Quest® Enterprise Reporter 3.6

Quick Start Guide

© 2025 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100
Aliso Viejo, CA 92656

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

Patents

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

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. Active Directory, Microsoft Entra ID, Microsoft 365, Microsoft Teams, Microsoft 365, OneDrive, PowerShell, SharePoint, SQL Server, Teams, Windows, and Windows Server are trademarks and registered trademarks of the Microsoft Corporation and the Microsoft group of companies.

All other trademarks and registered trademarks are the property of their respective owners.

Legend

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.

Enterprise Reporter Quick Start Guide
Updated - November 2025
Software Version - 3.6

Contents

Introducing Quest® Enterprise Reporter 4
Key Features of Enterprise Reporter 4
Enterprise Reporter Components 6
Enterprise Reporter Architecture 6
System Requirements 6
Minimum permissions for installing Enterprise Reporter 6
Kerberos Requirements 7
Port Requirements 7
Installing Enterprise Reporter 15
Create/Connect Your Enterprise Reporter Database 16
Configure Enterprise Reporter Licenses 17
Activating or Updating Your License 18
Create Your First Enterprise Reporter Cluster and Node 19
Step-By-Step Walkthroughs 20
Pre- and Post-Migration Assessment 20
Manage Compliance 23
Changing History Reporting 26
File Storage Consolidation 29
Microsoft 365 and Microsoft Entra ID Reporting 32

About us 37
Technical support resources 37

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 Microsoft Entra subscriptions, licenses, and service plans
    - information about your Microsoft Entra 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 Microsoft Entra 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 Microsoft Entra ID reports to answer questions about your Microsoft Entra subscriptions, licenses, and settings.
- Use the Microsoft Entra ID reports to answer questions about your Microsoft Entra environment.
- Use the Azure resource reports to answer questions about your Azure resources.
- Use 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.

NOTE: Azure Active Directory is now Microsoft Entra ID.

Enterprise Reporter Components

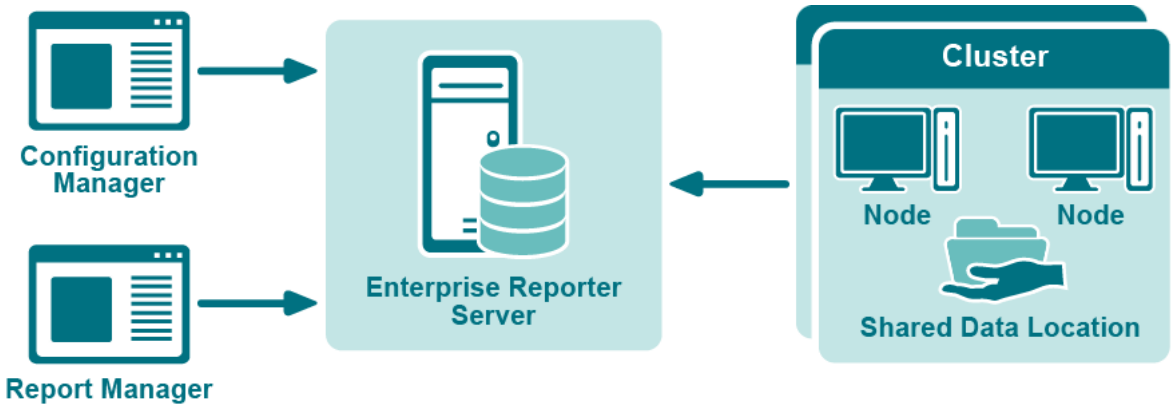
An Enterprise Reporter deployment includes (at minimum):

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

For information on installation, see Installing Enterprise Reporter.

Enterprise Reporter Architecture

Figure 1. Enterprise Reporter architecture



System Requirements

Before installing Enterprise Reporter, ensure that your system meets the minimum hardware and software requirements. See the Enterprise Reporter Release Notes for details.

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 1. 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 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.

Kerberos Requirements

If the network is using Kerberos for authentication, then there is an option to enter a UPN or SPN for both the Enterprise Reporter server and the node during install. This allows the node and Enterprise Reporter server to communicate in a Kerberos only environment.

