Restore database window, click **OK** to restore the database.

To connect Enterprise Reporter to the new Database location

- 1 On the Enterprise Reporter server, stop the Quest Enterprise Reporter Server (and the Quest Enterprise Reporter Node if a node was deployed on the Enterprise Reporter server).
- 2 You may have more than one node deployed, so be sure to stop all node services.
- 3 On the Enterprise Reporter server, select **All Programs | Database Wizard**.
- 4 Choose **Select/Upgrade Database** and click **Next**.

- 5 Browse to (or type in the name of) the new SQL Server® and make sure the Enterprise Reporter database name is correct (for example, dbReporter), and click **Next**.
- 6 Accept the defaults on the Security Groups screen and click **Next**.
- 7 Click **OK** on the Database Maintenance Wizard popup that appears regarding replication.
- 8 Click **Finish** to initiate the database configuration.
- 9 Click **OK** upon completion.
- 10 Once you are returned to the Main Menu of the Database Wizard, click **Close**.
- 11 Start the Enterprise Reporter Server service.
- 12 Start all Enterprise Reporter node services.

To verify that the database has been moved successfully

- 1 Open Configuration Manager **System | Information** and confirm the database location.

Disaster Recovery

The following backup/restore procedure is the Enterprise Reporter 3.2.2 strategy for disaster recovery. This strategy will help ensure that Enterprise Reporter will be available for use as soon as possible. With regularly scheduled backups of the Enterprise Reporter database, recovery requires re-installing Enterprise Reporter, restoring the data, restoring a registry key, and restarting Enterprise Reporter.

Topics

- [Back Up of Enterprise Reporter](#)
- [How to Deploy Enterprise Reporter to Another Computer After a Disaster](#)
- [Checking the Enterprise Reporter Configuration After a Recovery](#)

Back Up of Enterprise Reporter

One SQL Server® database is created and used by Enterprise Reporter and should be included with the regular SQL Server® backup. This Discovery Management database has a default name of dbReporter.

How to Deploy Enterprise Reporter to Another Computer After a Disaster

If the original computer is unavailable due to disaster or hardware failure, Enterprise Reporter may need to be deployed on a new computer. The Enterprise Reporter database will be required.

To deploy Enterprise Reporter on a new computer

- 1 Build a recovery computer with the same name as the previous computer on which to install Enterprise Reporter.

The recovery computer must have the same name as the previous Enterprise Reporter computer so that the agents and nodes that are still active in the environment can continue to use the computer name to contact the Enterprise Reporter services.

- 2 Recover the Enterprise Reporter database.

This step may or may not be needed depending on how the initial configuration of Enterprise Reporter was done. For example, if the database was created on a common SQL Server® and the Enterprise Reporter server was on a separate computer, then the database is still available for use. If SQL Server® was installed on the same computer where Enterprise Reporter was installed, and that computer was damaged, then SQL Server® must be installed on the recovery computer and the Enterprise Reporter database must be restored on the recovery computer or on another SQL Server®.

- 3 If you have recovered the Enterprise Reporter database, you will need to import the encryption key from the backup file using the Enterprise Reporter Encryption Key Manager and the password that was entered when the encryption key was created. For more information, see [Appendix: Encryption Key Manager](#) on page 99 and [Importing a Key File](#) on page 100.

i | **NOTE:** If the encryption key backup file is unavailable, you may use the Enterprise Reporter Encryption Key Manager to erase the encrypted passwords used by the Enterprise Reporter Credential Manager. After using this feature, the passwords for all credentials must be re-entered using the Enterprise Reporter Credential Manager.

- 4 Install Enterprise Reporter on the recovery computer.
- 5 Start the Database Wizard.
- 6 Click **Select/Upgrade Existing Database** in the Database Wizard to allow Enterprise Reporter to make all of the necessary connections to the database and click **Next**.
- 7 Enter the database server and the database name (or accept the default of dbReporter). Select the connection type (Windows or SQL, depending on the initial configuration) and click **Next**.
- 8 In Configure Security Groups, it is recommended to leave the default setting unless another configuration was selected during the initial install. Click **Next**.
- 9 Once the database processing has finished, click **Finish**.

i | **NOTE:** If SQL Server® is installed on the same recovery computer as Enterprise Reporter, review the popup message about upgrading Enterprise Reporter. Select "**I understand and wish to continue**".

