Quest® Enterprise Reporter 3.5.1

Installation and Deployment Guide

Legend

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

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

Contents

Product Overview

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. 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 Exchange Online environment
    - information about your Microsoft Teams
    - information about your SharePoint Online environments
- 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.
- Publish reports to SSRS.
- 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.
- Us the 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 Microsoft Teams.
- Use the Microsoft SharePoint Online reports to answer questions about your SharePoint Online environments.

> **i** | **NOTE:** Azure Active Directory is now Microsoft Entra ID.

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

See also:

- Enterprise Reporter Architecture

Enterprise Reporter Architecture

Figure 1 outlines the relationship between the components.

Figure 1. Enterprise Reporter Architecture
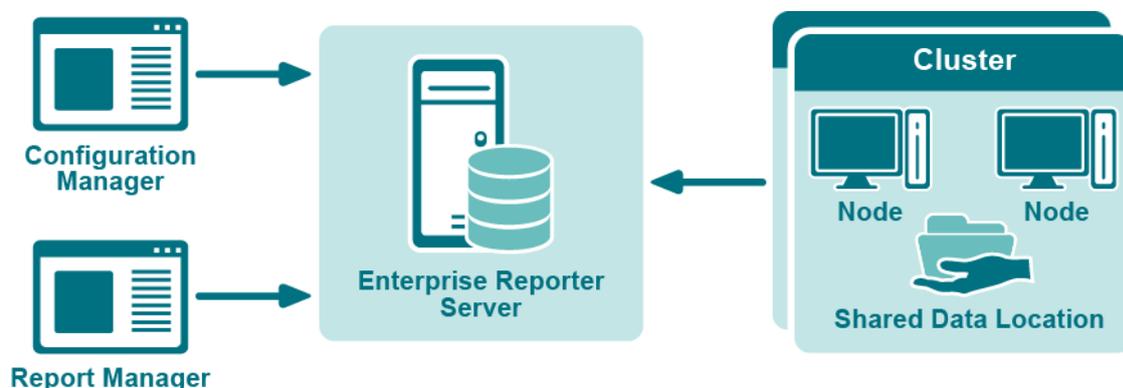
Installation Considerations for Enterprise Reporter

- Before You Install Enterprise Reporter
- Enterprise Reporter server and database considerations
- System Requirements
- Overview of Enterprise Reporter communications and required credentials
- 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.

See also:

- Enterprise Reporter server and database considerations
- System Requirements
- Minimum permissions for installing Enterprise Reporter
- Port Requirements
- Ports for Enterprise Reporter to connect to Active Roles server
- Configuring the Database and Security Groups
- Database Requirements

Enterprise Reporter server and database considerations

You must choose a host computer for Enterprise Reporter server and a SQL Server to host the Enterprise Reporter database. Your decision affects the performance of the product.

The Enterprise Reporter server communicates directly with the database frequently. For best results, locate the Enterprise Reporter server physically close to the SQL Server.

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.

See also:

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

Topics

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

Hardware requirements

Enterprise Reporter Server

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

Table 1. Enterprise Reporter Server Hardware Requirements

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

Configuration Manager and Report Manager

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

Table 2. Configuration Manager and Report Manager Hardware Requirements

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

Enterprise Reporter nodes

For the Enterprise Reporter nodes, we recommend the following minimum hardware. For detailed recommendations for node requirements, see *Optimize Node Setup* on page 63.

Table 3. Node Hardware Requirements

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

Enterprise Reporter SQL Server

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

Table 4. SQL Server Hardware Requirements

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

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

Database size estimator

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

Larger environments

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

- The type of collections being performed.

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

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

- The size of collections being performed.

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

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

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

New required hardware

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

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

Supported operating systems

The following operating systems are supported for Enterprise Reporter components.

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® 2022	X	X	X
Windows Server® 20H2	X		X
Windows Server® 2004	X		X
Windows Server® 1909	X		X
Windows Server® 1903	X		X
Windows Server® 2019	X	X	X

Table 5. Supported Operating Systems

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

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

Table 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® 2016 Functional Level	X				
Windows Server® 2012 R2 Functional Level	X				
Windows Server® 2012 Functional Level	X				
Computers					
Windows Server® 2022		X	X		
Windows Server® 20H2		X	X		
Windows Server® 2004		X	X		
Windows Server® 1909		X	X		
Windows Server® 1903		X	X		
Windows Server® 2019 and 1809		X	X		
Windows Server® 2016 and 1803		X	X		
Windows Server® 2012, 2012 R2, and 2012 Core		X	X		
Windows® 11		X	X		
Windows® 10		X	X		
Windows® 8.1		X	X		
Network Attached Storage (NAS) Devices					
Dell Fluid File System 6.0		X	X		
Dell Fuild File System 5.0		X	X		
NetApp® 9.4		X	X		

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

Active Roles supported versions

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

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

- Active Roles 7.0.2

IT Security Search supported versions

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

- IT Security Search 11.4.1
- IT Security Search 11.3

Supported Internet protocols

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

SQL Server supported versions

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

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

Using SQL Server certificates

SSL encryption of SQL Server connections using certificates

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

The steps required to configure this encryption are as follows.

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

- Import the certificate to all Enterprise Reporter computers that will communicate with the SQL Server, such as the:

    - Enterprise Reporter server host computer

    - Enterprise Reporter nodes

    - Enterprise Reporter Configuration Manager host computer

    - Enterprise Reporter Report Manager host computer

- Install Enterprise Reporter on a host computer.

Required software

The following software is required for Enterprise Reporter.

- Microsoft.NET Framework 4.8

- Microsoft Excel 2010, 2013, 2016, or 2019 (required to view reports exported as spreadsheets)

- Microsoft 365 Excel

- PowerShell 3.0

Active Roles required software

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

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

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

The following additional considerations are required:

- There must be a trust between the Enterprise Reporter domain and the Active Roles domain.

- The credentials used for the Active Roles discovery must have access to the Active Roles domain.

Exchange required software

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

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

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

- Impersonation needs to be configured on the Exchange organization. Refer to your Exchange Server documentation or use the following method to set up role assignments.

    - PowerShell can be used to add an assignment

      New-ManagementRoleAssignment –Name:impersonationAssignmentAdministrator –Role:ApplicationImpersonation –User:Administrator

    - Alternatively, you can create an administrator role with ApplicationImpersonation role assigned to it and add the required account as a member (or assign ApplicationImpersonation role to an existing administrator role)

Exchange Online required software

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

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

Multi-Factor Authentication Cloud Discovery Credential Limitations

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

Table 7. Cloud discoveries that may be excluded due to Multi-Factor Authentication

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

Required services

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

- Net.TCP Port Sharing

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

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

Overview of Enterprise Reporter communications and required credentials

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

Figure 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.

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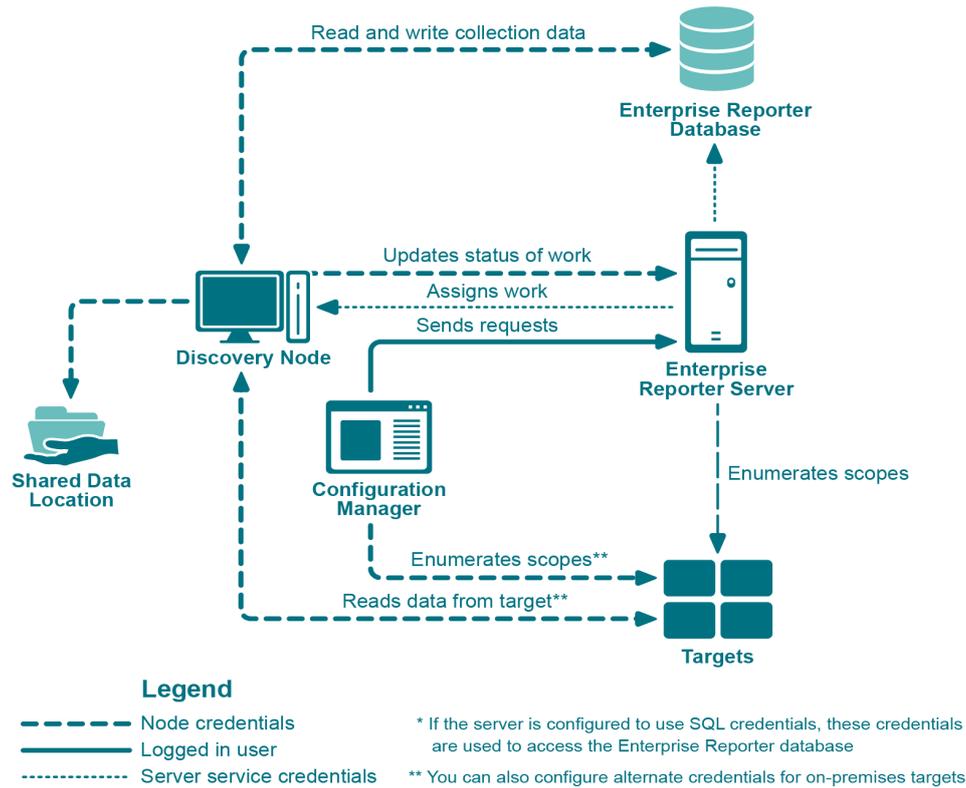
Topics