Port Requirements

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

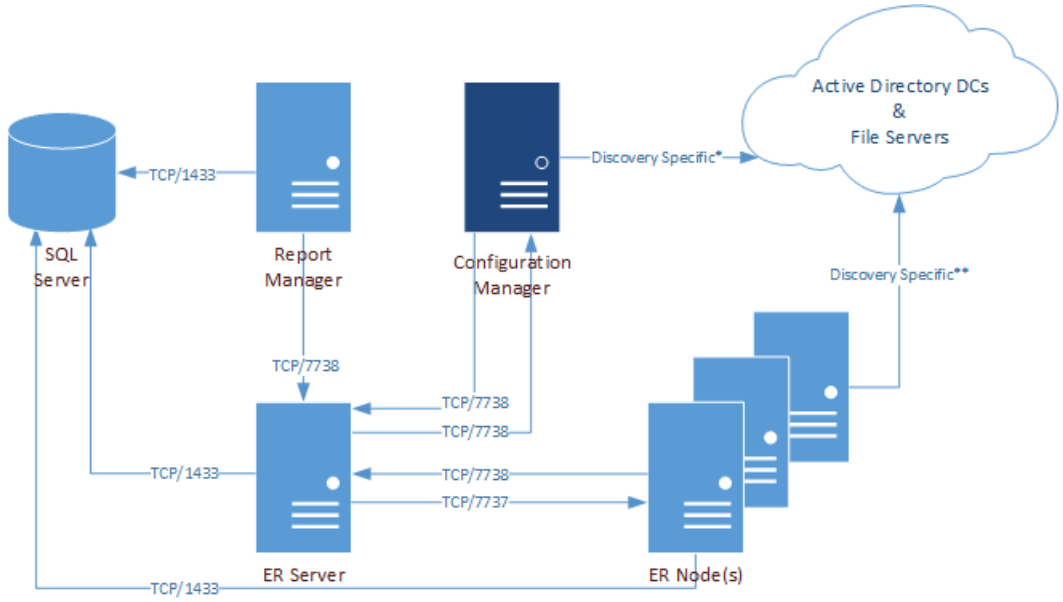
- The default port used for communication between the server and the consoles is 7738. This port is also used by the nodes to access the server. The port is configured during installation of the server, and is required in the connection dialog box for both the Configuration Manager and the Report Manager.

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 2. Ports used by Enterprise Reporter components.



*For more information on ports used when creating a discovery, see Table 2.

**For more information on ports used during data collections, see Table 3.

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

Table 2. Ports used by Enterprise Reporter components

Application	Port	Type	Components				
			Configuration Manager	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				

Table 2. Ports used by Enterprise Reporter components

Application	Port	Type	Components				
			Configuration Manager	Report Manager	SQL Server	ER Server	ER Nodes
NetBIOS Name Service	137	UDP				X	
NetBIOS Datagram (browsing)	138	UDP	X				
LDAP	389	TCP UDP	X				
SQL	1433	TCP		X	X	X	X
SQL Server Browser Service	1434	TCP UDP	X	X			
Enterprise Reporter Node	7737	TCP				X	X
Enterprise Reporter Server	7738	TCP	X	X		X	X

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

Table 3. Ports used by Enterprise Reporter discoveries

Application	Port	Type	Active Directory	Microsoft Entra ID	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		
DNS FQDN Resolution	53	TCP UDP	X			X	X		X		X		X		
HTTP	80	TCP		X	X		X*	X		X		X		X	
Kerberos	88	TCP UDP	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		
Remote Registry	139	TCP				X	X		X		X		X		
ICMP						X			X		X		X		
LDAP	389	TCP UDP	X			X	X		X		X		X		
HTTPS	443	TCP UDP		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							
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 3. Ports used by Active Directory collections