Checking the Enterprise Reporter Configuration After a Recovery

Start the Configuration Manager and check the health of the recovered Enterprise Reporter configuration.

To check the Enterprise Reporter Configuration after a recovery

- 1 Start the Configuration Manager.
- 2 Select **System | Information**.
Review and confirm all of the settings that Enterprise Reporter is currently using.
- 3 Select **Discovery Management | Manage Discoveries** and then click on the **Discovery Nodes** tab.
All the nodes are displayed.
- 4 Remove any node with a status of Faulted by selecting the node and clicking **Remove Node**.
- 5 Select **Yes** on the popup message.
- 6 Select **Discovery Management** and then click **Manage Discoveries**.

All of the discoveries should be available for use.

i | **NOTE:** If a Shared Data Location is being used with the Clusters, then delete files located in the share as the data in this share will be out of date and will cause errors in the data in reports.

Appendix: Database Content Wizard

Topics

- [Software Requirements](#)
- [Starting and Configuring the Enterprise Reporter Database Content Wizard](#)
- [Transferring an Enterprise Reporter Database](#)
- [Backing Up an Enterprise Reporter Database](#)
- [Restoring an Enterprise Reporter Database](#)
- [Cleaning an Enterprise Reporter Database](#)
- [Merging Two Enterprise Reporter Databases](#)
- [Running Custom Enterprise Reporter Scripts](#)

The Enterprise Reporter Database Content Wizard can be started from the Windows Start menu or from within the main Database Wizard. The Enterprise Reporter Database Content Wizard allows you to perform the following tasks on the information stored in Enterprise Reporter SQL Server® Databases:

- Configuration information (Clusters and Nodes, Discoveries, and Reports)
 - Transfer
 - Backup
 - Restore
- Collected data
 - Clean
 - Merge
- Custom scripts

Software Requirements

- PowerShell® 3.0

Starting and Configuring the Enterprise Reporter Database Content Wizard

To start and configure the Enterprise Reporter Database Content Wizard

- 1 Start the main Database Wizard by clicking the **Start** menu, and select **All Programs | Quest | Enterprise Reporter | Database Content Wizard**.
- 2 Optionally, click **Advanced Settings** to configure how long the server will wait for a response.

- 3 Optionally, set the **SQL Server Connection Timeout**.
- 4 Optionally, set the **SQL Server Command Timeout**.
- 5 Optionally, click **Reset to defaults** to restore both timeouts to 60 seconds.
- 6 Click **OK**.

Transferring an Enterprise Reporter Database

The transfer task allows the transfer of configuration data (Cluster, Node, Discovery, and Report information) between two Enterprise Reporter SQL Server® databases of the same version. This is useful for new Enterprise Reporter installations when Cluster, Node, Discovery, and Report information has already been configured.

i | **NOTE:** Collected data is not included in the transfer process.

To transfer an Enterprise Reporter database, complete the following steps:

- 1 Define the source database information.
- 2 Define the target database information.
- 3 Choose the data to transfer.

To define the source database information

- 1 Click **Transfer**.
- 2 Click **Define source database information**.
- 3 Enter the Source SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Source database name.
- OR -
Click the ellipsis to select a database from the specified Source SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To define the target database information

- 1 After defining the source database information, click **Define target database information**.
- 2 Enter the Target SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 3 Enter the Target database name.
- OR -
Click the ellipsis to select a database from the specified Target SQL Server.
- 4 Select an authentication method.
- 5 If SQL Server authentication was selected, enter the credentials.

- 6 Click **OK**.

To choose the data to transfer

- 1 After defining the target database information, click **Choose data to transfer**.
- 2 Select the elements to transfer.
 - i** | **NOTE:** Clearing the Clusters and Nodes option will remove the association between discoveries and clusters/nodes. They will need to be reconfigured manually.
- 3 If you have cleared the Clusters and Nodes option, click Yes to accept the warning and continue.
- 4 Click **Run**.

i | **CAUTION:** After the data transfer has completed successfully, you must restart your Enterprise Reporter Server service.

