Quest™ Enterprise Reporter 3.0

Quick Start Guide

Legend

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

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

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

Contents

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

Key Features of Enterprise Reporter

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

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

Using the Configuration Manager, you can:

- Configure your collection environment to minimize network traffic and optimize performance.
- Create discoveries to collect data that will be made available to the Report Manager:
    - information about your Active Directory® environment.
    - information about files and folders from domains, OUs, computers, NetApp® and EMC® filers, shares, and DFS shares and clusters.
    - 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® and Exchange Online™ environments.
    - information about your Azure subscriptions, licenses, and service plans.
    - information about your Azure Active Directory environment.
    - information about files and folders in your OneDrive® environment.
- 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 Knowledge Portal.
- 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® and Exchange Online™ 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.

Enterprise Reporter Components

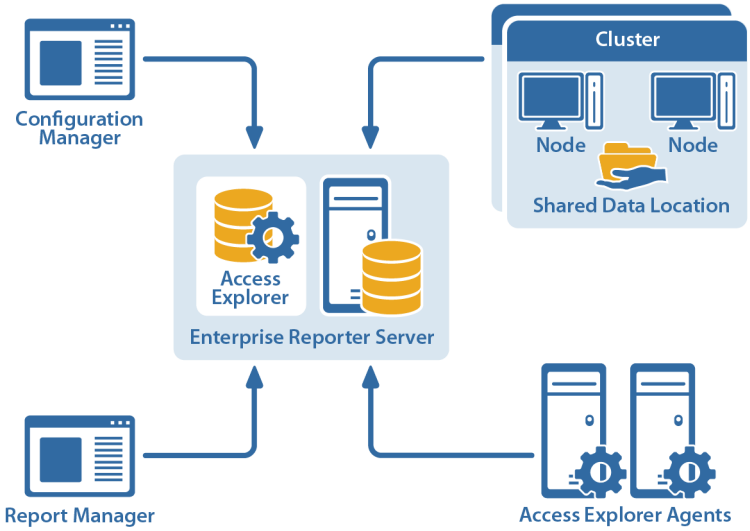
An Enterprise Reporter deployment includes (at minimum):

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

For information on installation, see Installing Enterprise Reporter on page 26.

Enterprise Reporter Architecture

Figure 1. Enterprise Reporter architecture



System Requirements

Before installing Enterprise Reporter 3.0, ensure that your system meets the following minimum hardware and software requirements.

Hardware Requirements

For each component you need the following minimum hardware:

Table 1. Hardware Requirements

	Enterprise Reporter
Memory	• Minimum: 16 GB RAM • Recommended: 16 GB RAM
Processor	• Intel® or AMD 2 GHz multiprocessor (with at least 2 cores) • 64-bit processor
Hard disk space	Disk space requirements will vary with the Enterprise Reporter components you install: • Server - 10 GB • Configuration Manager - 2 GB • Discovery Node - 10 GB for installed files, plus extra space (10 GB - 100 GB) for processing discoveries. Space required varies with the amount of data collected. • Report Manager - 10 GB • Database size varies with the amount of data you collect • The file share that you use for the Shared Data Location will require space for storage of collected data. Space required varies with the amount of data collected. • Total disk size if all components and databases are on the same system - 100 GB

New Required Hardware

The following hardware is required for Enterprise Reporter3.0 and higher.

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

Supported Operating Systems

The following operating systems are supported for Enterprise Reporter components.

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

Table 2. Supported Operating Systems

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

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

Table 3. Supported Operating Systems for Discovery Targets

Supported Operating Systems for Discovery Targets	Licences: Active Directory	Windows Server	File Storage Analysis	SQL Server	Exchange
Domain Functional Levels					
Windows Server® 2016 Functional Level	X				
Windows Server® 2012 R2 Functional Level	X				
Windows Server® 2012 Functional Level	X				
Windows Server® 2008 R2 Functional Level	X				
Windows Server® 2008 Functional Level	X				
Windows Server® 2003 Functional Level	X				
Computers					
Windows Server® 2016		X	X		
Windows Server® 2012 R2		X	X		
Windows Server® 2012		X	X		
Windows Server® Core 2012		X	X		
Windows Server® 2008 R2 with Service Pack 1		X	X		
Windows Server® Core 2008 R2 with Service Pack 1		X	X		
Windows Server® 2008 with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows Server® 2003 R2 with Service Pack 2 (64-bit)		X	X		
Windows Server® 2003 with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows® 10		X	X		
Windows® 8.1		X	X		
Windows® 8 (64-bit and 32 bit)		X	X		
Windows® 7 with Service Pack 1 (64-bit and 32 bit)		X	X		
Windows Vista® with Service Pack 2 (64-bit and 32 bit)		X	X		
Windows® XP Professional with Service Pack 3 (64-bit and 32 bit)		X	X		
Network Attached Storage (NAS) Devices					
Dell Fluid File System 6.0		X	X		
Dell Fuild File System 5.0		X	X		
Isilon One FS® 7.2 - 8.0 and above (Collections require a secure connection to Isilon with a valid certificate.)		X	X		
NetApp® Filer - Data ONTAP® 8..x - 9.x and above (Cluster mode is supported as of version 8.2)		X	X		
SQL Server Instances					

Supported Operating Systems for Discovery Targets	Active Directory Licences	Windows Server Licences	File Storage Analysis Licences	SQL Server Licences	Exchange Licences
SQL Server® Clusters				X	
SQL Server® 2016				X	
SQL Server® 2014				X	
SQL Server® 2012				X	
SQL Server® 2008 R2				X	
SQL Server® 2008 with Service Pack 2				X	
SQL Server® 2005 with Express Service Pack 3				X	
SQL Server® 2005 with Service Pack 3				X	
Exchange Servers					
Exchange Online™					X
Exchange® 2016					X
Exchange® 2013					X
Exchange® 2010					X
Exchange® 2007					X
Exchange® Mixed Modes (2007-2010, 2010-2013, 2007-2013)					X

Active Roles Supported Versions

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

- Active Roles 7.1.2
- Active Roles 7.0.4
- Active Roles 7.0.2
- Active Roles 6.9.0

IT Security Search Supported Versions

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

- IT Security Search 11.3

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® 2016
- SQL Server® 2014
- SQL Server® 2012
- SQL Server® 2008 R2
- SQL Server® 2008 with Service Pack 2
- SQL clusters and database mirroring are supported for your deployment, including
    - SQL Server® 2016 Always On
    - SQL Server® 2014 Always On
    - SQL Server® 2012 Always On

Using SQL Server Certificates

SSL Encryption of SQL Server Connections using Certificates

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

The steps required to configure this encryption are as follows.

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

New Required Software

The following software is required for Enterprise Reporter3.0 and higher.

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

Required Software

The following software is required for Enterprise Reporter.

- Microsoft®.NET Framework 4.6
- Microsoft®.NET Framework 4.0 (Full)
- Microsoft®.NET Framework 3.5 Service Pack 1
- Microsoft® Excel® (required to view reports exported as spreadsheets)
- Microsoft® Excel® 2010
- Microsoft® Excel® 2013
- Microsoft® Visual C++® 2012 Service Pack 1 Redistributable Package (x64) version 11.0.60610.1
- Microsoft® Visual C++® 2010 Service Pack 1 Redistributable Package (x64) version 10.0.40219
- Microsoft® Visual C++® 2005 Service Pack 1 Redistributable Package (x64) version 8.0.59192
- PowerShell™ 3.0

Active Roles Required Software

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

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

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

The following additional considerations are required:

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

Exchange Required Software

To collect Exchange® 2007 information, the following additional considerations are required:

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

Required Services

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

- Net.TCP Port Sharing

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

- Remote Registry

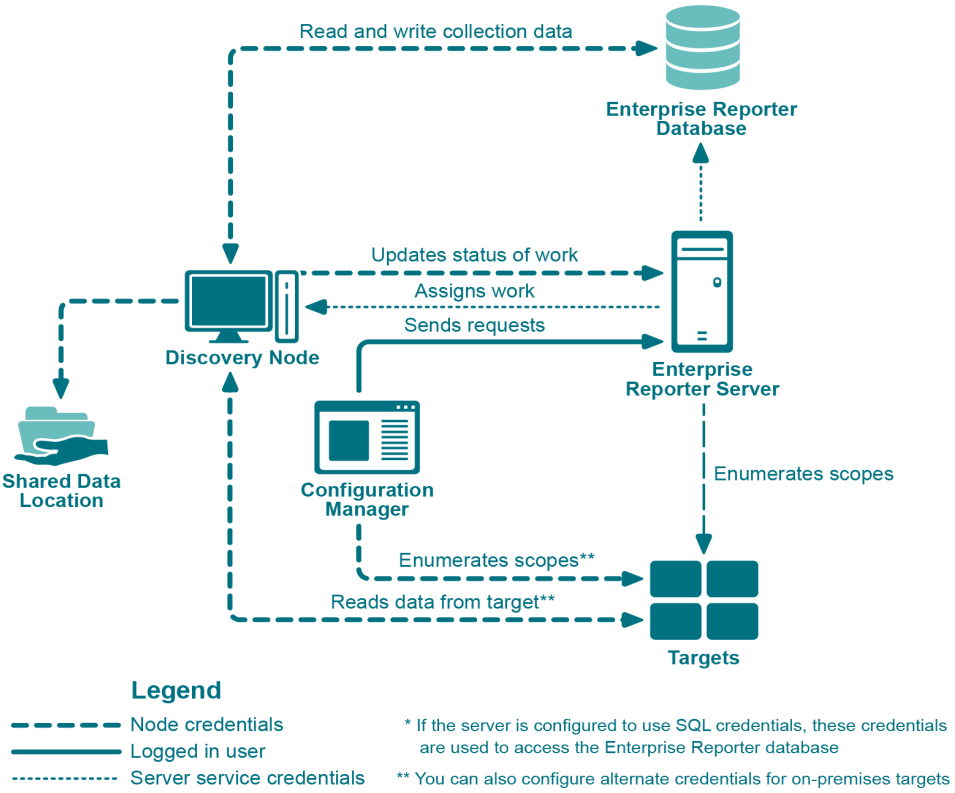
- Windows Management Instrumentation (WMI)

An Overview of the Configuration Manager Security

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

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

Figure 2. Credentials used to communicate in the Configuration Manager



Node Credential and Alternate Credential Details for On-Premises Discoveries

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

If you want to use different credentials for a particular discovery, you can configure them in the Discovery Wizard. By using these alternate credentials, you can target anything on-premises for which you have credentials, in any

domain. You can minimize the permissions given to node credentials, and use alternate credentials for scoping and collecting your on-premises discoveries.

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

Table 4. Node Credentials and Alternate Credentials in Configuration Manager

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

Table 4. Node Credentials and Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Database	There are two options for communicating with the database: 1. You can use the same service credentials that the node service uses. 2. You can specify SQL credentials only for use when the database is accessed. The credentials you choose must be able to read and write to the database.	The account must be in the Reporter_Discovery_Admins security group. (Note that if you use the same account as the Enterprise Reporter server it is already permissioned appropriately). For more information, see Role Based Security in Enterprise Reporter and Configuring the Database in the Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation. If you use SQL authentication to connect with the database, you must manually permission the SQL user, either by adding them to the database role Reporter_Discovery_Admin_Role (recommended) or by permissioning specific tables in the database.
Discovery Node	Targets	Read access on all targets. For on-premises discoveries, all domains with which the credentials have a forest or domain level trust will be enumerated. If required, you can configure alternate credentials for specific discoveries, instead of using the default node credentials.	The targets are defined as part of a discovery. The discovery tasks are assigned to a particular node based on availability, so all nodes in a cluster should have access to all targets defined in all discoveries assigned to the node's cluster. For on-premises discoveries, ensure the node credentials or alternate credentials have read access to the target. In addition, a trust is required between the node computer and the targets. For more information on Azure and Office 365 Discoveries, see Detailed Permissions for Enterprise Reporter Discoveries on page 15.

Detailed Permissions for Enterprise Reporter Discoveries

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

Table 5. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
Active Directory	An account with Active Directory read permissions is required to collect domain information, trusts, sites, domain controllers, and Active Directory computers, users, groups, and organizational units. The account being a member of the Built-in Domain Users group is sufficient to assign read permissions.
Azure Active Directory	An identity with read permission for the discovery target tenant. Read permissions are required for collection of tenant information, Azure Active Directory users, groups, group members, roles, and service principals. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Azure application required for this discovery. For more information, see Using the Tenant Application Manager on page 42.
Computer	An account with local administrator access on the scope computers to collect computer information, local groups and users, printers, services, policies, and event logs.
Exchange	To collect from Exchange targets, the credential account must have a mailbox on the target organization with access to read the permissions on the targets through EWS. To collect from Exchange 2007 targets, the credentials must be a member of the Exchange Organization Administrators Group. To collect from Exchange 2010, Exchange 2013, 2016, or Mixed Modes, the credentials must be a member of the Organization Management Group.
Exchange Online	An account with access to the discovery target tenant. Read permission is required for collection of all Exchange Online information including mailboxes, mailbox delegates, public folders, mail-enabled users, mail contacts, distribution groups, group members, and permissions. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above.
File Storage Analysis	An account with local administrator access on the scoped computer is required to collect file, folder, share, and home drive analysis data. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter Discoveries on NAS Devices on page 16.
Microsoft SQL	An account with local administrator access on the SQL Server is required. Additionally, the account must have read access to the scoped database to collect database information.
NTFS	If collecting through the administrator share, an account with local administrator access to the scoped computer is required. If collecting through a network share, an account with read permissions to the scoped shares is required. For permissions required when collecting NAS devices, see Permissions for Enterprise Reporter Discoveries on NAS Devices on page 16.

Table 5. Detailed Permissions required for Enterprise Reporter discoveries

Discovery Type	Permissions Required for Discovery Credential
OneDrive	An account with access to the discovery target tenant. Administrator permissions are required for collection of all drives including drive information, configuration settings, files, folders, and permissions. A SharePoint administrator role is recommended. Additionally, the discovery credentials must have site collection administrator rights to each drive that is being collected. If additional credentials are being specified to minimize Azure throttling limitations, these credentials must have the same permissions as stated above. Also refer to credentials required to create and consent to the Enterprise Reporter Azure application required for this discovery. For more information, see the Using the Tenant Application Manager section of the Configuration Manager User Guide in the Technical Documentation.
Registry	An account with local administrator access to the scoped computer is required to collect registry information.

Permissions for Enterprise Reporter Discoveries on NAS Devices

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

Table 6. Permissions required for Enterprise Reporter discoveries on NAS Devices

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

Permissions for Enterprise Reporter Tenant Applications

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

OneDrive Azure Application Permissions

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

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

- Microsoft Graph: Read user files
- Office 365 SharePoint Online: Read user files
- Windows Azure Active Directory: Access the directory as signed-in user
- Windows Azure Active Directory: Read directory data

Azure Active Directory Application Permissions

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

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

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

Minimum Permissions for Initially Installing Enterprise Reporter

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

Table 7. 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, and Reporter_Reporting_Operators 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, and Reporter_Reporting_Operators security groups when installing the server.	
Optional SQL credentials Supplied during installation	Can be used to create the Enterprise Reporter database	Must have the right to create databases, logins and groups.
	If supplied, are used to connect the database by the Enterprise Reporter server.	Read and write permissions are automatically granted during database creation.

Port Requirements

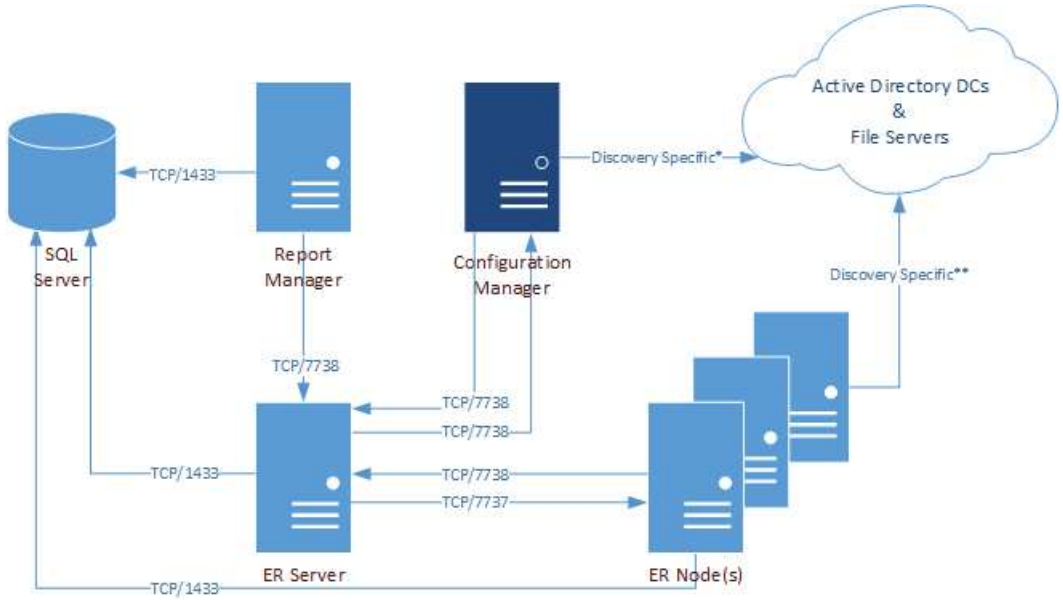
For the Enterprise Reporter components to communicate, some ports must be open.