- 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 8. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Server	Provide server with job status, errors, statistics and logs.	Configured during node creation, or when you edit the node properties to change the credentials. The node credentials must have local administrator access to the host computer and be a member of the group "Reporter_Discovery_Nodes".
Discovery Node	Shared Data Location (if the cluster is configured to use one)	Read and write to the shared data location during data collection.	The shared data location is configured during the creation of a cluster. Ensure the node has read and write access to this file share. For more information, see the Things to Consider Before Creating a Cluster section in the Configuration Manager User Guide
Discovery Node	Enterprise Reporter Database	There are two options for communicating with the database: 1. You can use the same service credentials that the node service uses. 2. You can specify SQL credentials only for use when the database is accessed. The credentials you choose must be able to read and write to the database.	The account must be in the Reporter_Discovery_Nodes security group. (Note that if you use the same account as the Enterprise Reporter server it is already permissioned appropriately). If you use SQL authentication to connect with the database, you must manually permission the SQL user, either by adding them to the database role Discovery_Nodes_Role or by permissioning specific tables in the database.
Discovery Node	Targets	Read access on all targets. For on-premises discoveries, all domains with which the credentials have a forest or domain level trust will be enumerated. If required, you can configure alternate credentials for specific discoveries, instead of using the default node credentials.	The targets are defined as part of a discovery. The discovery tasks are assigned to a particular node based on availability, so all nodes in a cluster should have access to all targets defined in all discoveries assigned to the node's cluster. For on-premises discoveries, ensure the node credentials or alternate credentials have read access to the target. In addition, a trust is required between the node computer and the targets. For more information on Azure and Microsoft 365 Discoveries, see Detailed permissions for Enterprise Reporter discoveries on page 21.

Detailed permissions for Enterprise Reporter discoveries

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

Table 9. Detailed permissions required for Enterprise Reporter discoveries

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

Table 9. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
File Storage Analysis	An account with local administrator access on the scoped computer is required to collect file, folder, share, and home drive analysis data. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 23.
Microsoft SQL	An account with local administrator access on the SQL Server is required. Additionally, the account must have read access to the scoped database to collect database information. At a minimum, if not using fixed roles, the following SQL permissions are required on the securable object being used for collection. • Grant View Any Definition • Grant View Server State • Grant View Connect Any Database • Grant View Select All Securables
Microsoft Teams	The user credentials used to collect Microsoft Teams information must have either the Teams Administrator or Global Administrator permissions. The user must also be a member of each Microsoft Teams group to prevent access denied errors during disk discovery. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Microsoft Teams application required for this discovery.
NTFS	If collecting through the administrator share, an account with local administrator access to the scoped computer is required. If collecting through a network share, an account with read permissions to the scoped shares is required. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 23.
OneDrive	An account with access to the discovery target tenant. Administrator permissions are required for collection of all drives including drive information, configuration settings, files, folders, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each drive that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter OneDrive application required for this discovery.

Table 9. Detailed permissions required for Enterprise Reporter discoveries

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

Permissions for Enterprise Reporter discoveries on NAS devices

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

Table 10. Permissions required for Enterprise Reporter discoveries on NAS Devices

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

Permissions for Enterprise Reporter tenant applications

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

Azure Active Directory application permissions

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

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

Table 11. Required permissions

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

Collecting user activity information

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

- Microsoft Graph: Read all usage reports

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

1 Open the Microsoft 365 admin center.

2 Navigate to **Settings | Org Settings | Services**.

3 Select **Reports**.

4 Clear the **Display concealed user, group, and site names in all reports** check box.

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

OneDrive application permissions

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

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

Table 12. Required permissions

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

Azure Resource application permissions

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

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

Table 13. Required permissions

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

Microsoft Teams application permissions

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

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

Table 14. Required permissions

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

SharePoint Online application permissions

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

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

Table 15. Required permissions

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

Minimum permissions for 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 16. 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.	
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 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.

The following figure shows the ports that are used by the various Enterprise Reporter components.

Figure 3. Ports used by Enterprise Reporter components.
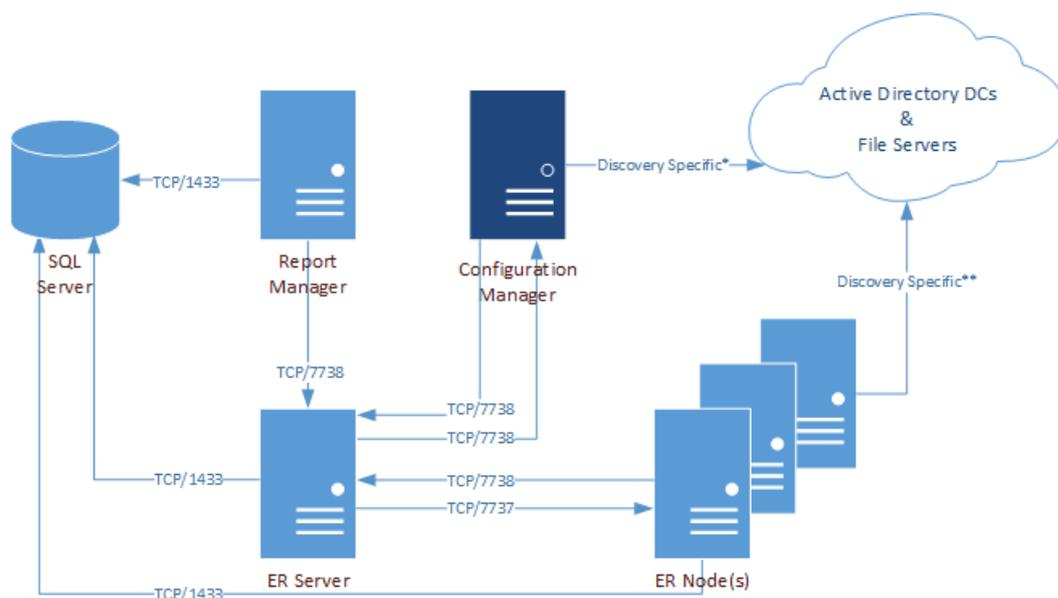
*For more information on ports used when creating a discovery, see Table 17.

**For more information on ports used during data collections, see Table 18.

The following table shows the ports used by all of the Enterprise Reporter components.

Table 17. Ports used by Enterprise Reporter components

Application	Port	Type	Configuration Manager	Report Manager	SQL Server	ER Server	ER Nodes
			Components				
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				

Table 17. Ports used by Enterprise Reporter components

Application	Port	Type	Configuration Manager	Report Manager	SQL Server	ER Server	ER Nodes
					Components		
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

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

Table 18. Ports used by Enterprise Reporter discoveries

Application	Port	Type	Active Directory	Azure Active Directory	Azure Resource	Computer	Exchange	Exchange Online	File Storage Analysis	Microsoft Teams	NTFS	OneDrive	Registry	SharePoint Online	SQL Server
									Discoveries						
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		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
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		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	X	X
SQL Server Browser Service	1434	UDP													X
LDAP GC	3268	TCP	X				X								
WinRM	5985 5986	TCP UDP					X	X							X
DCOM on Vista/2008 and above (uses an open port in this range)	49152 - 65535	TCP UDP		X	X	X	X		X		X				X