Backing Up an Enterprise Reporter Database

The backup task allows the backup of configuration data (Cluster, Node, Discovery, and Report information) from an Enterprise Reporter SQL Server® database into a single SQLite database file. This backup file can be stored in case the main database needs to be re-created. Regular backups may help save time in the event of database loss or corruption of data.

i | **NOTE:** Collected data is not included in the backup process.

To backup an Enterprise Reporter database, complete the following steps:

- 1 Define the source database information.
- 2 Define the backup database information.

To define the source database information

- 1 Click **Backup**.
- 2 Click **Define source database information**.
- 3 Enter the Source SQL Server name.
 - OR -
 - Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Source database name.
 - OR -
 - Click the ellipsis to select a database from the specified Source SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To define the backup database information

- 1 After defining the source database information, click **Define target database information**.
- 2 Enter the full file path and file name for the backup file.
 - OR -

Click the ellipsis to select a file location, enter a file name for the backup file, and click **Save**.

3 Enter a password.

i | **NOTE:** The password will be used to encrypt the backup file and will be required to access the file during any restore process.

4 Confirm the password by entering it again.

5 Click **OK**.

6 Click **Run**.

Restoring an Enterprise Reporter Database

The restore task allows the restoration of configuration data (Cluster, Node, Discovery, and Report information) from the SQLite file created in the Enterprise Reporter Database Content Wizard backup task into a new Enterprise Reporter SQL Server® database of the same version. The new database must be created using the Quest™ Enterprise Reporter Database Wizard. For more information, see the chapter named Using the Database Wizard to Create or Connect a Database in the [Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation](#).

i | **NOTE:** Collected data is not included in the restore process.

To restore an Enterprise Reporter database, complete the following steps:

- 1 Define the target database information.
- 2 Define the backup database information.

To define the target database information

- 1 Click **Restore**.
- 2 Click **Define target database information**.
- 3 Enter the Target SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Target database name.
- OR -
Click the ellipsis to select a database from the specified Target SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To define the backup database information

- 1 After defining the target database information, click **Define backup database information**.
- 2 Enter the full file path and file name of the existing backup file.
- OR -
Click the ellipsis to select the existing backup file and click **Open**.
- 3 Enter the password previously specified during the backup process.

- 4 Click **OK**.
- 5 Click **Run**.

Cleaning an Enterprise Reporter Database

The clean task allows the deletion of collected data from an Enterprise Reporter SQL Server® database. The clean task can be used to remove unwanted collected data if it becomes corrupt or inaccurate. You can delete all or each one of tombstoned, discovery run history, change history, and collected data.

i | **NOTE:** Configuration data (such as Cluster and Node, Discovery, and Report information) is not included in the clean process.

Each type of data can be further filtered by the following options:

- Discovery type: Active Directory, Azure Active Directory, Azure Resource, Computer, Exchange, Exchange Online, File Storage Analysis, Microsoft SQL, Microsoft Teams, NTFS, OneDrive, Registry
- Collection date (before a specific date or older than a certain number of days).

To clean an Enterprise Reporter database

- 1 Select an existing configuration file to specify the source database and the clean options.
- OR -
Define the source database information.
- 2 Choose the cleaning options.

To select an existing configuration file

- 1 Click **Clean**.
- 2 Enter the full path and file name of the configuration file.
i | **NOTE:** You can generate a configuration file using the steps in [To choose the cleaning options](#) on page 96.
- OR -
Click the ellipsis to select the existing configuration file and click **Open**.

To define the source database information

- 1 Click **Clean**.
- 2 Click **Define source database information**.
- 3 Enter the Source SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Source database name.
- OR -
Click the ellipsis to select a database from the specified Source SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To choose the cleaning options

- 1 After defining the source database information, click **Choose cleaning options**.
- 2 Select each type of data to be deleted during the clean.
- 3 Optionally, click **Filter options** for each selected data type and set the additional filters to apply.
- 4 Optionally, select **Save these options in a file** and enter the full path and file name of the file to create.
 - i** | **NOTE:** The file created by enabling this option can be used as a configuration file for subsequent or scheduled clean processes.
- 5 Once cleaning options are selected, click **OK**.
 - i** | **NOTE:** If you have selected **Save these options in a file**, that file is created now.
- 6 Click **Run**.