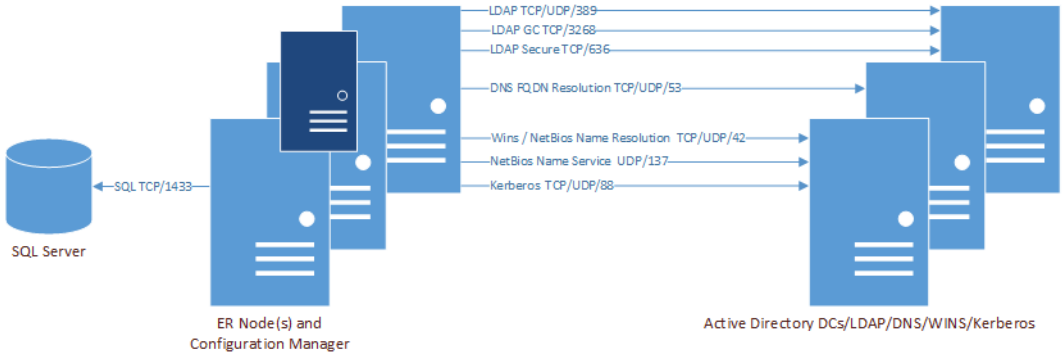
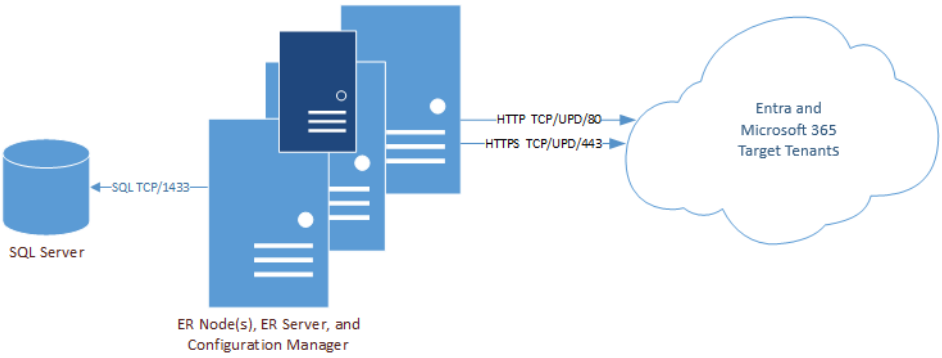


Figure 4. Ports used by Microsoft Entra ID and Microsoft 365 collections (Exchange Online, MS Teams, OneDrive, and SharePoint Online)