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

  You can view the port currently in use on the System | Information page in the Configuration Manager, and the System Information tab in the Report Manager.
- The default port used for communication from the Enterprise Reporter server to the nodes is port 7737. This port may be configured during installation.

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

Figure 3. Ports used by Enterprise Reporter components.



*For more information on ports used when creating a discovery, see Table 8.

**For more information on ports used during data collections, see Table 9.

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

Table 8. Ports used by Enterprise Reporter components

Application	Port	Type	Components				
			Configuration Manager[a]	Report Manager	SQL Server	ER Server	ER Nodes
FTP	20, 21	TCP		X			
SMTP	25	TCP	X	X		X	
WINS / NetBiOS Name Resolution	42	TCP UDP				X	
DNS FQDN Resolution	53	TCP UDP	X	X		X	
Kerberos	88	TCP UDP	X			X	
RPC Service & Endpoint Mapper / WMI	135	TCP UDP	X				
NetBIOS Name Service	137	UDP				X	
NetBIOS Datagram (browsing)	138	UDP	X				
LDAP	389	TCP UDP	X				

Table 8. Ports used by Enterprise Reporter components

Application	Port	Type	Components				
			Configuration Manager[a]	Report Manager	SQL Server	ER Server	ER Nodes
SQL	1433	TCP		X	X	X	X
SQL Server Browser Service	1434	TCP UDP	X	X			
Enterprise Reporter Node	7737	TCP				X	X
Enterprise Reporter Server	7738	TCP	X	X		X	X

a.For the Configuration Manager, also include the ports listed in Table 9.

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

Table 9. Ports used by Enterprise Reporter discoveries

Application	Port	Type	Active Directory	Azure Active Directory	Computer	Exchange	Exchange Online	File Storage Analysis	NTFS	OneDrive	Registry	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		
Kerberos	88	TCP UDP	X		X	X*		X	X		X	X
RPC Service & Endpoint Mapper / WMI	135	TCP UDP			X	X**		X	X		X	X
NetBIOS Name Service	137	UDP	X		X	X		X	X		X	X
Remote Registry	139	TCP			X	X		X	X		X	
ICMP					X			X	X		X	X
LDAP	389	TCP UDP	X		X	X		X	X		X	X
HTTPS	443	TCP UPD		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
LDAP GC	3268	TCP	X			X						
Exchange PowerShell	12067	TCP				X**						
DCOM on Vista/2008 and above (uses an open port in this range)	49152 - 65535	TCP UDP			X	X		X	X			X