Merging Two Enterprise Reporter Databases

The merge task allows merging of collected data in a source Enterprise Reporter SQL Server® database into a target Enterprise Reporter SQL Server® database of the same version. The target database will contain data from both the source and target databases.

i | **NOTE:** Configuration data (such as Cluster and Node, Discovery, and Report information) is not included in the merge process.

! | **CAUTION:** It is strongly recommended that you back up your databases before starting the merge. You can restore the backup if there are issues with the merge.

To merge two Enterprise Reporter databases, complete the following steps:

- 1 Define the source database information.
- 2 Define the target database information.

To define the source database information

- 1 Click **Merge**.
- 2 Click **Define source database information**.
- 3 Enter the Source SQL Server name.
 - OR -
 - Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Source database name.
 - OR -
 - Click the ellipsis to select a database from the specified Source SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To define the target database information

- 1 After defining the source database information, click **Define target database information**.

- 2 Enter the Target SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 3 Enter the Target database name.
- OR -
Click the ellipsis to select a database from the specified Target SQL Server.
- 4 Select an authentication method.
- 5 If SQL Server authentication was selected, enter the credentials.
- 6 Click **OK**.
- 7 Click **Run**.
A warning is displayed indicating that the data will be permanently merged and that this action is permanent.
- 8 Select **I understand**, and click **OK**.

Running Custom Enterprise Reporter Scripts

The script task allows you to run custom scripts to modify the data in an Enterprise Reporter SQL Server® database. The target database will be modified based on the content of the custom script.

! | **CAUTION: It is strongly recommended that you back up your databases before starting the script. You can restore the backup if there are issues with processing the script.**

To run a custom script on the Enterprise Reporter database, complete the following steps:

- 1 Define the target database information.
- 2 Select a custom script.
- 3 Optionally, enter script arguments.

To define the target database information

- 1 Click **Script**.
- 2 Click **Define target database information**.
- 3 Enter the Target SQL Server name.
- OR -
Click the ellipsis to enumerate all broadcasting SQL Servers on the network and select one.
- 4 Enter the Target database name.
- OR -
Click the ellipsis to select a database from the specified Target SQL Server.
- 5 Select an authentication method.
- 6 If SQL Server authentication was selected, enter the credentials.
- 7 Click **OK**.

To select the custom script

- 1 After defining the target database information, click **Select a script**.
- 2 Select a custom script to run.
- 3 Click **OK**.
- 4 Click **Run**.

- OR -

Optionally, enter any arguments required for this script.

To enter script arguments

- 1 After selecting a custom script, click **Enter script arguments**.
- 2 Type the required information for each argument.
- 3 Click **OK**.
- 4 Click **Run**.

Appendix: Encryption Key Manager

Topics

- [Starting the Encryption Key Manager](#)
- [Generating a Key File](#)
- [Importing a Key File](#)
- [Exporting a Key File](#)
- [Resetting Credentials](#)

Enterprise Reporter makes use of FIPS 140-2 compliant encryption to secure user credentials and includes an encryption key management tool. The Enterprise Reporter Encryption Key Manager can be started from the Windows Start menu. This tool allows you to perform the following tasks related to the Enterprise Reporter encryption key.

- Generating an encryption key
- Importing an encryption key from a backup file
- Exporting an encryption key to a backup file
- Resetting Enterprise Reporter user credentials

Starting the Encryption Key Manager

To start the Encryption Key Manager from the Windows Start menu

- 1 Click Programs | Quest | Enterprise Reporter | Encryption Key Manager

Generating a Key File

The Encryption Key Manager can be used to generate a new encryption key. If Enterprise Reporter contains credentials with passwords, selecting this option will force the decryption and re-encryption of all Enterprise Reporter user credentials. If the decryption of the existing passwords fails, the procedure is unsuccessful, errors are returned, and no key file is generated. If the decryption and re-encryption is successful, the procedure continues and the new encryption key is written to the secure Windows Credential Manager (not to be confused with the Enterprise Reporter Credential Manager). The user is prompted to export the new key to a backup file.