Additional ports for Microsoft Entra ID and Microsoft 365 discoveries to be set on the Node:

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

Figure 5. Ports used by Computer collections

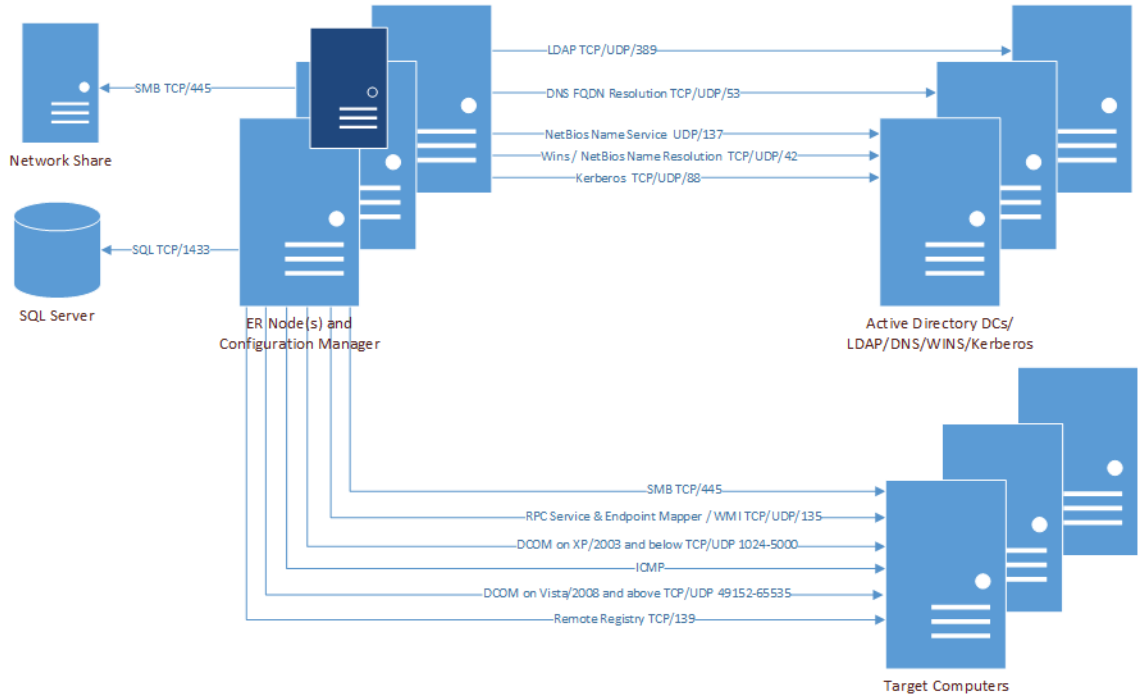
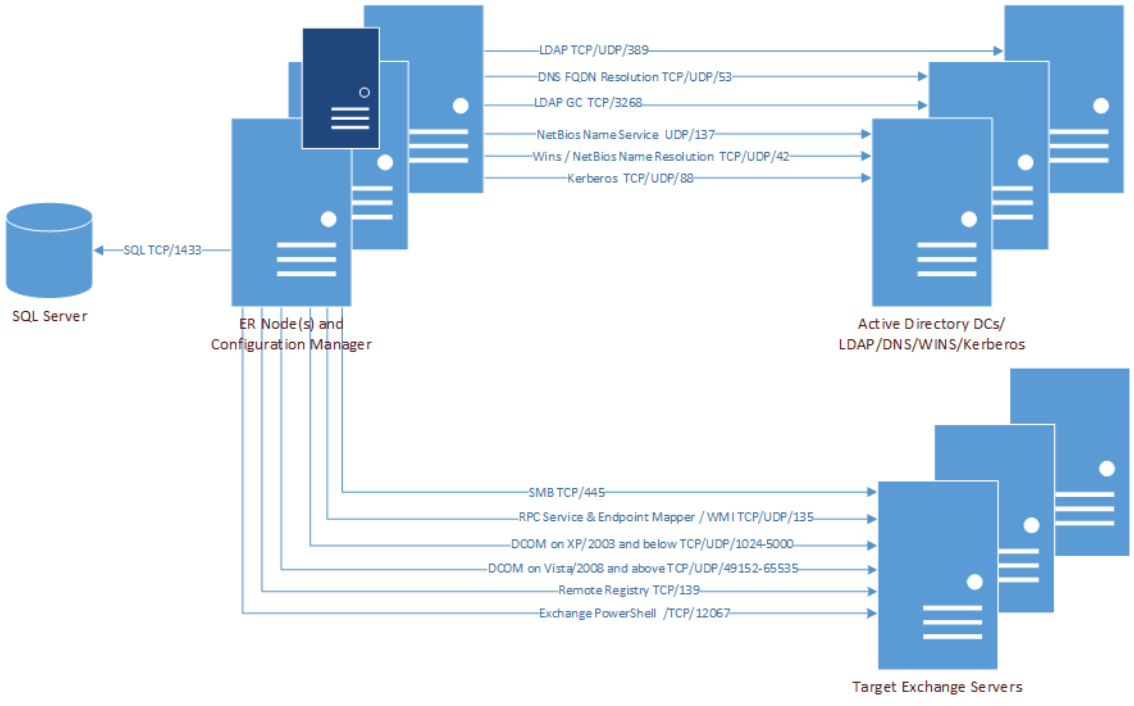