*Exchange 2010 and higher, **Exchange 2007 only

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

Figure 4. Ports used by Active Directory collections

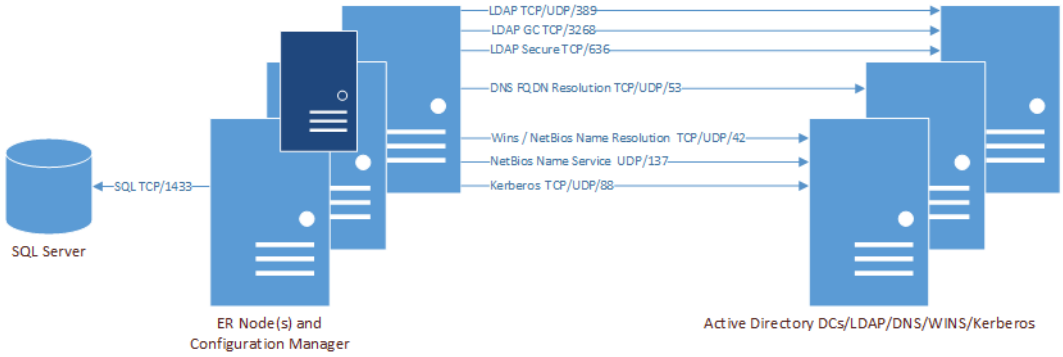


Figure 5. Ports used by Azure and OneDrive collections

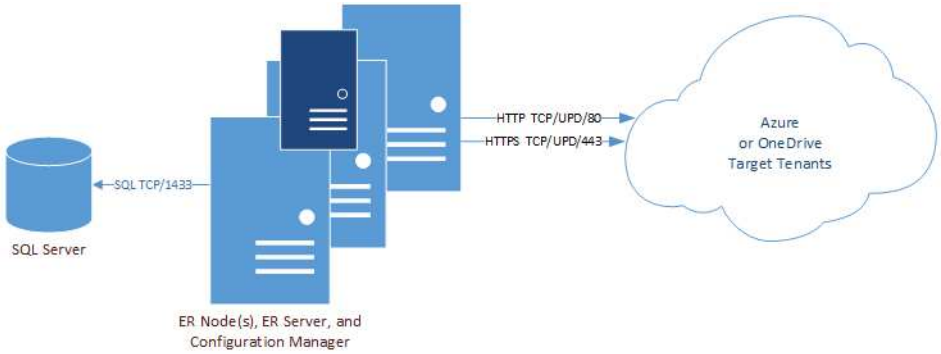


Figure 6. Ports used by Computer collections

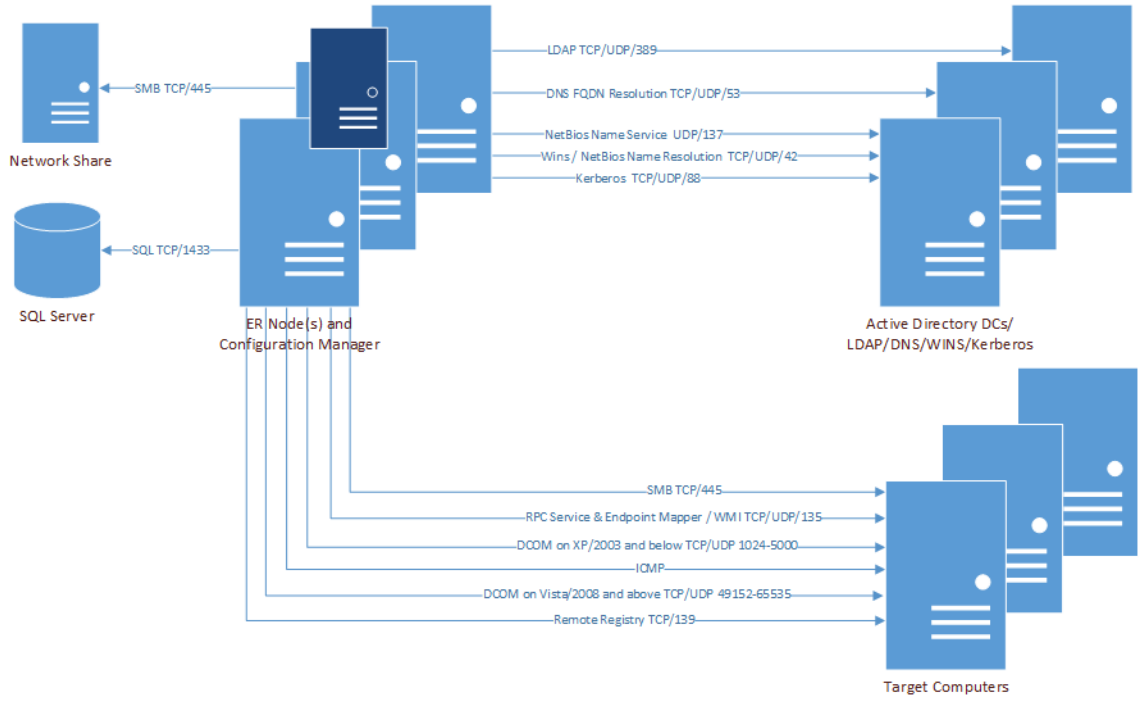


Figure 7. Ports used by Exchange collections

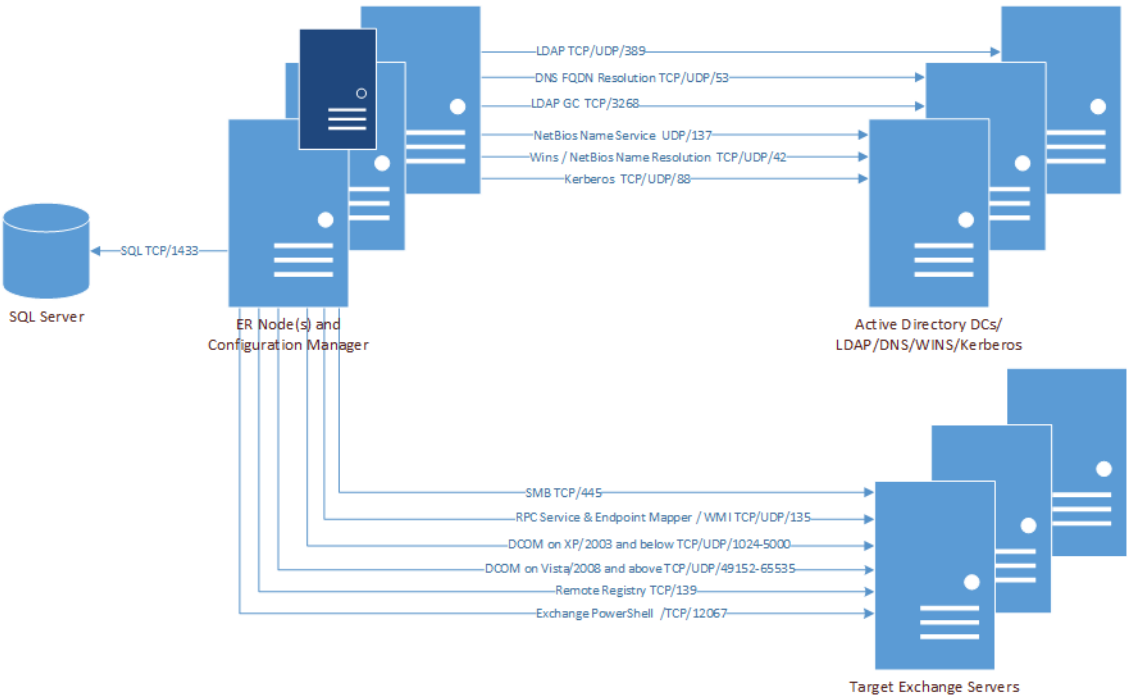


Figure 8. Ports used by Exchange Online collections

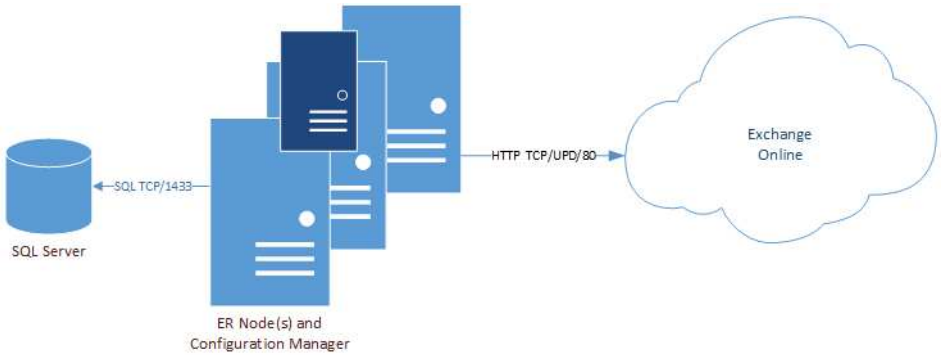


Figure 9. Ports used by File Storage Analysis collections

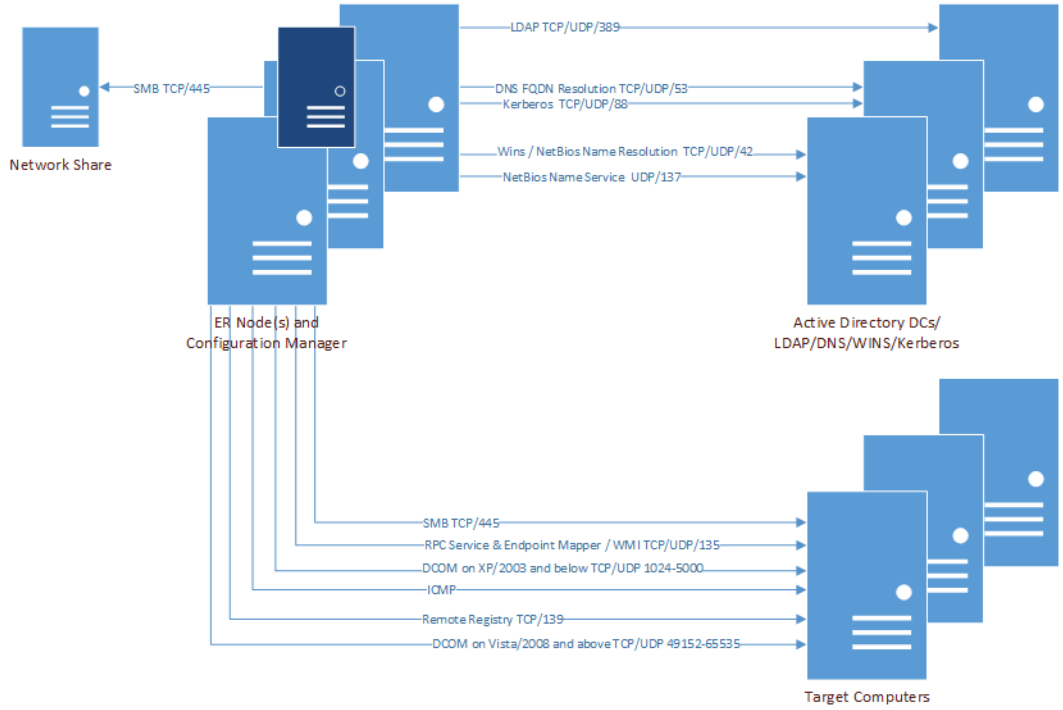


Figure 10. Ports used by NTFS collections

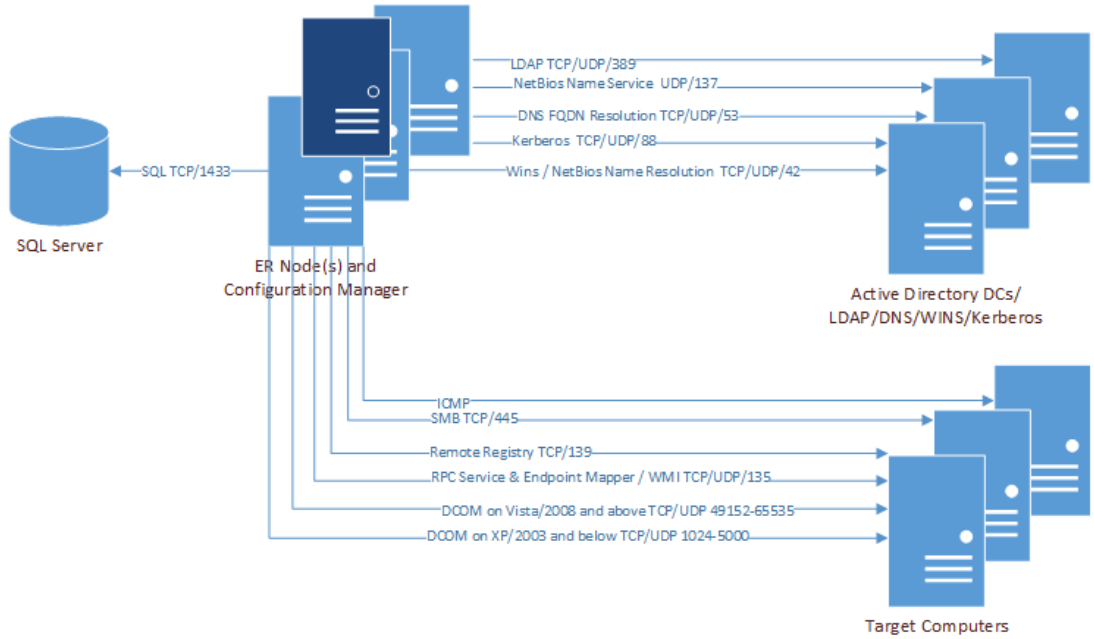


Figure 11. Ports used by Registry collections

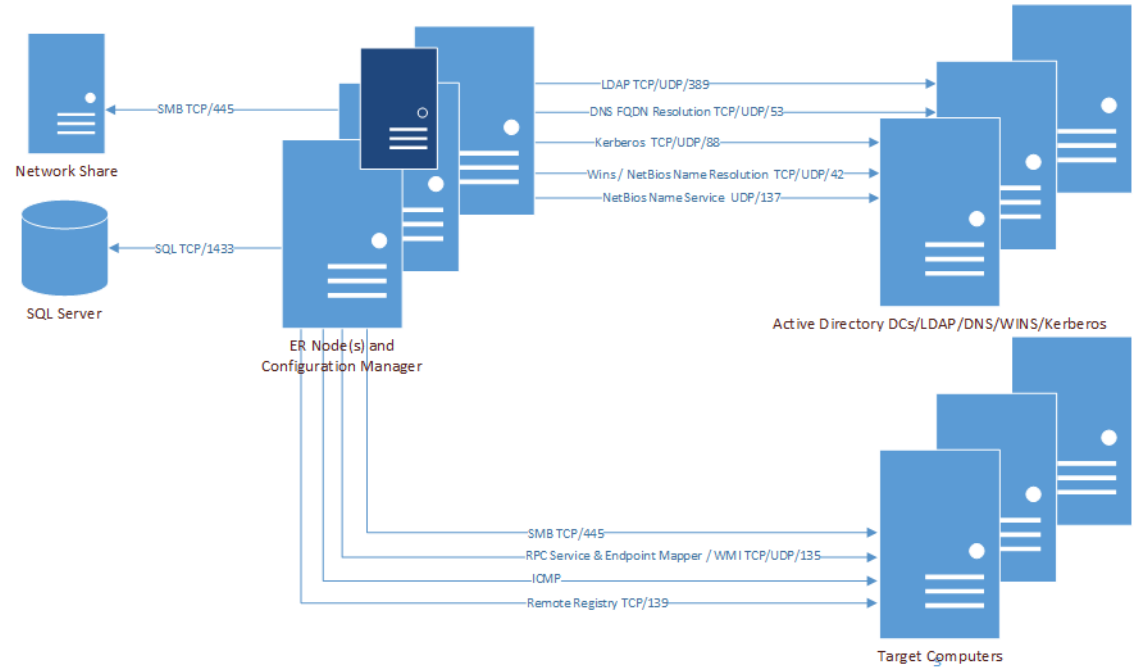
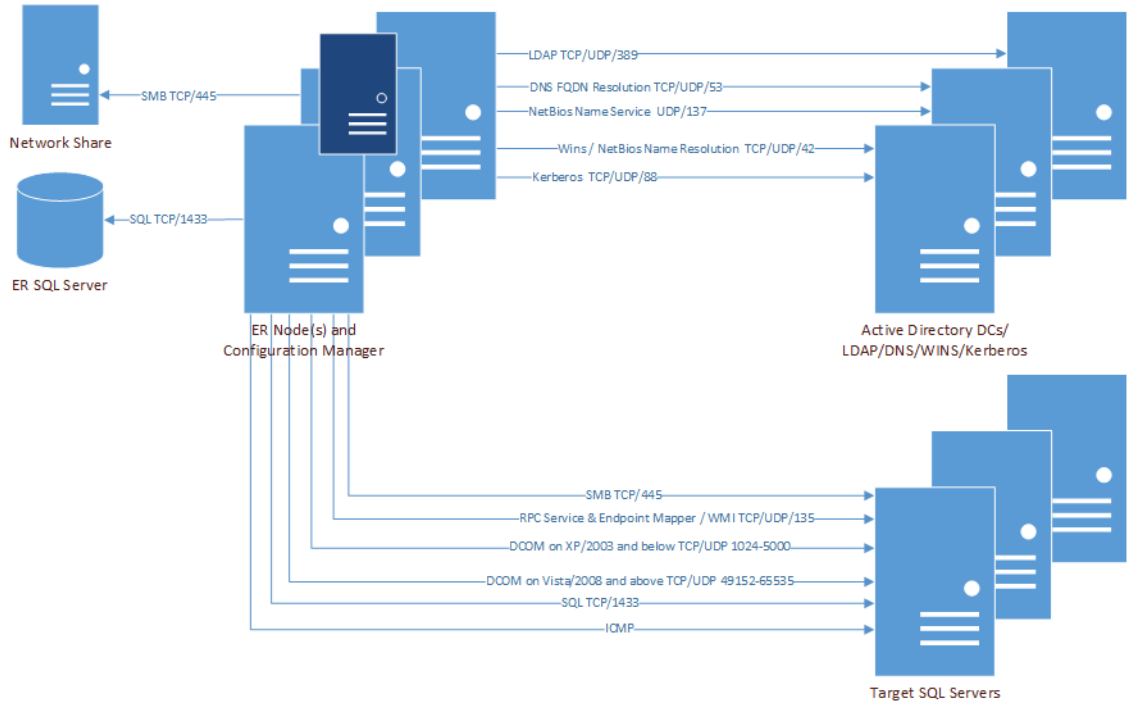


Figure 12. Ports used by SQL collections



Installing Enterprise Reporter

Once you have ensured that your computers meet the system requirements, you can install the Enterprise Reporter server and consoles, and set up the Enterprise Reporter database. For full information on installing Enterprise Reporter, see Installing and Configuring Enterprise Reporter in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

To install Enterprise Reporter components

1 Open the Autorun.

You can access all product documentation on the Documentation tab of the Autorun. You can also use the Autorun to set up the Knowledge Portal and IT Security Search.

2 On the Home page, click the **Enterprise Reporter Setup** tab.

3 Click **Open** next to the edition of **Quest Enterprise Reporter** for your operating system (64 bit).

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 to accept the agreement**, click **OK** to close the agreement, and click **Next** to continue the installation.

- OR -

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

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 that will be used by the Enterprise Reporter server service, and click **Next**.

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

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 Select the country where you are installing the product, and click **Next**.

12 Review the Software Improvement Program overview, and click **Next**.

- OR -

If you are presented with the option to opt in or opt out of the Software Improvement Program, make your selection, and click **Next**.

You may also opt in or opt out of the program after installation is complete. Select **Configuration Manager | System | Configuration** or **Report Manager | System Configuration**, and click **Change software improvement preferences.**

13 Click **Install**.

14 Click **Close**.

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

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

- OR -

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

For more information, see Role Based Security in Enterprise Reporter in the Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation.

Create/Connect Your Enterprise Reporter Database

Next, you must create the Enterprise Reporter database. The Database Wizard appears automatically when you install the Enterprise Reporter server.

1 Choose **Create/Connect 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**.

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 in the Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation.

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 Optionally, accept the default to start the Reporter Server.

This option starts the Enterprise Reporter Server service that must be running for Enterprise Reporter to function.

11 Click **Finish** to create the database.

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

For help troubleshooting errors, see Database Configuration Issues in the Quest Enterprise Reporter Installation and Deployment Guide in the Technical Documentation.

Configure Enterprise Reporter Licenses

You need either a trial or full license to use Enterprise Reporter. Activate or update your license in the Configuration Manager on the System | Information page. 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.

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**.

Create Your First Enterprise Reporter Cluster and Node