To generate a key file

- 1 Stop all Enterprise Reporter nodes.
- 2 Start the Enterprise Reporter Encryption Key Manager.
- 3 Click the **Generate Key** button.
- 4 Read and accept the warning.
- 5 Click **OK** to generate a new key file.

- 6 Click **OK** to continue to export the key file to a backup file.
For more information, see [Exporting a Key File](#) on page 100.

Importing a Key File

The Encryption Key Manager can be used to import an encryption key from an Enterprise Reporter backup file. This option requires the user-supplied password that was used to create the backup file. If Enterprise Reporter contains credentials with passwords, this procedure will decrypt and re-encrypt all of them and store the imported encryption key in the secure Windows Credential Manager (not to be confused with the Enterprise Reporter Credential Manager).

To import a key file

- 1 Stop all Enterprise Reporter nodes.
- 2 Start the Enterprise Reporter Encryption Key Manager.
- 3 Click the **Import Key** button.
- 4 Enter the fully qualified filename of the backup file.
- OR -
Click the ellipsis to navigate to the Import Location of the backup file.
- 5 Enter the user-supplied password for the backup file.
- 6 Read and accept the warning.
- 7 Click **OK** to import the backup file.
- 8 Click **OK** to accept the successful import notification.

Exporting a Key File

The Encryption Key Manager can be used to export the current encryption key to a backup file encrypted with a user-supplied password.

 | **IMPORTANT:** It is very important to remember this password as it is non-recoverable.

To export a key file

- 1 Click the **Export Key** button.
- 2 Enter a fully qualified filename as an export location for the backup file.
- OR -
Click the ellipsis to navigate to an Export Location for the backup file.
- 3 Enter a password with a minimum of 10 characters.
- 4 Enter the password again to confirm the password.
- 5 Click **OK** to create the backup file.
- 6 Click **OK** to accept the successful backup notification.

Resetting Credentials

The Encryption Key Manager can be used to erase all encrypted passwords used by the Enterprise Reporter Credential Manager when it is impossible to restore a valid encryption key. After using this feature, passwords for all credentials must be re-entered using the Enterprise Reporter Credential Manager. The Credential Manager will display a red key icon next to each account that requires a password.

CAUTION: Use the **Reset Credentials** option only when it is impossible to restore a valid encryption key.

To reset credentials

- 1 Click the **Reset Credentials** button.
- 2 Read and accept the warning.
- 3 Click **OK** to erase all passwords for credentials stored in the Enterprise Reporter Credential Manager.
- 4 Click **OK** to confirm that you wish to erase all passwords.
- 5 Click **OK** to accept the successful reset notification.

•

Appendix: Log Viewer

Topics

- [Starting the Enterprise Reporter Log Viewer](#)
- [Finding and Opening Log Files](#)
- [Viewing and Searching Log File Entries](#)
- [Filtering Log File Entries](#)

The Enterprise Reporter Log Viewer can be started from the Configuration Manager, the Report Manager, or the Windows Start menu. The Enterprise Reporter Database Log Viewer allows you to perform the following tasks on the log files generated by Enterprise Reporter.

- Browsing for log files
- Unzipping log files
- Drag and drop to open log files
- Correlating events from multiple log files and displaying them chronologically
- Searching within log files for specific events or errors
- Limiting the events displayed using filters

Starting the Enterprise Reporter Log Viewer

To start the Enterprise Reporter Log Viewer in the Configuration Manager

- 1 Click **System | Information | Log Viewer | View Logs**

To start the Enterprise Reporter Log Viewer in the Report Manager

- 1 Click **System Information | log viewer |View Logs**

To start the Enterprise Reporter Log Viewer from the Windows Start menu

- 1 Click **Programs | Quest | Enterprise Reporter | Log Viewer**

Finding and Opening Log Files

The first time the Log Viewer is started, it displays the contents of the default Enterprise Reporter log folder including date, time, and file size information.

```
\programdata\quest\enterprise_reporter
```

To navigate to different folder containing log files, click the ellipsis to the right of the log folder path. The files in the selected folder will be listed in the Log Viewer file browser. During the time the Log Viewer is open, the contents of the folder may be updated by clicking the Refresh icon next to the log folder path.