Figure 6. Ports used by Exchange collections



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

- Open WinRM HTTP port 5985 TCP Outbound

Figure 7. Ports used by File Storage Analysis collections

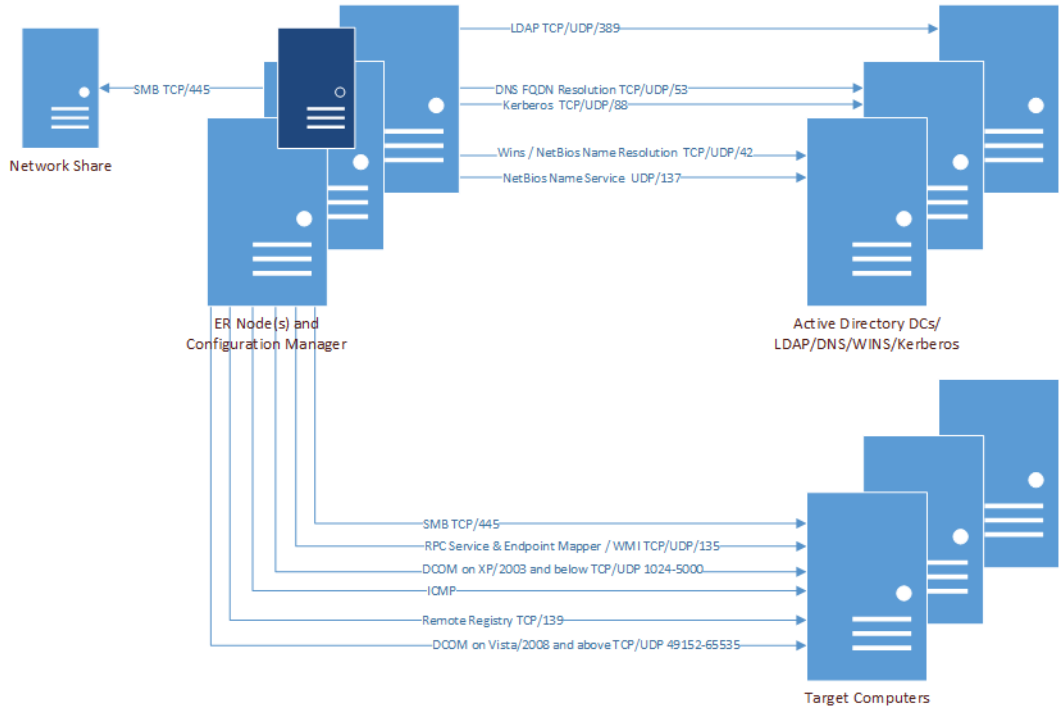


Figure 8. Ports used by NTFS collections

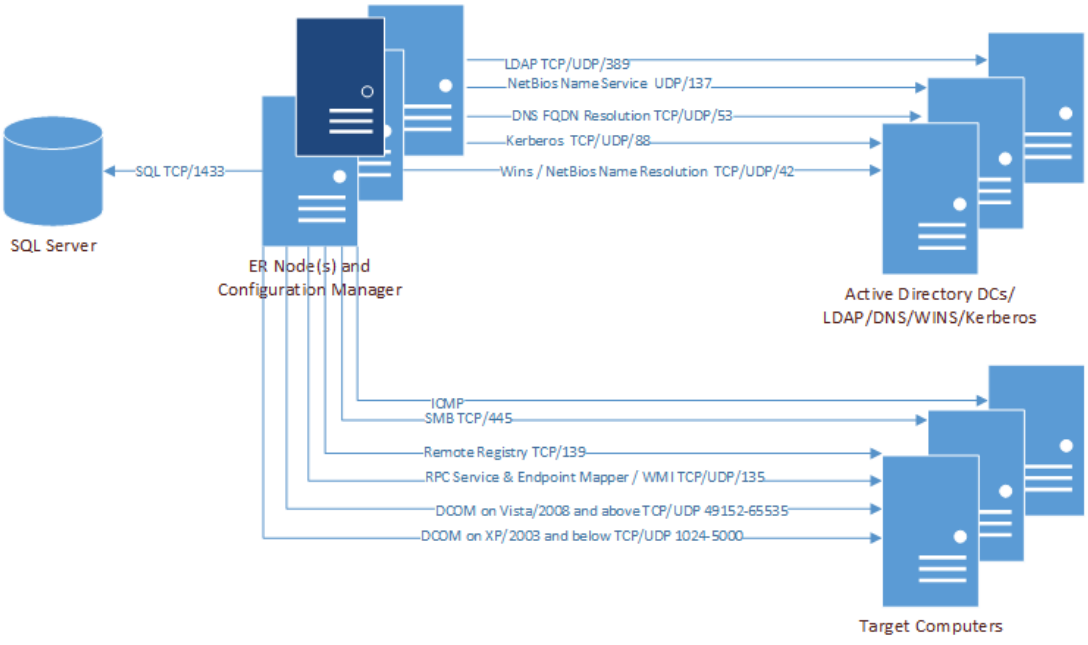


Figure 9. Ports used by Registry collections

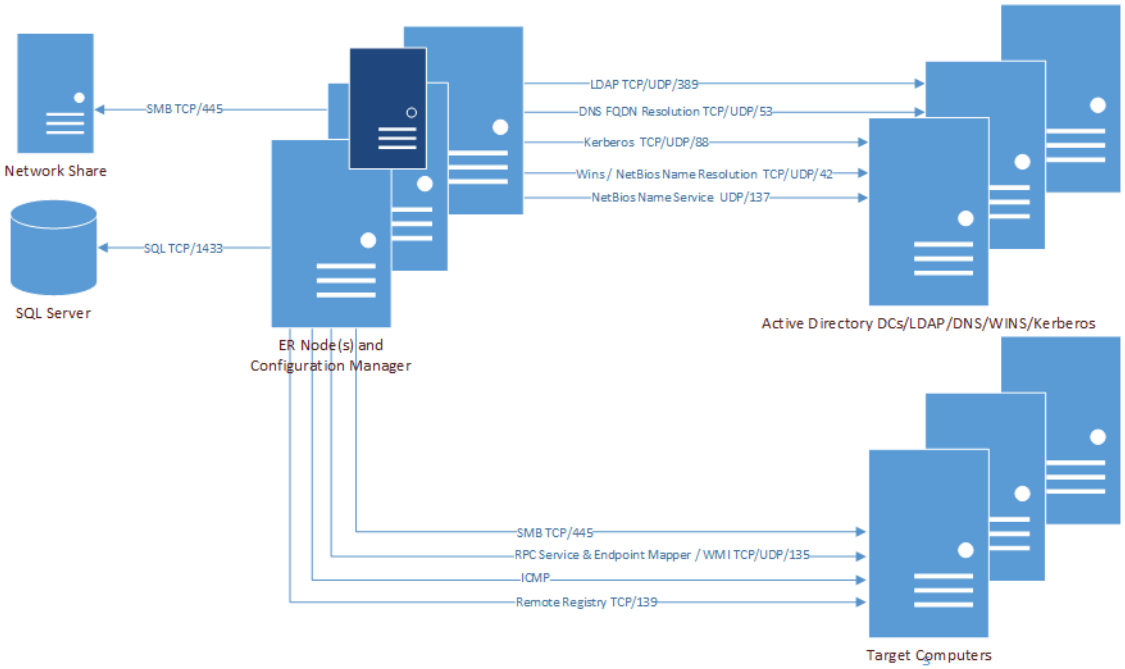
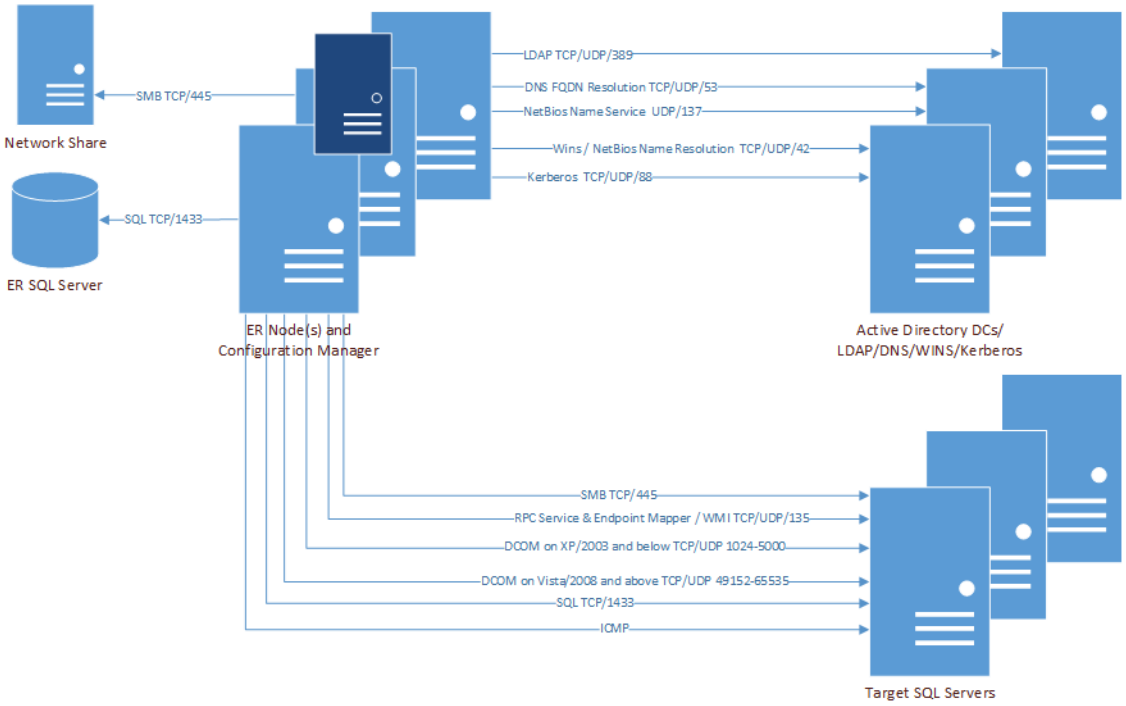


Figure 10. Ports used by SQL collections



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.

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**.

If you have selected to not install the Reporter Server, and the network is using Kerberos for authentication, then enter a UPN or SPN.

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.

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

- If the network is using Kerberos for authentication, then enter a UPN or SPN for the Enterprise Reporter server to use.

- Verify the default port of 7738 to be used for the Enterprise Reporter server.

  If the default port 7738 is in use, specify an alternate port for the server.

10 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 in the Quest Enterprise Reporter Installation and Deployment Guide.

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 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**.
5. Select the appropriate level of encryption for the data sent between the client and SQL server.