The Configuration Manager contains a wizard that walks you through the process of creating clusters and nodes. You can create a cluster without a node, and add the nodes later, but you will not be able to run a discovery without an enabled node.

To create your first cluster and node

1. On the Manage Discovery Clusters pane, click **Create Cluster**.
2. Enter a name for the cluster.

   A default name, First Cluster, is provided, but you should change this to something meaningful, such as the location of your cluster.
3. Browse to your shared data location, and click **OK**.

   - OR -

   Select **No network share specified**.

   For more information, see Things to Consider Before Creating a Cluster in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

   If desired provide a description.
4. Click **Next**.

   If you do not wish to add any nodes at this time, skip to step 11.
5. Browse to the computer where the node is to be created, and click **OK**.

   If you do not change the default entry, the first node is created on the current computer.
6. Select an account from the Credential Manager.

   If the account you want is not on the list, click **Add**, enter the account, and select it from the list.

   NOTE: These credentials are also used to access the target computers during a discovery, unless alternate credentials are specified for a discovery.

   For more information, see Using the Credential Manager in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

   To use SQL credentials to connect to the database, select **Database Credential**, choose **SQL Authentication**, and select the SQL account from the Credential Manager.
7. Configure the number of concurrent tasks the node can process.

   For more information, see Nodes in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

   Click **Add**.

   You can add more than one node at a time to the same cluster. Repeat steps 6 through 9 until you have added all of your nodes.

   By default, nodes are enabled after they are created. If you prefer to manually enable the nodes, clear the Enable Node check box. At least one node must be enabled in order for your cluster to be functional.
8. Click **Finish**.

   If you chose to create a cluster without any nodes, click Yes.

The new node appears on the Discovery Nodes tab. Your node will be enabled, unless you cleared the Enable the nodes check box.

For a listing of possible node statuses, see What does the status of a node or cluster indicate? in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

NOTE: When a node is deployed and enabled, the cluster is also enabled. If you deployed the node without enabling it, you have to manually enable the cluster.

For more information, see Enabling a Cluster in the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

Step-By-Step Walkthroughs

Enterprise Reporter is a very flexible reporting tool, that can be used for many different purposes. This section uses examples of common uses to highlight how to set up Enterprise Reporter to maximize its potential.

- Pre- and Post-Migration Assessment — Assess your network environment before migrating to identify any issues, and re-assess once the migration is complete to ensure that everything went as planned.
- Manage Compliance — Set up reports to automatically generate and be delivered, minimizing the time you have to spend demonstrating compliance.
- Change History Reporting — Track changes in your network environment using Change History Reporting. You can monitor changes to hardware, SQL databases, files, folders and so on.
- File Storage Consolidation — Prepare for storage migration by identifying and excluding from migration files that are unused, orphaned, or are in violation of your storage usage policy.

This walkthrough will guide you through each of these use cases for Enterprise Reporter. Each scenario shows you how to leverage Enterprise Reporter to get the information you want when you need it.

NOTE: These scenarios assume you have installed Enterprise Reporter and set up the database. For more information, see Installing Enterprise Reporter on page 26.

Pre- and Post-Migration Assessment

Before you migrate computers and users to a new environment, you should assess their current state. Using reports generated by Enterprise Reporter, you can ensure that everything is ready to be migrated. Once the migration is complete, you can re-assess to ensure your environment is as you expect, and identify any issues that need resolving.