To open log files using the Log Viewer browser

- 1 Double-click the log file containing entries to be viewed.
- OR -
Select the log file containing entries to be viewed and click the **Open** icon.
- OR -
Drag the log file containing entries to be viewed onto the main log entry viewing panel.
- OR -
Drag a log file from Windows File Explorer onto the main log entry viewing panel.

To unzip log files in the Log Folder panel

- 1 Select the log file containing entries to be unzipped and click the **Unzip** icon.
- OR -
Right-click the log file containing entries to be unzipped and select the **Unzip** icon.

To clear log files in the Imported Log Files panel

- 1 Select the log file containing the entries to be cleared from the main log entry viewing panel and click the **Clear** icon.
- OR -
Right-click the log file containing entries to be cleared from the main log entry viewing panel and select the **Clear** option.

Viewing and Searching Log File Entries

The files listed in the Imported Log Files panel have their contents correlated and displayed in the main log entry viewing panel sorted by date and time.

To search for specific text within the log entries

- 1 Enter the text to locate in the **Find** text box.
- 2 Press **Enter** to locate the first occurrence of the text within the log entries being viewed.
The matching log entry will be highlighted.
- 3 Optionally, click the **Find Next** icon to find the next occurrence of the text within the log entries being viewed.
- 4 Optionally, click the **Find Previous** icon to find the previous occurrence of the text within the log entries being viewed.

To search for errors by error text within the log entries

- 1 Enter the error text to locate in the **Find** text box.
- 2 Optionally, click the **Next Error** icon to find the next occurrence of the text within the ERROR log entries being viewed.
- 3 Optionally, click the **Previous Error** icon to find the previous occurrence of the text within the ERROR log entries being viewed.

To browse for errors within the log entries

- 1 Click on the log entry from which you wish to browse.
- 2 Optionally, right-click the log entry and select **Next Error** to browse to the next error within the log entries being viewed.
- 3 Optionally, right-click the log entry and select **Previous Error** to browse to the next error within the log entries being viewed.

To view the details of a log entry

- 1 Double-click a log entry.
- OR -
Right-click a log entry and select **View Details**.
- OR -
Select a log entry and click the **View Details** icon above the main log entry viewing panel.

To clear all event log entries

- 1 Click the **Clear All** button above the main log entry viewing panel.
- 2 Accept the warning message to continue with removing all of the log entries.

Filtering Log File Entries

Once a listing of log file entries is displayed, the Filters option can be used to limit the entries by dates and other properties. For more information, see [Viewing and Searching Log File Entries](#) on page 103. Setting a Start Date will display entries with a time stamp that occurs on or after that date. Setting an End Date will display entries with a time stamp that occurs on or before that date. Selecting options for each property will display entries matching those options.

To filter log file entries

- 1 Once you are viewing a listing of log file entries, click the **Filters** button.
- 2 Optionally enter a Start Date.
- 3 Optionally, enter an End Date.
- 4 Optionally, select at least one option per property.
- 5 Optionally, click the reset button to clear all filters and start again.
- 6 Click **Apply** to display the log file entries that match the filters.