*Exchange 2013 and higher

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

Figure 4. Ports used by Active Directory collections
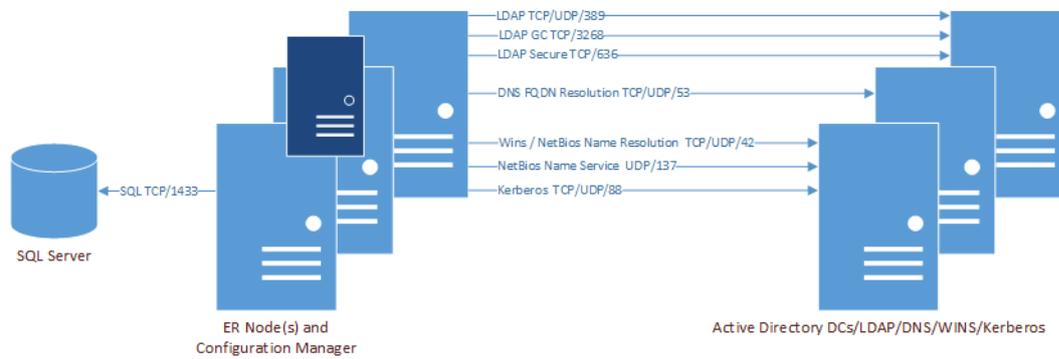
Figure 5. Ports used by Azure and Microsoft 365 collections (Exchange Online, MS Teams, OneDrive, and SharePoint Online)
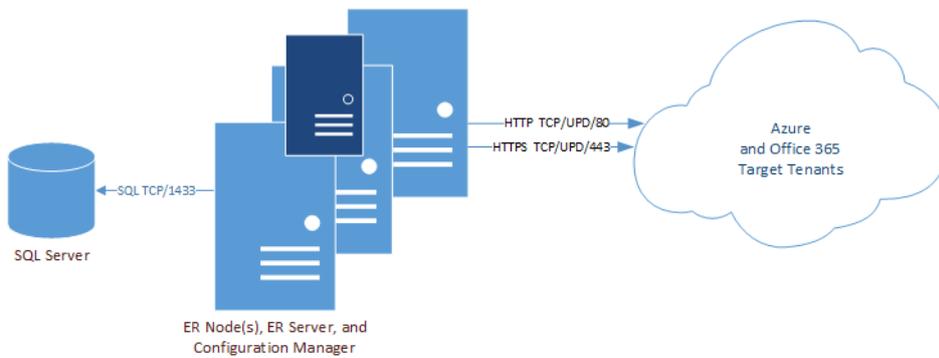
Additional ports for Azure and Microsoft 365 discoveries to be set on the Node:

- Open ports 49151-65535 TCP Outbound
- Open ports 49151-65535 UDP Outbound

Figure 6. Ports used by Computer collections

Network Share
SMB TCP/445

SQL Server
SQL TCP/1433

ER Node(s) and
Configuration Manager

LDAP TCP/UDP/389
DNS FQDN Resolution TCP/UDP/53
NetBios Name Service UDP/137
Wins / NetBios Name Resolution TCP/UDP/42
Kerberos TCP/UDP/88

Active Directory DCs/
LDAP/DNS/WINS/Kerberos

SMB TCP/445
RPC Service & Endpoint Mapper / WMI TCP/UDP/135
DCOM on XP/2003 and below TCP/UDP 1024-5000
ICMP
DCOM on Vista/2008 and above TCP/UDP 49152-65535
Remote Registry TCP/139

Target Computers

Figure 7. Ports used by Exchange collections

SQL Server
SQL TCP/1433

ER Node(s) and
Configuration Manager

LDAP TCP/UDP/389
DNS FQDN Resolution TCP/UDP/53
LDAP GC TCP/3268
NetBios Name Service UDP/137
Wins / NetBios Name Resolution TCP/UDP/42
Kerberos TCP/UDP/88

Active Directory DCs/
LDAP/DNS/WINS/Kerberos

SMB TCP/445
RPC Service & Endpoint Mapper / WMI TCP/UDP/135
DCOM on XP/2003 and below TCP/UDP/1024-5000
DCOM on Vista/2008 and above TCP/UDP/49152-65535
Remote Registry TCP/139
Exchange PowerShell /TCP/12067

Target Exchange Servers

Additional port for Exchange discovery to be set on the Node:

• Open WinRM HTTP port 5985 TCP Outbound

Figure 8. Ports used by File Storage Analysis collections
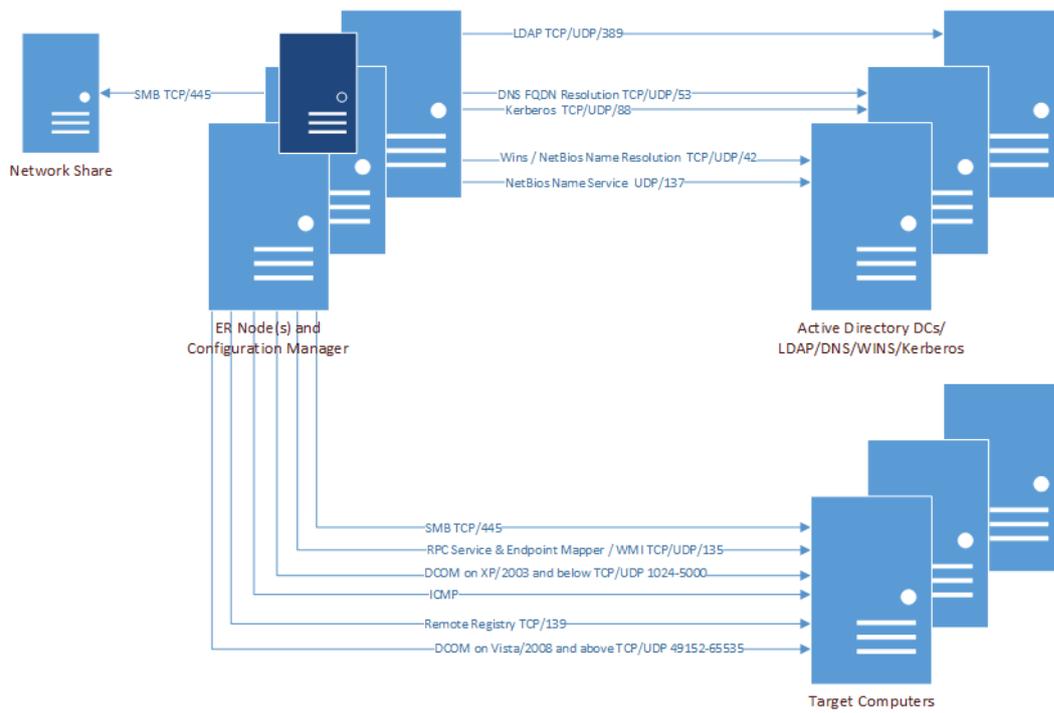
Figure 9. Ports used by NTFS collections
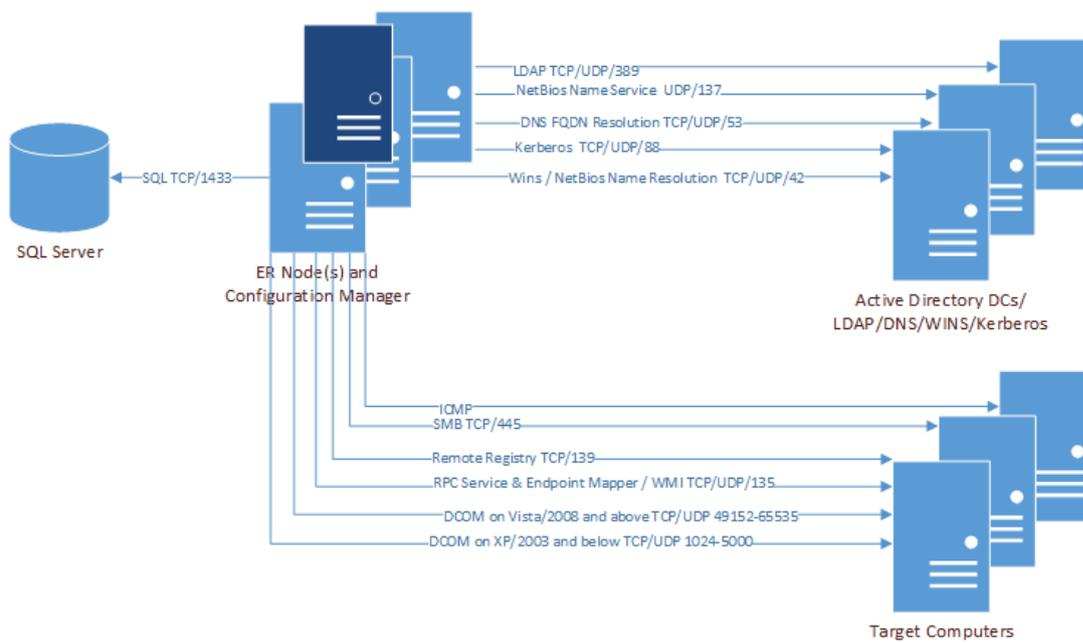
Figure 10. Ports used by Registry collections
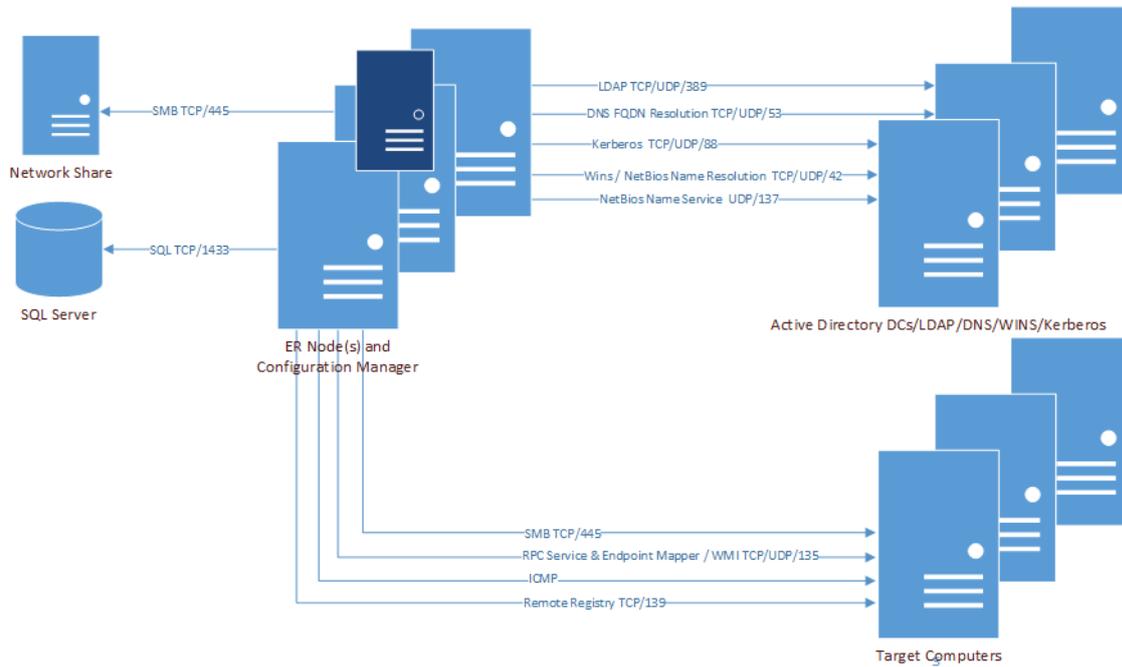
Figure 11. Ports used by SQL collections
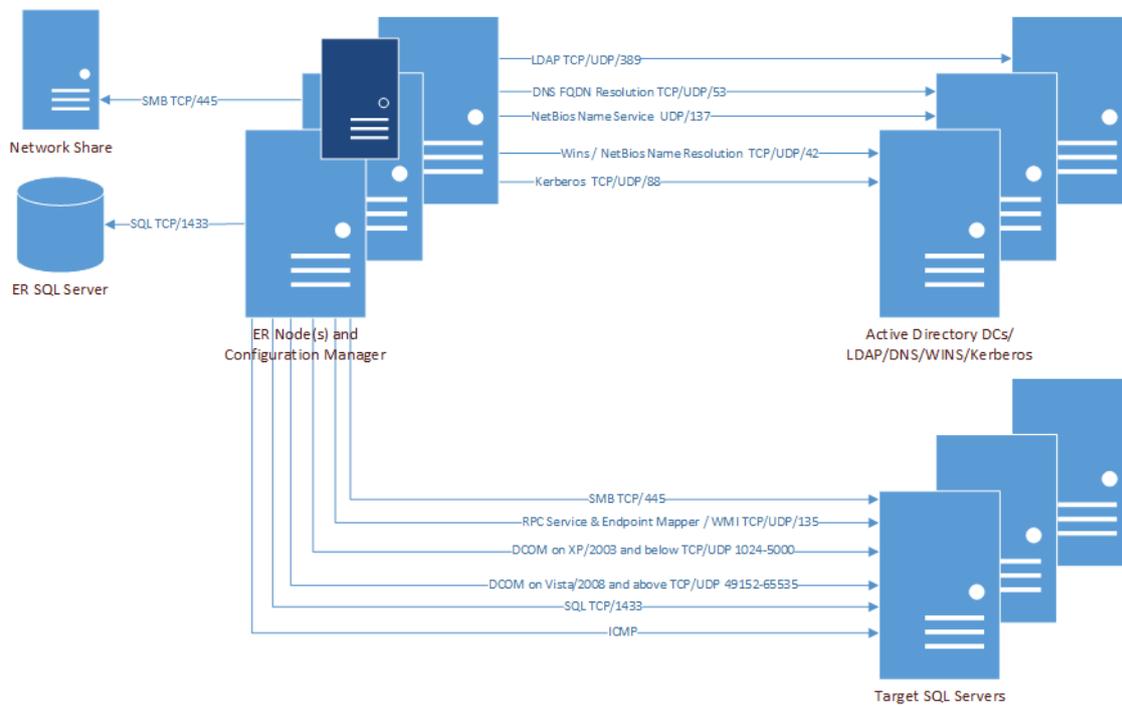
Ports for Enterprise Reporter to connect to Active Roles server