Scenario

You have received a request to identify all users, groups, and group memberships for a particular domain, and to provide it in Excel format for tracking purposes. This same report will be required after migrating all users to a new domain.

You will need to take the following steps:

1. Configure a Cluster to Perform the Data Discovery
2. Create a Discovery to Define the Data Collection
3. Run the Discovery to Collect the Data
4. Run the Reports You Need and Export Them to Excel

Configure a Cluster to Perform the Data Discovery

You must configure at least one cluster. A cluster is a logical collection of one or more computers (nodes) on which discoveries are executed. A discovery must be assigned to a cluster. A cluster can access an optional shared data location for discovery data. This reduces network traffic, and the processing load on the server.

TIP: In order to reduce network traffic and avoid delays in communication, a cluster should serve a single geographic location.

Clusters are created in the Configuration Manager. To ensure you have the necessary access to the consoles and reports, make sure you are still logged in to your computer with the same user account that you used to install Enterprise Reporter.

If you do not have the Configuration Manager open, perform the following steps:

To connect to a server

1. Click the **Start** menu and select **All Programs** | **Quest** | **Enterprise Reporter** | **Configuration Manager**.
2. Type the name of the server.

   - OR -

   Click **Browse**, and locate the computer where the server is installed.

   Once you have connected to a server, the server name is stored in the list for future use.
3. If necessary, type in the port number.
4. Click **Connect**.

   If this is your first time opening the console, you will need to provide your country so your status in the Software Improvement Program can be determined. You can choose to participate by configuring the software improvement settings on the System | Configuration page.

The Create Cluster wizard walks you through the process of setting up a cluster. If you want to create a new Cluster, see To create your first cluster and node on page 29.

Create a Discovery to Define the Data Collection

Once you have configured a cluster, you can begin setting up discoveries. Discoveries define the targets from which you will be collecting data. Enterprise Reporter uses a "collect all" model. After you run a discovery, you can run reports that include the data you have collected.

In this scenario, you need to collect all users, groups, and group memberships for a particular domain, therefore you need to create an Active Directory® discovery. You will assign the discovery to the cluster you just created.

To create an Active Directory discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery** | **Active Directory**.
2. On the name page, enter **AD - [Domain Name]** so you can identify the discovery easily once you have a list of discoveries.
3. Since you only have one cluster, it is automatically selected, and you can click **Next**.
4. On the Scopes page, click **Add** to choose your domain.
5. Browse to the domain for which you want to collect data, click **Include**, and click **OK** to close the Browse dialog box.

   If you only wanted to know about a specific OU, you can drill into the domain and select it. The parent domain is automatically included, but only the OU will be collected.

6 To shorten collection time, you can select only the options you want to collect. Clear the following options: **Computers**, **Domain Controllers**, **Permissions**, **Trusts, Sites, Deleted Objects, and Active Roles Virtual Attributes**.

7 For the **Users** option and the **Groups and Members** option, select the main heading and clear all sub-options.

By carefully considering the data your reporting users require, you can ensure that collection time is minimized.

8 Click **Next**.

9 Since we want to run this discovery right away, no schedule is necessary and you can click **Finish**.

Run the Discovery to Collect the Data

You can schedule discoveries or run them on demand. In this case, we want to collect this data right away. Each discovery is broken down into tasks, which are assigned to the node for processing. If you have more than one node, Enterprise Reporter uses load balancing to ensure the most efficient processing. You can track the progress of your discovery.

To run a discovery

1 On the Manage Discoveries page, select the discovery **AD - [Domain Name]**.

2 Click **Run**.

3 To view the progress of the discovery, click the **Processing** link in the Next Run column.

When the discovery is complete, the status in the Last Run Status column will change. If there were any errors during collection, click the status to view the details of the last run.

Run the Reports You Need and Export Them to Excel

Once data is collected, you can run reports against it. When you run a report, it returns data based on the most recent data collected by the discoveries, the selected fields, and any parameter values you enter. Some reports may have required parameters; in this case, the report will not run unless you enter valid parameter values.

To produce the requested information, you must run three reports that are included in Enterprise Reporter:

- Domain Groups — shows all the groups in the domain.
- Domain Groups and Members — shows the members of all groups in the selected domain.
- Domain Users — shows all the users in the domain

Once you have run a report, you can export it to the Excel format.

To run each report

1 Open the Report Manager by selecting **Start** | **All Programs** | **Quest** | **Enterprise Reporter** | **Report Manager**.

2 In the connection dialog box, enter the name of the computer where the server is hosted and click **Connect**.

3 On the Report tab, expand **Report Library** | **Active Directory** and select your first report, for example Domain Groups.

4 In the **Include the following domains** parameter, type the domain name, and click **Add**.

You also can click **Search**, locate and add the domain, and click **OK**.

5 Click **Run Report**.

The report appears in a new window. Depending on the amount of data, it may take a few minutes to generate.

6 On the tool bar, click the **Export Document** drop-down arrow, and choose **XLS** (older versions of Excel or XLSX (Excel 2007 and later).

7 In the Export Options dialog box, click **OK**.

8 In the Save As dialog box, select a location for the report, and change the name if desired.

9 Click **Save**.

10 Click **Yes** to view the report in Excel.

You can now use the spreadsheet as needed to perform pre- and post-migration analysis.

You can repeat this process for the other two reports. Once you have completed the migration, you can create a new discovery to run against the new domain, and ensure that the migration was successful.

Manage Compliance

If you are required to regularly show compliance with corporate or regulatory security requirements, Enterprise Reporter can be of great assistance by automatically gathering information and reporting on it.

Scenario

At the beginning of each month, you must deliver a report that shows that users who have been inactive for three months have their accounts disabled, in line with your corporate security policy. You are going to use two reports to do this: one report for yourself, in order to identify accounts that are not compliant, and one report that is sent to the stakeholders showing compliance. You will automate the delivery of the monthly report, to ensure it is always on time. You will need to take the following steps:

1 Modify an Existing Report

2 Schedule the Discovery

3 Schedule Report Delivery to Stakeholders

Modify an Existing Report

You need to modify an existing report to only show accounts that have been inactive for 90 days and are not disabled. You should manually run an appropriate Active Directory® discovery right before you run the report to ensure you are getting up to date data. This will allow you to address any issues before your compliance report is sent out. To do this, you must perform the following steps:

1 Copy the report from the Library to My Reports, which is the only container in which you can edit reports.

2 Edit the report to remove unnecessary fields from the report, and to create a hidden parameter to filter disabled accounts.

3 Modify the report layout to remove unnecessary fields.

4 Run the report to identify issues.

To copy the report so you can edit it

1 On the Report tab of the Report Manager, expand **Report Library** | **Active Directory.**

2 Locate the **Domain Users without Recent Logons** report, and drag it into the **My Reports** container.

To edit the report name, fields, and parameters

1 In the My Report container, select the **Domain Users without Recent Logons** report, and click **Edit Report**.

2 Change the report name to **Domain Users to be Disabled**.

3 Change the report description to **Shows users in the selected domains who have not logged on in the past 90 days and whose accounts are still enabled**.

4 Select the **Fields** tab.

5 In the Selected Fields list, select **Is Locked** and **Number of Logons**, and click **Remove**.

A warning dialog box appears, indicating that the report layout needs to be updated. Click **Yes**.

You could skip this step, however your report will be more usable if it contains only the required information.

6 Select the **Parameters** tab.

7 Click **+Create**.

8 Set the Usage to **Hidden**.

9 Set the associated field to **IsDisabled**.

10 Set the operator to **Equals** and the value to **No**.

11 Click **OK**.

Leave the dialog box open so you can modify the layout.

To modify the report layout

1 In the Edit Report dialog box, click the **Layout** tab.

It may take a few seconds for the layout to generate.

2 Click **Edit**.

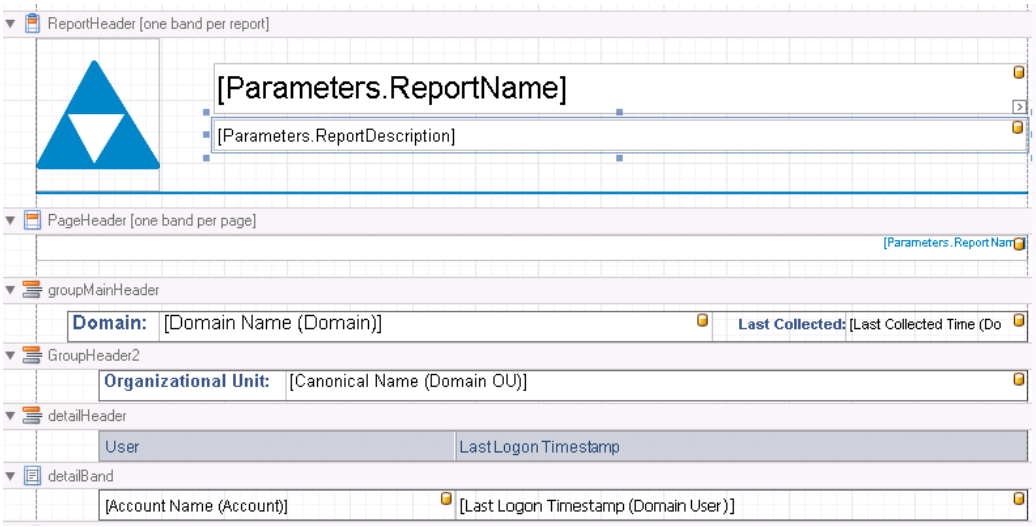
3 To change the report title, double-click in the text box containing the current title, and replace the text with **Domain Users to be Disabled**.