NOTE: Enterprise Reporter supports TLS 1.3; however, TLS 1.2 remains a requirement since SQL Server 2022 satellite services require TLS 1.2 to be enabled. For more information on TLS support, see Microsoft documentation.

- **Strict (SQL Server 2022)**: Select this option for SQL Server 2022 and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled.
- **Mandatory**: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but **Trust server certificate** is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection.
- Optional

  Enabling **Trust server certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication.

  Under **Host name in the certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases. Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.

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

6. 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.
7. If required, enter the domain of the Enterprise Reporter server's service account.
8. Enter the names for the security groups, and click **Next**.

   Using the default group names is recommended.

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

- OR -

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

10 Optionally, accept the default to open Configuration Manager.

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

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

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

12 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 119.

- OR -

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

Configure Enterprise Reporter Licenses

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 4. 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 • Microsoft | Azure Resources
Enterprise Reporter for Active Directory	• Active Directory • Microsoft Entra ID	• Active Directory • Microsoft | Entra ID • Change History • Hybrid
Enterprise Reporter for SQL Server	• MS SQL	• Microsoft SQL Server • Change History

Table 4. Enterprise Reporter Licenses

Enterprise Reporter License	Discovery Types Available with License	Report Libraries Available with License
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
Enterprise Reporter for Microsoft 365	• Microsoft Entra ID • Azure Resource • Exchange Online • OneDrive • Microsoft Teams • SharePoint Online	• Microsoft | Entra ID • Microsoft 365 | Exchange Online • Microsoft 365 | OneDrive • Microsoft 365 | Microsoft Teams • Microsoft 365 | SharePoint Online
Enterprise Reporter Suite	• Active Directory • Microsoft Entra ID • Azure Resource • Computer • File Storage Analysis • Exchange • Exchange Online • Microsoft Teams • SharePoint Online • MS SQL • NTFS • OneDrive • Registry	• Active Directory • Microsoft | Entra ID • 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**.

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 cannot run a discovery without an enabled node.

To create the 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.

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

   If you do not wish to add any nodes at this time, skip to step 8.
5. Click **Add** to browse to the computer where the node is to be created.
6. Select an account from the Credential Manager and click **OK**.

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

   NOTE: The node credentials must have local administrator access to the host computer and be a member of the Reporter_Discovery_Nodes group.

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

   If the network is using Kerberos for authentication, then enter a UPN or SPN for the Enterprise Reporter server to use.

   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. Optionally, set tasks to be System - managed or specify a Maximum number of tasks..

   For more information, see Nodes in the Quest Enterprise Reporter Configuration Manager User Guide.
8. Click **OK**.

   You can add more than one node at a time to the same cluster. Repeat steps 5 through 7 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.
9. 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.

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.

Step-By-Step Walkthroughs

Enterprise Reporter is a 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.
- Changing 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.
- Microsoft 365 and Microsoft Entra ID Reporting - Assess your Microsoft 365 and Microsoft Entra ID usage and configuration.

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 15.

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 do the following steps:

Configure a cluster for data discovery

Create a discovery to define the data collection

Run the discover to collect the data

Run the reports you want and export them

Configure a cluster for 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 **Quest** | **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 **Log In**.

The Create Cluster wizard walks you through the process of setting up a cluster.

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 discover 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 want and export them

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** | **Quest** | **Report Manager**.

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

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 To** 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 must take the following steps:

1 Modifying an Existing Report

2 Scheduling the Report

3 Scheduling Report Delivery to Recipients

Modifying 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 **+Add**.