These ports need to be set on Active Roles server and Enterprise Reporter server:

- Active Roles Administration Service open port 15172,1024-65535 TCP Inbound/Outbound
- Active Roles Web Interface open port 80 HTTP Inbound/Outbound
- Active Roles Web Interface open port 443 HTTPS Inbound/Outbound

Port for Enterprise Reporter to connect to IT Security Search

- On the Enterprise Reporter server open port 8087 TCP Outbound
- On the IT Security Search server open port 8087 TCP Inbound

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 19. Firewall requirements for a discovery

Operating System	Firewall Requirement
Windows 2022	**Start	Control Panel	System and Security	Windows Defender Firewall**
	Scroll down and select **Allow an app or feature through Windows Defender Firewall**
	Select **File and Print Sharing and Windows Management Instrumentation (WMI)** (if not already selected)
	The check box in the Domain column will be selected.
	Click **OK**..
Windows 2019	**Start	Control Panel	System and Security	Windows Defender Firewall**
	Scroll down and select **Allow an app through Windows Firewall**
	Select **Windows Management Instrumentation (WMI) and File and Print Sharing** (if not already selected)
	The check box in the Domain column will be selected.
	Click **OK**.
Windows 2016	**Start	Control Panel	System and Security**
	Select **Allow an app through Windows Firewall**
	Select **Windows Management Instrumentation (WMI)** and **File and Print Sharing**
	The check box in the Domain column will be selected.
	Click **OK**.

Table 19. Firewall requirements for a discovery

Operating System	Firewall Requirement
Windows 2012 and Windows 2012 R2	**Start	Control Panel	System and Security** Select **Allow an app through Windows Firewall**. Select **Windows Management Instrumentation (WMI).** The check box in the Domain column will be selected. Click **OK**.
Windows 2008 R2	**Start	Control Panel	System and Security	Windows Firewall**. Select **Allow a program or feature through Windows Firewall**. Select **Windows Management Instrumentation (WMI)**. The check box in the Domain column will be selected. Click **OK**.
Windows 2008	**Start	Control Panel	Windows Firewall**. Select **Allow a program through Windows Firewall**. Select the **Exceptions** tab. Scroll down and select **Windows Management Instrumentation (WMI)** and click **OK**.
Windows 2003 and Windows 2003 R2	Run the following command-line context: netsh firewall set service type = remoteadmin mode = enable
Windows 11	In the center on the Task Bar, select **Search** and type **Windows Defender Firewall** Select **Allow a program or feature through Windows Firewall**. Select **File and Printer Sharing and Windows Management Instrumentation (WMI).** The checkbox in the Domain column will be selected. Click **OK**. Start the **Remote Registry** service and set it to **Automatic**. This step is required to collect data such as installed software, event logs, and security policies.
Windows 8, Windows 8.1, and Windows 10	In the lower left hand corned of the screen right click and select Control Panel. Select **System and Security	Windows Firewall**. Select **Allow a program or feature through Windows Firewall**. Select **File and Printer Sharing** and **Windows Management Instrumentation (WMI)**. The checkbox in the Domain column will be selected. Click **OK**. Start the Remote Registry service and set it to **Automatic**. This step is required to collect data such as installed software, event logs, and security policies.
Windows 7	**Start	Control Panel	System and Security	Windows Firewall**. Select **Allow a program or feature through Windows Firewall**. Select **File and Printer Sharing** and **Windows Management Instrumentation (WMI)**. The checkbox in the Domain column will be selected. Click **OK**. Start the Remote Registry service and set it to **Automatic**. This step is required to collect data such as installed software, event logs, and security policies.

Table 19. Firewall requirements for a discovery

Operating System	Firewall Requirement
Windows Vista	**Start** | **Control Panel** | **Security** | **Windows Firewall**. Select **Allow a program or feature through Windows Firewall**. Select the **Exceptions** tab. Select **File and Printer Sharing** and **Windows Management Instrumentation (WMI)**. Click **OK**.
Windows XP	**Start** | **Control Panel** | **Security Center**| **Windows Firewall**. Select the **Exceptions** tab. Select **File and Printer Sharing**. Click **OK**.