4 In the detailHeader row of the report layout, right-click **Number of Logons**, and select **Delete**.

5 Repeat for **IsDisabled** and **IsLocked**.

6 In the detailBand row of the report layout, remove all fields except **Account Name** and **Last Logon (Domain User)**.

7 Check your report layout to ensure it is accurate:



8 Click **OK** to close the Edit Report dialog box.

9 Click **OK** to close the Edit Report Definition dialog box, and finish editing the report.

To run the report and save the parameter values for future report runs

1 If necessary, in the My Reports container, select the **Domain Users to be Disabled** report.

2 In the **Include the following domains** parameter, type the domain name, and click **Add**.

   You can also click **Search**, locate and add the domain, and click **OK**.

3 In the **Users not logged on in the last (days)** parameter, change the number of days to **90**.

4 To make these the default parameter values, click **Save parameters as default**, and click **OK** in the confirmation dialog box.

5 Click **Run report**.

Your report appears, listing all users who are not in compliance. You can now make any changes you need prior to the sending the compliance report to your stakeholders.

Schedule the Discovery

In this scenario, the Active Directory® collection previously configured collects the necessary data. We will edit it to run on a scheduled basis, so that the scheduled reports have up-to-date data. You can also run it manually before you run the report you modified that identifies any compliance issues.

To edit a discovery and create a schedule

1 On the Manage Discoveries page of the Configuration Manager, select the **AD - [Domain Name]** discovery you created, and click **Edit**.

   - OR -

   If you did not create an Active Directory® discovery that collects accounts, follow the steps in Create a Discovery to Define the Data Collection on page 31, but stop on the Schedule page.

2 If necessary, click the **Schedule** tab.

3 Click **Monthly**, and select the last Friday of the month.

4 Click **+Add**.

5 Click **OK** if you edited an existing discovery.

   - OR -

   Click **Finish** if you created a new discovery.

Schedule Report Delivery to Stakeholders

Once the data has been collected, the reports can be generated. Using the Schedule tab of the Report Manager, you can create a schedule that will automatically deliver the desired reports to your specified recipients.

To do this, you must:

1 Copy the Domain Users without Recent Logons report to My Reports, the only container from which you can schedule a report.

2 Create a report schedule.

3 Configure your SMTP server.

4 Schedule the report, and provide parameter values.

To copy the report so you can schedule it

1 On the Report tab of the Report Manager, expand **Report Library** | **Active Directory.**

2 Locate the **Domain Users without Recent Logons** report, and drag it into the **My Reports** container.

   If you did not rename the report when you modified an existing report (see Modify an Existing Report), the report will have a (1) after its name so you can differentiate them.

To create a report schedule

1. In the Report Manager, click the **Schedule** tab.
2. Click **+New Schedule**.
3. Name the schedule **Compliance Reports**.
4. Click **Monthly**, and select day **1** of the month.
5. Launch the Credential Manager, and add an account that has read access to the database.
6. In the Delivery section, choose a network share where the reports will be delivered.

   Ensure the credentials provided in the previous step have write access to this share.

   Leave the dialog box open to configure email delivery.

To configure email delivery

1. In the Delivery section of the Create or Edit Schedule dialog box, enable the **Send Email** option.
2. Click **Configure mail server**, and enter the server name and port number.
3. Launch the Credential Manager, and select the account used to access the mail server.

   If your SMTP server is configured to accept anonymous connections, you do not need to provide an account.

   You can test your connection to ensure the mail server is properly configured.
4. In the From field, type the email address of the sender.
5. In the To field, type the email addresses of the recipients, separated by a comma or semicolon.
6. Click **OK**.

   The schedule card is created.

To schedule a report

1. On the Compliance Reports schedule card, click **+Schedule Report**.
2. Select **Domain Users without Recent Logons**, and click **OK**.
3. In the Parameters pane, in the Description text box, type **[Domain Name] Users not logged in for 90 days** to identify the parameter values you will use.
4. In the **Include the following domains** parameter, type the domain name, and click **Add**.

   You can also click **Search**, locate and add the domain, and click **OK**.
5. In the **Users not logged on in the last (days)** parameter, change the number of days to **90**.
6. Click **Save**.

Your report will now run automatically, reporting on the data from your scheduled discovery.

Change History Reporting

Enterprise Reporter can help you quickly identify changes that have occurred in your environment. If you enable change history, a record of all changes over time is kept. You can then report on these changes, and ensure that required changes have been made, or investigate unwanted changes. You can track changes to:

- Group membership
- Active Directory® domains
- Computers
- NTFS files, folders or shares

- Registry keys or values
- SQL servers or databases

Scenario

As part of your job, you are responsible for monitoring changes to critical services. Once a week, you must generate a report to ensure only expected changes are being made. Since collecting change history involves more data, you want to scale up your cluster to handle the increased traffic. You will need to take the following steps:

- Add Another Node to a Cluster
- Enable Change History for the Computer Discovery Type
- Create and Schedule a Discovery
- Schedule the Report

Add Another Node to a Cluster

Each target is assigned to a node, balancing the distribution across the nodes until all the nodes are processing as many tasks as they are able. If no nodes are available to process the task, it must wait until a node becomes available.

When you run a computer discovery, each computer in the discovery is separate task that can be assigned to a node. In this case, adding nodes will speed up the performance of your discovery. This is particularly important as we are collecting change history data as well, which will increase the time taken to process each task.

In this scenario, you are going to add another node to handle collecting more data from a larger number of targets.

To create a node

1. On the Manage Discovery Clusters pane, select the cluster you created.
2. In the bottom pane, on the Discovery Nodes tab, click **Add Node**.
3. Browse to the computer where the node is to be created, and click **OK**.
4. Select the service account from the Credential Manager.

   If you want to use a different account, you can add it to the Credential Manager.
5. Click **Add**.

   All other configuration is optional.

Enable Change History for the Computer Discovery Type

You configure change history at a global level for each discovery. All discoveries of that type will collect this data. When you create a discovery, the Name page indicates whether change history is enabled for the discovery type.

In this scenario, it is important to enable change history before running the first discovery, so that all changes are captured.

To enable history for a computer discovery

1. On the Discovery Management | Configuration page, click **Configure global change history settings**.

   A button shows the current status of the change history configuration for each discovery type.
2. For the Computer discovery type, click **Disabled** to toggle the setting.

   The button changes to Enabled, indicating that Change History data will be collected.
3. Click **Close**.

Create and Schedule a Discovery

Since you need this weekly, you can create a weekly discovery. In this simple case, we are assuming that the targeted computers are located relatively close together. If they were very dispersed, you would create different discoveries in the appropriate cluster to ensure faster collections. Each computer should only be in one discovery, so while we are going to configure the discovery to collect the minimal needed data, if at a later time more information is needed, this discovery should be expanded, rather than creating a new one to gather the new data.

To create and schedule a computer discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery** | **Computer**.
2. On the name page, enter **Computer Services** so you can identify the discovery easily once you have a list of discoveries.
3. Since you only have one cluster, it is automatically selected, and you can click **Next**.
4. On the Scopes page, click **Add** to choose your computers.
   Browse to locate the computers, click **Include**, and click **OK** to close the Browse dialog box.

   - OR -

   On the Scopes page, click **Import** to add computers from a file.
   Browse to locate the file containing the computers to add, select the file, click **Open** to start the import, review the import results, and click **OK** to close the results screen. For more information, see the Importing Computers to Your Scopes section of the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.
5. To shorten collection time, you can select only the options you want to collect. Click **Deselect All** and then select the **Services** check box.

   Remember that if you later decide to collect more information from the targeted computers, you should edit this discovery, not create a new one.
6. Click **Next**.
7. Click **Weekly** and schedule the discovery to run once a week.
8. Click **Finish**.

Schedule the Report

When you are scheduling a report with time-sensitive information in it, you must make sure the discovery has time to finish collecting all of its data before you run the report. For small, simple discoveries, this should be easy to predict, but for large discoveries, or discoveries that are slowed down by network issues, such as nodes placed far from their targets or connectivity problems, it may take a few runs to learn how long it will take.