•

A

- active directory discoveries
 - node setup, 63

Active Roles

- software requirements, 18
- supported versions, 16

alternate credentials

- node, 21

Azure

- software requirements, 18

azure

- credentials, 23

azure active directory application

- permissions, 26

azure active directory discoveries

- node setup, 63

azure resource application

- permissions, 26

C

- changing database connection credentials, 58

- changing databases, 58

cluster

- deployment considerations, 61

- fine tune, 61

cluster structure

- discovery targets, 69

- collecting data, 70

- options, 71

computer discoveries

- node setup, 64

credential use

- planning, 65

credentials

- azure, 23

- database creation, 37

- exchange online, 23

- minimizing the number of, 67

- minimizing the permissions required for, 67

- node, 21

- onedrive, 24

- scenarios, 66

- troubleshooting database creation, 79

D

- data collection, 70

- nested group membership, 75, 76

- options, 71

- data transfer

- optimize, 69

database

- backup, 93

- changing connection information, 58

- changing to a different, 58

- clean, 95

- considerations, 10, 60

- deleting, 56

- maintenance, 54, 59

- merge, 96

- restore, 94

- transfer, 91

- upgrading, 55

database configuration

- credentials, 78, 79

- errors, 78, 79

- existing database, 42

- methods, 36

database content wizard

- software requirements, 91

- start, configure, 91

database creation

- credentials, 37

Database Wizard

- change database, 58

- changing security mode, 57

- database maintenance, 59

- deleting a database, 56

- introduction, 53

- upgrading a database, 55

- deployment considerations, 61

- data to collect, 61

- determining your software version, 86

discovery

- considerations, 69

- permissions, 23

- permissions on nas devices, 25

- scheduling, 75

- targets
 - cluster structure, 69
 - troubleshooting, 84

E

- encryption key manager
 - export key, 100
 - generate key, 99
 - import key, 100
 - reset credentials, 101
 - starting, 99
- errors, 86
- Exchange
 - software requirements, 18
- Exchange Online
 - software requirements, 19
- exchange online
 - credentials, 23
- existing database
 - using during installation, 42
- export
 - logs, 85

F

- failover recovery
 - using SQL clusters, 11, 61
- file storage analysis discoveries
 - node setup, 64

I

- installation, 40, 46
 - Discovery Manager, 43
 - Report Manager, 44
 - server, 40, 47
- IT Security Search
 - supported versions, 16

K

- key features, 7

L

- log viewer
 - filtering log file entries, 104
 - finding log files, 102
 - opening log files, 102
 - searching log file entries, 103
 - starting, 102
 - viewing log file entries, 103
- logs
 - discovery manager, 85
 - exporting, 85

M

- manual node deployment, 82
- microsoft sql discoveries
 - node setup, 64
- minimum
 - permissions, 27
- multi-domain controller issues, 78

N

- nested group membership
 - collection, 75, 76
- node
 - alternate credentials, 21
 - credentials, 21
 - deploying in a trusted domain, 68
 - fine tune, 61
 - manually deploying, 82
 - manually install, 82
 - optimize setup, 62
 - setup
 - active directory discoveries, 63
 - azure active directory discoveries, 63
 - computer discoveries, 64
 - file storage analysis discoveries, 64
 - microsoft sql discoveries, 64
 - ntfs discoveries, 65
 - office 365 discoveries, 65
 - troubleshooting, 82
 - unassociated node, 82
- nodes
 - deployment considerations, 61
 - remote
 - effectively deploy, 68
- ntfs discoveries
 - node setup, 65

O

- office 365 discoveries
 - node setup, 65
- OneDrive
 - software requirements, 19
- onedrive
 - credentials, 24
- onedrive azure application
 - permissions, 25

P

- permissions
 - azure active directory application, 26
 - azure resource application, 26
 - discoveries, 23

- discoveries on nas devices, 25
- microsoft teams application, 26
- onedrive azure application, 25
- tenant applications, 25

port

- current port, 86
- requirements, 28

R

- remote nodes
 - effectively deploy, 68
- reports
 - scheduling, 75
- requirements
 - firewall, 35
 - hardware, 11
 - operating systems, 13
 - port, 28
 - services, 19
 - software, 18
- role based security, 52
- roles
 - described, 52

S

- scheduling
 - discovery, 75
 - reports, 75
- scripts
 - custom, 97
- security groups
 - creation, 51
 - described, 51
 - error creating, 79
 - group names, 37
- server
 - considerations, 10, 60
- software requirements, 18
 - Active Roles, 18
 - Azure, 18
 - Exchange, 18
 - Exchange Online, 19
 - OneDrive, 19
- SQL clusters
 - failover recovery, 11, 61
- SQL logins
 - described, 38
- SQL roles
 - described, 37
 - error creating, 79
- SQL Server

- certificates, 17
 - changing security mode, 57
 - supported versions, 16
- SQL server
 - choosing, 41, 54
 - troubleshooting connection, 77
- sql server
 - current database, 86
- SQL Server Browser service, 84
- SQL Server command timeout, 92
- SQL Server connection timeout, 92
- statistics, 86
- system
 - information, 86

T

- tenant applications
 - permissions, 25
- trusted domain
 - nodes, 68

U

- uac, 78
- unassociated node, 82

W

- wmi, 84

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at <https://support.quest.com>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.