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 16.

See also:

- Configuring the Database and Security Groups

Configuring the Database and Security Groups

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 55.

  > **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 52.

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

> **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

- Installing Enterprise Reporter
- Installing the 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 about how to install all of the Enterprise Reporter components onto one server, see the *Enterprise Reporter Quick Start Guide*.

After the initial installation process is complete, you must 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 98.

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.

See also:

- 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.

> **i** | **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.

To install Enterprise Reporter components

1   Open the self-extracting file named **Enterprise_Reporter_<version number>_x64.exe**.

2   Select a location for the extracted files.

3   In the folder Quest Enterprise Reporter\en-US double-click the **Enterprise_Reporter_<version number>_x64.msi** file.

4   On the Welcome screen of the Setup Wizard, click **Next**.

5   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.

6   Select I **accept these terms**, click **OK** to close the agreement, and click **Next** to continue the installation.

    - OR -

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

7   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.

8   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.

9   If you are installing the Enterprise Reporter server, specify the credentials to 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.

10 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**.

11 Click **Install**.

12 Click **Close**.

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

13 If you have installed the server, you must 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 cannot open the console.

For more information, see Role-Based Security in Enterprise Reporter on page 52.

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 can 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.

For more information, see Security Groups in Enterprise Reporter on page 52.

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 110.

- OR -

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

For help troubleshooting errors, see Database Configuration Issues on page 85.

To use an existing Enterprise Reporter database during the initial installation

> **!** | **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**.

6 Confirm that you have created a backup of your database by selecting I understand and with 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 110.

- 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 85.

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 SSRS
- 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. 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 *Enterprise Reporter Configuration Manager User Guide*.

ℹ️ | **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.

ℹ️ | **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 54.

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.

    > **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 55

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 SSRS

You can configure Enterprise Reporter for publishing reports to SQL Server Reporting Services (SSRS). Once it is configured in your environment, reporting administrators can publish reports from Enterprise Reporter. These reports can then be run from a web browser instead of the Report Manager. For information about installing and configuring Knowledge Portal, see the Knowledge Portal documentation in your download package or CD.

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.

Before you upgrade the components, you must shut down all Enterprise Reporter components. While the upgrade is in progress, data collection will stop and no reports are 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, permissions, 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 and the encryption key. You can restore the backup if there are issues with the upgrade.

> **CAUTION:** If upgrading from Enterprise Reporter 3.2, it is strongly recommended that you 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.

> **NOTE:** During an upgrade, all Exchange Online data that was stored before the upgrade is 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:** 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 abort 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 Open the self-extracting file named **Enterprise_Reporter_<version number>_x64.exe**.

2 Select a location for the extracted files.

3 In the folder Quest Enterprise Reporter\en-US double-click the **Enterprise_Reporter_<version number>_x64.msi** file.

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 and click **Next**.

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

8   Click **Install**.

9   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 56.

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 since 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 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** and click **Next**.

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

     Using the Domain Local group type is recommended. For information on security groups, see Security Groups in Enterprise Reporter on page 52.

9   If required, enter or browse to the domain of the Enterprise Reporter server 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 85.

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 111.

- OR -

Select the **Import Key** option to import an encryption key backup file. For more information, see Importing a key file on page 111.

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 48.

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.

5 Optionally, select **Specify an alternate credential for Node service deployment**, then select the account.

i | **NOTE:** This account must have permission to copy files in the Admin$ share folder and to install and run services.

6 Click **Yes**.

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 that require manual entry of credentials before upgrade will display the message 'Manually configured' in the Service Account column and 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 *Enterprise Reporter Configuration Manager User Guide*.

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 *Enterprise Reporter Configuration Manager User Guide*..

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 20. Enterprise Reporter Licenses

Enterprise Reporter License	Discovery Types Available with License	Report Libraries Available with License
Enterprise Reporter for Windows Servers	• NTFS • Computer • Registry • OneDrive • Azure Resource	• NTFS • Computer • Registry • Microsoft 365 | OneDrive • Change History • Hybrid • Azure | Resources
Enterprise Reporter for Active Directory	• Active Directory • Azure Active Directory	• Active Directory • Azure • Change History • Hybrid
Enterprise Reporter for SQL Server	• MS SQL	• Microsoft SQL Server • Change History
Enterprise Reporter for File Storage Analysis	• File Storage Analysis	• File Storage Analysis
Enterprise Reporter for Exchange	• Exchange • Exchange Online	• Exchange • Microsoft 365 | Exchange Online • Hybrid

Table 20. Enterprise Reporter Licenses

Enterprise Reporter License	Discovery Types Available with License	Report Libraries Available with License
Enterprise Reporter for Microsoft 365	• Azure Active Directory • Azure Resource • Exchange Online • OneDrive • Microsoft Teams • SharePoint Online	• Azure • Microsoft 365 | Exchange Online • Microsoft 365 | OneDrive • Microsoft 365 | Microsoft Teams • Microsoft 365 | SharePoint Online
Enterprise Reporter Suite	• Active Directory • Azure Active Directory • Azure Resource • Computer • File Storage Analysis • Exchange • Exchange Online • Microsoft Teams • SharePoint Online • MS SQL • NTFS • OneDrive • Registry	• Active Directory • Azure • Change History • Computer • Exchange • File Storage Analysis • Hybrid • Microsoft SQL Server • NTFS • Microsoft 365 | Exchange Online • Microsoft 365 | Microsoft Teams • Microsoft 365 | OneDrive • Microsoft 365 | SharePoint Online • 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 3.5.1 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 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 21. 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 affect 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:** 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 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.

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.

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.

To be able to open a console, you 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 22. Security Group and SQL Role Permissions

Security Group	SQL Role	Permissions
Reporter_Discovery_Admins	Discovery_Admin_Role (also known as discovery administrator)	• Access to all functionality in the Configuration Manager
Reporter_Reporting_Operators	Reporting_Operator_Role (also known as reporting user)	• Access to reports that are in the Published Reports and My Reports. • 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) **NOTE:** Users is in the this group: • Can only edit or modify reports after they have been copied from Published Reports to My Reports. • Can only "Set parameters as default" if the report is in My Reports. • Cannot modify or schedule reports that are located in Published Reports. To create a schedule and send a report to a location or through email, users need to copy the report from Published reports and place it into My Reports.

Table 22. Security Group and SQL Role Permissions

Security Group	SQL Role	Permissions
Reporter_Reporting_Admins	Reporting_Admin_Role (also known as reporting administrator)	• 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	• 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 native tools to add the user to the Reporter_Discovery_Admins group.

    ▫ To add an account to the reporting administrator role, use native tools to add the user to the Reporter_Reporting_Admins group.

    ▫ To add an account to the reporting user role, use native tools to add the user to the Reporter_Reporting_Operators group.

    ▫ To add an account to the discovery node role, use native 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.

See also:

- 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,** 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.

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.

> **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 110.

- OR -

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

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

> **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.**

> **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 since 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 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** and click **Next**.

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

Using the Domain Local group type is recommended. For information on security groups, see Security Groups in Enterprise Reporter on page 52.

9   If required, enter or browse to the domain of the Enterprise Reporter server 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 85.

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 111.

- OR -

Select the **Import Key** option to import an encryption key backup file. For more information, see Importing a key file on page 111.

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 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 the 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 37. 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.

  > **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 59.

- 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 56.

> **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.

   - If desired, change the SQL Server or database name.

   - If desired, change the authentication type and provide a user name and password if necessary.

   - If desired, change security groups.

4. Click **OK** to accept the message.

5. Click **Next**.

6. Click **Finish** to close the wizard.

7. When the database has been selected successfully, click **OK** to open the Encryption Key manager.

8. Select the **Export Key** option to create an encryption key backup file. For more information, see Exporting a key file on page 111.

   - OR -

   Select the **Import Key** option to import an encryption key backup file. For more information, see Importing a key file on page 111.

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

- 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.

See also:

- Enterprise Reporter server and database considerations
- Cluster Deployment Considerations
- Discovery Considerations

Enterprise Reporter server and database considerations

You must choose a host computer for Enterprise Reporter server and a SQL Server to host the Enterprise Reporter database. Your decision affects the performance of the product.

The Enterprise Reporter server communicates directly with the database frequently. For best results, locate the Enterprise Reporter server physically close to the SQL Server.

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.

See also:

- 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.

See also:

- Optimize Node Setup

Fine Tune Each Cluster and Node

A discovery is resolved to a number of tasks. Each task is 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 23. 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 Microsoft 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
SharePoint Online	Each tenant

See also:

- 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, Microsoft 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 a 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 the section titled Choosing your Active Directory Scopes in the *Quest Enterprise Reporter Configuration Manager User Guide*.