For more details on the steps to take to schedule a report, see Schedule Report Delivery to Stakeholders on page 35.

To copy the report so you can schedule it

1. On the Report tab of the Report Manager, expand **Report Library** | **Change History** and drag the Computer Change History report to **My Reports**.
2. On the Schedule tab, click **+New Schedule,** and enter **Service Changes** as the schedule name.
3. Create a weekly schedule for a time after the discovery will complete.
4. Launch the Credential Manager, and add an account that has read access to the database.
5. In the Delivery section, choose a network share where the reports will be delivered.

   Ensure the credentials provided in the previous step have write access to this share.
6. In the From field, type the email address of the sender.

This assumes that the mail server delivery has already been set up as outlined in Schedule Report Delivery to Stakeholders on page 35.

7 In the To field, type the email addresses of the recipients, separated by a comma or semicolon.

8 Click **OK**.

The schedule card is created.

To add the report

1 On the Service Changes schedule card, click **+Schedule Report**.

2 Select **Computer Change History**, and click **OK**.

3 In the Parameters pane, in the Description text box, type **Changed services on [computer names]** to identify the parameter values you will use.

4 In the **Include the following domains** parameter, type the domain name, and click **Add**.

You also can click **Search**, locate and add the domain, and click **OK**.

5 In the **Include the following computers** parameter, click **Search**, and add the computers you targeted.

If you want to add all computers in the selected domains, you can use the * wildcard, and click **Add** instead of searching for specific computers.

6 In the **Include the following changes** parameter, click **Search** and add **Services**.

7 Click **Save**.

Your report will now run automatically, reporting on the data from your scheduled discovery.

File Storage Consolidation

Before you migrate computers to a new environment, you should assess their file storage. Using reports generated by Enterprise Reporter, you can ensure that only the required data is moved.

Scenario

You have received a request to get ready for storage migration and consolidation by identifying (and excluding from migration) files that are duplicate, unused, orphaned or that violate storage usage policy.

You will need to take the following steps:

1 Configure a Cluster to Perform the Data Discovery

2 Create Discoveries to Define the Data Collection

3 Run the Discoveries to Collect the Data

4 Run the Reports You Need

Configure a Cluster to Perform the Data Discovery

You must configure at least one cluster. A cluster is a logical collection of one or more computers (nodes) on which discoveries are executed. A discovery must be assigned to a cluster. A cluster can access an optional shared data location for discovery data. This reduces network traffic, and the processing load on the server.

TIP: In order to reduce network traffic and avoid delays in communication, a cluster should serve a single geographic location.

Clusters are created in the Configuration Manager. To ensure you have the necessary access to the consoles and reports, make sure you are still logged in to your computer with the same user account that you used to install Enterprise Reporter.

If you do not have the Configuration Manager open, perform the following steps:

To connect to a server

1. Click the **Start** menu and select **All Programs** | **Quest** | **Enterprise Reporter** | **Configuration Manager**.
2. Type the name of the server.

   - OR -

   Click **Browse**, and locate the computer where the server is installed.

   Once you have connected to a server, the server name is stored in the list for future use.
3. If necessary, type in the port number.
4. Click **Connect**.

   If this is your first time opening the console, you will need to provide your country so your status in the Software Improvement Program can be determined. You can choose to participate by configuring the software improvement settings on the System | Configuration page.

The Create Cluster wizard walks you through the process of setting up a cluster. If you want to create a new Cluster, see To create your first cluster and node on page 29.

Create Discoveries to Define the Data Collection

Once you have configured a cluster, you can begin setting up discoveries. Discoveries define the targets from which you will be collecting data. Enterprise Reporter uses a "collect all" model. After you run a discovery, you can run reports that include the data you have collected.

In this scenario, you need to collect information about the files and folders stored on particular servers and then analyze it. Since there is information you will need at the server level, the folder level, and the file level, and then you will analyze it, you need to create multiple discoveries targeting the same computers to collect each type of information.

- File Storage Analysis discovery to assess the file storage information
- Computer discovery to collect server information
- NTFS discovery to collect file and folder information

To create a File Storage Analysis discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery** | **File Storage Analysis**.
2. To name the discovery, enter **File Storage Analysis - [Server Name]** so you can identify the discovery easily once you have a list of discoveries.
3. Since you only have one cluster, it is automatically selected, and you can click **Next**.
4. On the Scopes page, click **Add** to choose the computer to analyze.
5. Browse to the computer for which you want to collect data, click **Include**, and click **OK** to close the Browse dialog box.

   If you want to include additional computers, navigate to each one and include it.
6. To populate reports with the applicable information to analyze, select the following collection options: **Files**, **Folders Shares**, **Owners**.
7. Click **Next**.
8. Since we want to run this discovery right away, no schedule is necessary and you can click **Finish**.

To create a Computer discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery** | **Computer**.
2. To name the discovery, enter **Computer - [Server Name]** so you can identify the discovery easily once you have a list of discoveries.
3. Since you only have one cluster, it is automatically selected, and you can click **Next**.
4. On the Scopes page, click **Add** to choose your computer.
5. Browse to the same computers as the File Storage Analysis Discovery as you want to collect information from the same computers, click **Include**, and click **OK** to close the Browse dialog box.

   If you included additional computers in the File Storage Analysis discovery, navigate to each one and include it in this discovery as well.
6. To populate reports with the applicable information to analyze, select the following collection options: **Shares**, **Volumes**, and **Accounts**.
7. Click **Next**.
8. Since we want to run this discovery right away, no schedule is necessary and you can click **Finish**.

To create an NTFS discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery** | **NTFS**.
2. On the name page, enter **NTFS - [Server Name]** so you can identify the discovery easily once you have a list of discoveries.
3. Since you only have one cluster, it is automatically selected, and you can click **Next**.
4. On the Scopes page, click **Add** to choose your computer.
5. Browse to the same computers as the File Storage Analysis Discovery as you want to collect information from the same computers, click **Include**, and click **OK** to close the Browse dialog box.

   If you included additional computers in the File Storage Analysis discovery, navigate to each one and include it in this discovery as well.

   To populate reports with the applicable information to analyze, select only the following options:

   - For all computers resolved in the discovery, collect: **Folders on all volumes**
   - For this discovery, collect through: **The network share**
   - Recursion Options: **All folder levels**
6. Click **Next**.
7. Optionally, you could narrow the discovery by selecting specific files; however, we will collect all files for this scenario.
8. Click **Next**.
9. Since we want to run this discovery right away, no schedule is necessary and you can click **Finish**.

Run the Discoveries to Collect the Data

You can schedule discoveries or run them on demand. In this case, we want to collect this data right away. Each discovery is broken down into tasks, which are assigned to the node for processing. If you have more than one node, Enterprise Reporter uses load balancing to ensure the most efficient processing. You can track the progress of your discovery.

To run the discoveries

1. On the Manage Discoveries page, select the discovery **File Storage Analysis - [Server Name]**.
2. Click **Run**.

3 Repeat steps 1 and 2 for each of the other discoveries.

4 To view the progress of a discovery, click the **Processing** link in the Next Run column.

When a discovery is complete, the status in the Last Run Status column will change. If there were any errors during collection, click the status to view the details of the last run.

Run the Reports You Need

Once the discovery information is collected, you can run reports against it. When you run a report, it returns data based on the most recent data collected by the discoveries, the selected fields, and any parameter values you enter. Some reports may have required parameters; in this case, the report will not run unless you enter valid parameter values.

To produce the requested information, you must run a File Storage Analysis report in Enterprise Reporter. The Files and Folders report contains the following sections:

- Storage Cleanup Summary - space recommended for cleanup on all servers
- Duplicate Files - space wasted by duplicate files on the servers
- Against Policy File Category - space used by against policy files on the servers (includes wasted space and media files)
- Orphaned Files- space used by files for which the owner is unknown
- Old Data - spaced used by files which have not been accessed in over a year

You can drill down from this report to more detailed reports for each specific section within this report. The following example illustrates this process starting with the Against Policy File Category.

To drill down from this report to more detailed reports

1 On the Storage Cleanup report, scroll to the **Against Policy File Category**.

2 Click any **server name** and the FSA - Files by Category report is displayed showing the number of files, size, and size on disk for the Against Policy category on that server.

3 Click the **Against Policy** category link and the FSA - File Category Details report is displayed showing the 10 file types that are using the most space.

4 Scroll down to the corresponding table and click on any **file extension** link (such as JPG) and the NTFS - File Information by Extension report is displayed showing all files with this extension on the selected computers.

5 Optionally, click the Next Report or Previous Report buttons in the toolbar to navigate between reports you have viewed.

You can repeat this process starting with the File Storage Analysis Files and Folders report. You can drill down through the various sections of the report to identify files that are duplicate, unused, orphaned or that violate storage usage policy.

About Quest

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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

View services to assist you with your product.