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 24. 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	•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 25. 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 26. 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 27. 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 28. 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 29. Node Considerations for NTFS Discoveries

	Performance Influences					
# Objects	**Network Bandwidth**	**RAM**	**Disk Speed**	**CPU**	**# Nodes Needed**	**Discovery Settings**
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 that you deploy 10 nodes or less.

Microsoft 365 Discoveries: Node Setup

These considerations apply to Exchange Online, SharePoint 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 30. Node Considerations for Microsoft 365 Discoveries

	Performance Influences				
# Objects	**Network Bandwidth**	**RAM**	**Disk Speed**	**CPU**	**# Nodes Needed**
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.

See also:

- 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 email server for email delivery through an SMTP server or a Microsoft 365 Exchange Online connection.

- Publishing reports to SQL Server Reporting Service (SSRS).

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 31. 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
	Publish to SSRS	Write access to the SSRS server
	Deliver reports by email	Access to the SMTP server
	Enumerate report delivery shares and deliver reports	Read and write access to the delivery share

Table 31. Required Permissions

Account	Use	Permissions
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 32. 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
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
SharePoint Online An account with access to the discovery target tenant.	Collection of all SharePoint Online site collections	Administrator permissions, including tenant settings and policies, site information, and permissions are required. A SharePoint administrator role is recommended.

You also need:

Table 33. 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	Must be a member of the Reporter_Reporting_Admins group
	Publish to SSRS	Write access to the SSRS server
	Deliver reports by email	Access to the SMTP server
	Enumerate report delivery shares and deliver reports	Read and write access to the delivery share
SharePoint Online	Collection of all SharePoint Online site collections	The discovery credentials must have site collection administrator rights to each site collection that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions. Refer to credentials required to create and consent to the Enterprise Reporter SharePoint Online application required for this discovery.

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 77.

- 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 80.

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 89. You can also supply alternate credentials to be used for Node service deployment. This account must have permission to copy files in the Admin$ share folder and to install and run services.

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 27.

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 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 34. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
Active Directory®	• Users 　▪ Token groups count 　▪ Domain controller last logon 　▪ Remote desktop information for domain users 　▪ Photographs for domain users • Groups and Members 　▪ 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	• Users 　▪ Additional attributes from Microsoft 365 　▪ Multi-factor authentication attributes 　▪ Users flagged for risk 　▪ Active user data • Contacts • Devices • Groups 　▪ Additional attributes from Microsoft 365' • Roles • Applications and Service Principals
Azure Resource	• Subscriptions (all or specific) • Resources 　▪ Virtual machines 　▪ Disks 　▪ Networking 　▪ Storage Accounts • Access control 　▪ Nested group members

Table 34. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options
Computer	• Printers • Shares • Volumes • Accounts • Installed Software • Microsoft Store Applications • Hotfixes • Policies • Services • Event Log Configuration • Extended WMI Entities • Nested group members

Exchange	• Mailboxes
	    ▪ Mailbox subfolders
	    ▪ Mailbox delegates
	        ▫ Include system delegates
	• Mail-Enabled Users
	• Mail Contacts
	• Public Folders
	    ▪ System public folders
	• Distribution Groups
	• Permissions
	    ▪ Mailbox AD permissions
	    ▪ Mailbox Exchange permissions
	    ▪ Mailbox folder permissions
	    ▪ Public folder permissions
	    ▪ Optionally, only explicit permissions
	• Nested group members

Table 34. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options

Exchange Online	• Mailboxes
	   ▪ Mailbox delegates
	   ▪ Mailbox statistics
	   ▪ Mailbox folders
	• Public Folders
	   ▪ System Public Folders
	• Mail-Enabled Users
	• Mail Contacts
	• Distribution Groups
	   ▪ Group members
	   ▪ Dynamic group members
	• Permissions
	   ▪ Mailbox folder permissions
	   ▪ Optionally, only explicit permissions
	• Nested group members

File Storage Analysis	• Shares
	   ▪ Hidden Shares
	   ▪ Home Directories
	• Collect NAS using Configuration
	   ▪ If unable to collect volumes then collect shares as volumes
	• Files
	• Folders
	   ▪ Follow Directory Symbolic Links
	• Owners

Microsoft SQL	• 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 76.
MS Teams	• Channels • Files and Folders • Applications

Table 34. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options

NTFS	• How to collect the information:
	
	  ▪ Collect all available public shares
	    □ Include hidden hares
	
	  ▪ Collect all available volumes
	    □ Based on your selected scope, if you are collecting against NAS devices, do you want to use specified NAS Configurations?
	      - Yes
	      - No
	
	  ▪ Collect only selected shares, folders and DFS shares. Collection of all public shares or volumes will not occur.
	
	• Folder options:
	
	  ▪ All folder levels
	  ▪ Folder depth— determines how far into the folder structure to collect data
	
	• File options:
	
	  ▪ 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:
	
	  ▪ 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
	    □ 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.
	
	    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 76.
	
	• Advanced options:
	
	  ▪ 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 34. Collection Options For Each Type Of Discovery

Discovery Type	Collection Options

OneDrive	• Drives
	    ▪ All drives
	    ▪ Selected drives
	• Folders
	    ▪ Files
	• Permissions
	    ▪ Nested group members
	• Configuration Settings

Registry	• 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 76. • 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 Microsoft 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.

Discovery Permission Requirements

The following sections outline the permission requirements for discoveries.

See also:

- Detailed permissions for Enterprise Reporter discoveries
- Permissions for Enterprise Reporter discoveries on NAS devices
- Permissions for Enterprise Reporter tenant applications

Detailed permissions for Enterprise Reporter discoveries

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

Table 35. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Active Directory	An account with Active Directory read permissions is required to collect domain information, trusts, sites, domain controllers, and Active Directory computers, users, groups, and organizational units.
	The account being a member of the Built-in Domain Users group is sufficient to assign read permissions.
	To collect Fine Grained Password Policy and AD object level permissions, Domain Admin is required.
Azure Active Directory	An identity with read permission for the discovery target tenant. Read permissions are required for collection of tenant information, Azure Active Directory users, groups, group members, roles, and service principals.
	If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above.
	Also refer to credentials required to create and consent to the Enterprise Reporter Azure application required for this discovery.

Table 35. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Azure Resource	An identity with read permissions for the discovery target tenant. Read permissions are required for collection of subscription, Resource groups, and resources. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Azure Resource application required for this discovery.
Computer	An account with local administrator access on the scope computers to collect computer information, local groups and users, printers, services, policies, and event logs.
Exchange	To collect from Exchange targets, the credential account must have a mailbox on the target organization with access to read the permissions on the targets through EWS. To collect from Exchange 2013, 2016, or Mixed Modes, the credentials must be a member of the Organization Management Group. To collect from Exchange 2016 or Exchange 2019, the credentials must have an administrator role with an assigned "ApplicationImpersonation" role.
Exchange Online	An account with access to the discovery target tenant. Read permission is required for collection of all Exchange Online information including mailboxes, mailbox delegates, public folders, mail-enabled users, mail contacts, distribution groups, group members, and permissions. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as previously stated.
File Storage Analysis	An account with local administrator access on the scoped computer is required to collect file, folder, share, and home drive analysis data. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 79.
Microsoft SQL	An account with local administrator access on the SQL Server is required. Additionally, the account must have read access to the scoped database to collect database information. At a minimum, if not using fixed roles, the following SQL permissions are required on the securable object being used for collection. • Grant View Any Definition • Grant View Server State • Grant View Connect Any Database • Grant View Select All Securables
Microsoft Teams	The user credentials used to collect Microsoft Teams information must have either the Teams Administrator or Global Administrator permissions. The user must also be a member of each Microsoft Teams group to prevent access denied errors during disk discovery. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Microsoft Teams application required for this discovery.

Table 35. Detailed permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
NTFS	If collecting through the administrator share, an account with local administrator access to the scoped computer is required. If collecting through a network share, an account with read permissions to the scoped shares is required. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter discoveries on NAS devices on page 79.
OneDrive	An account with access to the discovery target tenant. Administrator permissions are required for collection of all drives including drive information, configuration settings, files, folders, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each drive that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter OneDrive application required for this discovery.
Registry	An account with local administrator access to the scoped computer is required to collect registry information.
SharePoint Online	An account with access to the discovery target tenant. Administrator permissions are required for collection of all SharePoint Online site collections, including tenant settings and policies, site information, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each site collection that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter SharePoint Online application required for this discovery.

Permissions for Enterprise Reporter discoveries on NAS devices

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

Table 36. 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.

Table 36. Permissions required for Enterprise Reporter discoveries on NAS Devices

Discovery Type	Permissions Required for Discovery Credential
NetApp Filer	The vFiler can be a discovery target. In this case, the NAS configuration must point to the storage controller from which the vFilers are derived and the credentials must have read access to the storage controller.
Dell Fluid FS	The discovery target can be any Fluid FS VM. The NAS configuration must be the machine name or IP where Dell Enterprise Manager is installed and credentials must have access to Dell Enterprise Manager.
EMC Isilon	The discovery target can be any Isilon virtual machine. The NAS configuration must be the machine or IP that hosts the OneFS administration site and the credentials must have read access to it. By default, the connection is established using https and, if the connection is not deemed to be secure, the discovery will fail.

Permissions for Enterprise Reporter tenant applications

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

Azure Active Directory application permissions

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

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

Table 37. Required permissions

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

Collecting user activity information

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

- Microsoft Graph: Read all usage reports

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

1 Open the Microsoft 365 admin center.

2 Navigate to **Settings | Org Settings | Services**.

3 Select **Reports**.

4 Clear the **Display concealed user, group, and site names in all reports** check box.

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

OneDrive application permissions

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

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

Table 38. Required permissions

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

Azure Resource application permissions

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

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

Table 39. Required permissions

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

Microsoft Teams application permissions

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

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

Table 40. Required permissions

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

SharePoint Online application permissions

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

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

Table 41. Required permissions

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

Troubleshooting Issues with Enterprise Reporter

- 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.

See also:

- 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 55.

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.

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 37.

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 57. You may need to have an administrator with the database creation right run the Database Wizard or installer to create the database.

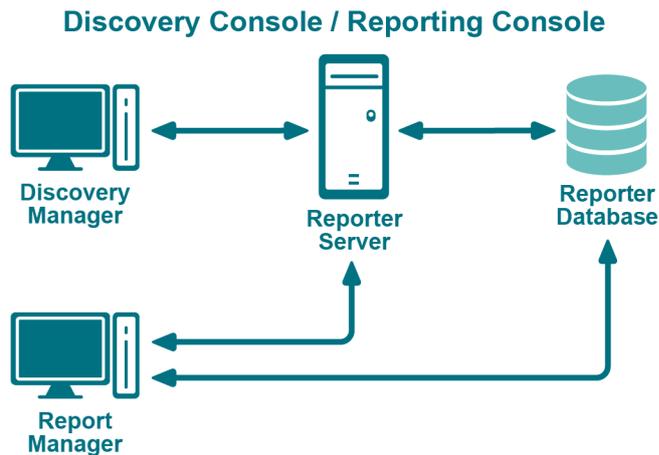The following table outlines possible solutions to each error.

Table 42.

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 55. 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 55.
Could not create all logins	The credentials you used do not have permissions to create logins. Groups do 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 55.
Could not create all SQL roles	The credentials you used do 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 55.
Could not add Service account to all groups	The groups have not been created. The service account does not exist on the domain or SQL Server. The credentials you used do 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 the 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.

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 the SQL Server om which 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 *Configuration Manager User Guide*.

- 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 see Modifying a Cluster in the *Configuration Manager User Guide*. 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—you can change any of them. While most changes are processed smoothly, occasionally issues in the network environment may prevent changes from being applied. When a change fails, you must determine the reason, and manually make the changes.

- If you must manually change a credential on a node, 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.

- Problems deleting a node
- 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. You must have administrative permissions on the node host computer to install the node.

> **i** | **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 *Configuration Manager User Guide*.

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

2   Locate the node installer, Enterprise_ReporterNode_3.5.1.xxxxx_x64.msi (where xxxxx is a unique 5-digit code), in the Quest\Enterprise Reporter\Server folder in the install location.

> **i** | **NOTE:** If you are installing the node on a remote computer, copy the appropriate Enterprise_ReporterNode_3.5.1.xxxxx_x64.msi file to that computer.

3   Run the node installer.

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 is collect 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 that you can examine:

*   The errors generated for a task provide a good starting point for troubleshooting. For more information, see Viewing Statistics on page 128.

*   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 details, see AD Discovery: Optionally select one or more domain controllers on page 80.

*   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 127. 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 details, see Node credential and alternate credential details for on-premises discoveries on page 20.
  - If you have used alternate credentials for the discovery, ensure that they are permissioned correctly.
  - If an Azure or Microsoft 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.
  - 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 88.
  - A task can 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 information about discoveries, see the Enterprise Reporter Configuration Manager User Guide.
- 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 logs for discoveries

Logs can be used to troubleshoot issues with discoveries. 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 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 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**.

    An Export Logs dialog box appears giving a status of the node logs retrieved. Log retrieval may take time depending on the log size and node location on the network. Once the node logs have been retrieved, a link is displayed for the exported logs.

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**.

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

Deleting logs for discoveries

If you want only the most recent issue to be displayed in the logs, you can delete old logs. This deletes logs from the default server Logs folder as well as from the Exported Logs folder, except for the most recently exported logs. You can delete logs for a selected cluster or you can delete all server logs.

To delete logs for a selected cluster

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 **Delete Logs**.

3　If necessary, change the selected cluster.

4　Click **Delete**.

To delete all server 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 **Delete Logs**.

3　Select all the clusters.

If you do not select all the clusters, some node logs may remain without their related server logs.

4　Select the **Delete all server logs** check box.

5　Click **Delete**.

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 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.

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 **Information** and confirm the database location.

Disaster Recovery

The following backup/restore procedure is the Enterprise Reporter 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

*   Backing up Enterprise Reporter
*   Deploying Enterprise Reporter to another computer after a disaster
*   Checking the Enterprise Reporter configuration after recovery

Backing up 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.

Deploying 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 167 and Importing a key file on page 168.

    > **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 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 **Information**.

Review and confirm all of the settings that Enterprise Reporter is currently using.

3   Click 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 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

The Enterprise Reporter Database Content Wizard can be started from the Windows Start menu or from within the main Database Wizard.

To run the Database Content Wizard, you must have control and alter permission on the database. During installation, if the sa account is not selected, the Enterprise Reporter service account is added as a member of the Discovery_Admin_Role and Discovery_Nodes_Role roles. Both accounts have control and alter database permissions.

> **i** | **NOTE:** The Merge and Clean tasks can be destructive so it is highly recommended that only the db_owner runs those tasks. Control database level permissions has the same permissions as db_owner except that it can be assigned or removed by db_owner. Control database level permission has the same permissions as db_owner except that it can be assigned or removed by db_owner.

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. The new database must be created using the Quest® Enterprise Reporter Database Wizard prior to the transfer. 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.

> **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**.

> **!** | **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 prior to the restore. 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.

> **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 and SharePoint Online

- 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 103.

     - 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.

   > **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**.

   > **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.

> **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**.

PowerShell cmdlets

The Enterprise Reporter Database Content Wizard includes PowerShell cmdlets that can be used to schedule database content management tasks.

See also:

- Requirements

- Database Content Wizard cmdlets

- Loading the Database Content Wizard cmdlet

- Backing Up An Enterprise Reporter Database

- Cleaning an Enterprise Reporter Database

- Merging Two Enterprise Reporter Databases

- Restoring an Enterprise Reporter Database

- Transferring an Enterprise Reporter Database

Requirements

- Windows Management Framework 3.0

Database Content Wizard cmdlets

The cmdlets included with the Database Content Wizard are as follows:

- Start-ERBackup
- Start-ERClean
- Start-ERMerge
- Start-ERRestore
- Start-ERTransfer

Loading the Database Content Wizard cmdlet

To load the Database Content Wizard cmdlet (without feedback):

- Import-Module "File path to the DatabaseContentWizardCmdlets.dll"

To load the Database Content Wizard cmdlet (with feedback):

- Import-Module "File path to the DatabaseContentWizardCmdlets.dll" –verbose

To redirect PowerShell error logging

- Append the command with 2>{full path}

    Example: Start-ERBackup 2>C:/error.txt

Backing Up An Enterprise Reporter Database

This section provides details about the Backup task.

Syntax

```
Start-ERBackup [-SourceSqlHost] <string> [-SourceDatabaseName] <string>
[[-SourceUserID] <string>][[-SourcePassword] <string>] [-FilePath] <string>
[-Password] <string> [<CommonParameters>]
```

Parameters

- [-SourceSqlHost] is the name of the SQL Server that holds the source database.
- [-SourceDatabaseName] is the name of the database containing the data to be backed up.
- [-SourceUserID] (optional) is the SQL Server user ID used to connect to the source database. If not provided, Windows credentials are used.
- [-SourcePassword] (optional) is the SQL Server password to the source database. If not provided, Windows credentials are used.
- [-FilePath] is the full path to the backup file, including the file name.
  Example: C:\Users\Jane\Desktop\BackupFile.erbackup
- [-Password] is the password that will be used to encrypt the backup file and will be required to access the file during any restore process. This password is encrypted and is unrecoverable.

To back up a database using Windows authentication

- Provide values for SourceSqlHost, SourceDatabaseName, FilePath, and Password.

        ```
        Start-ERBackup –SourceSqlHost Sample.Sql.Server –SourceDatabaseName
        TestDB –FilePath C:\Users\Bob\Documents\TestDB –Password 77dhw
        ```

To back up a database using SQL Server authentication

- Provide values for SourceSqlHost, SourceDatabaseName, SourceUserID, SourcePassword, FilePath, and Password.

```
Start-ERBackup –SourceSqlHost Sample.Sql.Server –SourceDatabaseName
TestDB –SourceUserID TestUser –SourcePassword fee3td –FilePath
C:\Users\Bob\Documents\TestDB –Password 77dhw
```

Cleaning an Enterprise Reporter Database

This section provides details about the Clean task.

Syntax

```
Start-ERClean [-XmlFilePath] <string> [<CommonParameters>]
```

Parameters

- [-XmlFilePath] is the full path of the XML file used for running the clean task.

To clean a database using Windows authentication

- Provide values for SqlHost and DatabaseName for the SourceSqlParameters element within the XML.

```
Start-ERClean -XmlFilePath C:\Users\Bob\Documents\CleanTask.xml
```

To clean a database using SQL Server authentication

- Provide values for SqlHost, DatabaseName, UserName and Password for the SourceSqlParameters element within the XML.

```
Start-ERClean -XmlFilePath C:\Users\Bob\Documents\CleanTask.xml
```

Merging Two Enterprise Reporter Databases

This section provides details about the Merge task.

> **!** **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.**

Syntax

```
Start-ERMerge [-SourceSqlHost] <string> [-SourceDatabaseName] <string>
[[-SourceUserID] <string>] [[-SourcePassword] <string>] [-TargetSqlHost] <string>
[-TargetDatabaseName] <string> [[-TargetUserID] <string>] [[-TargetPassword]
<string>] [<CommonParameters>]
```

Parameters

- [-SourceSqlHost] is the name of the SQL Server that holds the source database to be merged.

- [-SourceDatabaseName] is the name of the database containing the data that will be moved in the merge.

- [-SourceUserID] (optional) is the SQL Server user ID used to connect to the source database. If not provided, Windows credentials are used.

- [-SourcePassword] (optional) is the SQL Server a to the source database. If not provided, Windows credentials are used.

- [-TargetSqlHost] is the name of the SQL Server that holds the target database.

- [-TargetDatabaseName] is the name of the database that will contain the merged data.

- [-TargetUserID] (optional) is the SQL Server user ID used to connect to the target database. If not provided, Windows credentials are used.

- [-TargetPassword] (optional) is the SQL Server password to the target database. If not provided, Windows credentials are used.

To merge two databases using Windows authentication

- Provide values for SourceSqlHost, SourceDatabaseName, TargetSqlHost and TargetDatabaseName.

```
Start-ERMerge –SourceSqlHost Sample.Sql.Server –SourceDatabaseName
SourceDatabase –TargetSqlHost TargetSample.Sql.Server –TargetDatabaseName
TargetDatabase
```

To merge two databases using SQL Server authentication

- Provide values for SourceSqlHost, SourceDatabaseName, SourceUserID, SourcePassword, TargetSqlHost, TargetDatabaseName, TargetUserID and TargetPassword.

```
Start-ERMerge –SourceSqlHost Sample.Sql.Server –SourceDatabaseName
SourceDatabase –SourceUserID TestUser –SourcePassword fee3td
–TargetSqlHost TargetSample.Sql.Server –TargetDatabaseName TargetDatabase
–TargetUserId TargetUser –TargetPassword fhfsk8
```

Restoring an Enterprise Reporter Database

This section provides details about the Restore task.

Syntax

```
Start-ERRestore [-TargetSqlHost] <string> [-TargetDatabaseName] <string>
[[-TargetUserID] <string>][[-TargetPassword] <string>] [-FilePath] <string>
[-Password] <string> [<CommonParameters>]
```

Parameters

- [-TargetSqlHost] is the name of the SQL Server that holds the target database.

- [-TargetDatabaseName] is the name of the database that the restore task will populate with restored data.

- [-TargetUserID] (optional) is the SQL Server user ID used to connect to the target database. If not provided, Windows credentials are used.

- [-TargetPassword] (optional) The SQL Server password to the target database. If not provided, Windows credentials are used.

- [-FilePath] is the full path to the backup .erbackup file, including the file name with file extension. Example: C:\Users\Jane\Desktop\BackupFile.erbackup

- [-Password] is the password that was be used to encrypt the backup file and is now required to access the file during the restore process.

To restore a database using Windows authentication

- Provide values for TargetSqlHost, TargetDatabaseName. FilePath, and Password.

```
Start-ERRestore –TargetSqlHost Sample.Sql.Server –TargetDatabaseName
RestoreDB –FilePath C:\Users\Bob\Documents\TestDB –Password 77dhw
```

To restore a database using SQL Server authentication

- Provide values for TargetSqlHost, TargetDatabaseName, TargetUserID, and TargetPassword.

```
Start-ERRestore –TargetSqlHost Sample.Sql.Server –TargetDatabaseName
RestoreDB –TargetUserId TestUser –FilePath fee3td –FilePath
C:\Users\Bob\Documents\TestDB –Password 77dhw
```

Transferring an Enterprise Reporter Database

This section provides details about the Transfer task.

Syntax

```
Start-ERTransfer [-SourceSqlHost] <string> [[-SourceDatabaseName] <string>]
[[-SourceUserID] <string>][[-SourcePassword] <string>] [-TargetSqlHost] <string>
[-TargetDatabaseName] <string> [[-TargetUserID] <string>] [[-TargetPassword]
<string>] [-SelectedOptions] <TransferDataSelectionEnum>
{None | ClustersAndNodes | Discoveries | Reports} [<CommonParameters>]
```

Parameters

*   [-SourceSqlHost] is the name of the SQL Server that holds the source database.

*   [-SourceDatabaseName] is the name of the database containing the data that will be transferred into a clean target database.

*   [-SourceUserID] (optional) is the SQL Server user ID used to connect to the source database. If not provided, Windows credentials are used.

*   [-SourcePassword] (optional) is the SQL Server password to the source database. If not provided, Windows credentials are used.

*   [-TargetSqlHost] is the name of the SQL Server that holds the target database.

*   [-TargetDatabaseName] is the name of the database that the data will contain the transferred data.

*   [-TargetUserID] (optional) is the SQL Server user ID used to connect to the target database. If not provided, Windows credentials are used.

*   [-TargetPassword] (optional) is the SQL Server password to the target database. If not provided, Windows credentials are used.

*   [-SelectedOptions] are the three choices of data to transfer in any combination. You may specify each data type using its name or numerical equivalent. ClustersAndNodes (or 1), Discoveries (or 2), and Reports (or 4).

To transfer clusters and nodes, discoveries and reports using Windows authentication

*   Provide values for SourceSqlHost, SourceDatabaseName, TargetSqlHost, TargetDatabaseName. and SelectedOptions.

    ```
    Start-ERTransfer –SourceSqlHost Sample.Sql.Server –SourceDatabaseName
    SourceDatabase –TargetSqlHost TargetSample.Sql.Server –TargetDatabaseName
    TargetDatabase –SelectedOptions 1, 2, 4
    ```

To transfer clusters and nodes, discoveries and reports using SQL server authentication

*   Provide values for SourceSqlHost, SourceDatabaseName, SourceUserID, SourcePassword, TargetSqlHost, TargetDatabaseName, TargetUserID and TargetPassword.

```
Start-ERMerge –SourceSqlHost Sample.Sql.Server –SourceDatabaseName SourceDatabase –
SourceUserID TestUser –SourcePassword fee3td
–TargetSqlHost TargetSample.Sql.Server –TargetDatabaseName TargetDatabase –
TargetUserId TargetUser –TargetPassword fhfsk8 –SelectedOptions ClustersAndNodes,
Discoveries, Reports
```

Appendix: Encryption Key Manager

- 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.

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.

> **i** | **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 beside 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

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 **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 114. 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.

Index

About us

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

Technical support resources

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

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

* Submit and manage a Service Request.

* View Knowledge Base articles.

* Sign up for product notifications.

* Download software and technical documentation.

* View how-to-videos.

* Engage in community discussions.

* Chat with support engineers online.

* View services to assist you with your product.