8 Set **This parameter is:** to **Hidden**.

9 Set **Select the field to associate with this parameter:** 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.

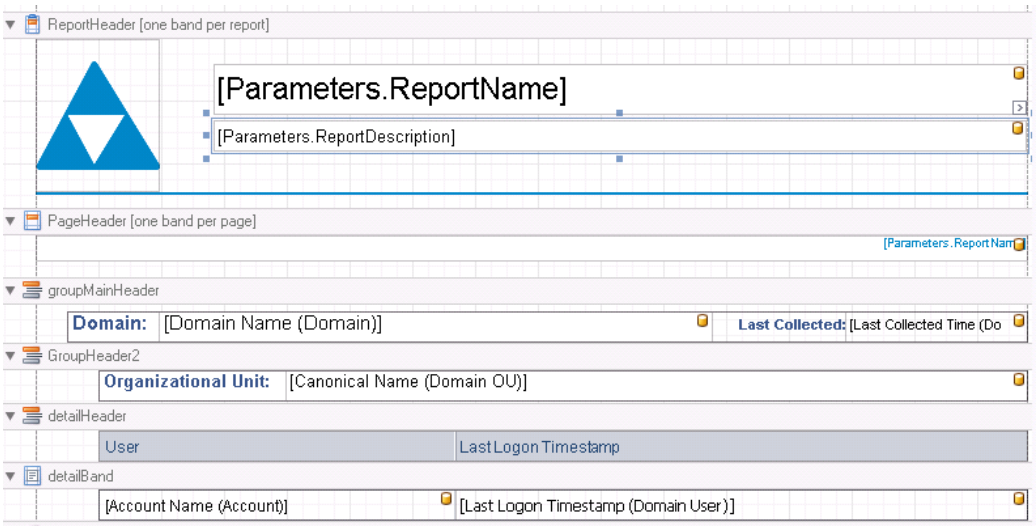
2 Click **Edit**.

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

4 Repeat for **IsDisabled** and **IsLocked**.

5 Repeat for all fields in the detailBand row of the report layout except **Account Name** and **Last Logon (Domain User)**.

6 Click the **Preview** tab below the report to ensure the new layout it is accurate:



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

8 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.

Scheduling 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 Discoveries to Define the Data Collection on page 30, 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.

Scheduling Report Delivery to Recipients

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 automatically delivers 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 email 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 Modifying 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**.
3. There are two ways to configure email delivery: SMTP or Exchange Online.
   - If your administrator has configured a default email SMTP server, the fields are filled in.
   - If your administrator has configured email to use Exchange Online, the fields are filled in.

     For information about configuring a default server, see “Configuring a Default Email Server” in the *Report Manager User Guide.*

     NOTE: To use Exchange Online, you must register an application for Enterprise Reporter with Microsoft Entra ID, using certificate-based authentication. For more information, see “Registering an Enterprise Reporter Application for Exchange Online Email Delivery” in the *Configuration Manager User Guide*.
4. Launch the Credential Manager, and select the account used to access the mail server.

   If your SMTP email 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.
5. In the From field, type the email address of the sender.
6. In the To field, type the email addresses of the recipients, separated by a comma or semicolon.
7. Click **OK**.

   The schedule card is created.

To schedule a report

1. On the Compliance Reports schedule card, click **+Add a report to this schedule**.
2. Select **Domain Users without Recent Logons**, and click **OK**.
3. Click the **Modify Report Parameters** icon for the Domain Users without Recent Logons report.
4. In the Report Parameters pane, complete the **Parameter Set Name:** by typing **[Domain Name] Users not logged in for 90 days** to identify the parameter values you will use.
5. 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**.
6. In the **Users not logged on in the last (days)** parameter, change the number of days to **90**.
7. Click **Save**.

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

Changing 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
- Scheduling 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. If the network is using Kerberos for authentication, then enter a UPN or SPN for the Enterprise Reporter server to use.
6. 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 Configuration page, click **Manage 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**.

Scheduling 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 details about the steps to take to schedule a report, see Scheduling Report Delivery to Recipients on page 25.

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 was set up as described in Scheduling Report Delivery to Recipients on page 25.

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 **+Add a report to this schedule**.

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

3 Click the **Modify Report Parameters** icon for the Computer Change History report.

4 In the Report Parameters pane, complete the **Parameter Set Name:** by typing **Changed services on [computer names]** to identify the parameter values you will use.

5 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**.

6 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.

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

8 In the **Include changes in the following date range:** parameter, set dates to limit the number of changes included.

9 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 **Quest** | **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 **Log In**.

The Create Cluster wizard walks you through the process of setting up a cluster.

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 **Next** then **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 (since 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 (since 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: **Collect all available public shares**
- Folder 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 **Next** then **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.

Microsoft 365 and Microsoft Entra ID Reporting

If you are required to administer your Microsoft 365 and Microsoft Entra environments, including subscriptions and licenses, Enterprise Reporter can be of assistance by automatically gathering information and reporting on it.

Scenario

Each week you need a report that shows an overview of your Microsoft 365 tenant. You are going to use three reports to monitor this: one report for an overview of Microsoft 365, one report for tenant settings, and one report for Microsoft Entra subscription information. You will automate the delivery of the weekly reports to ensure they are always received.

You will need to take the following steps:

1. Setup Enterprise Reporter Microsoft Entra Applications for Microsoft 365 Discoveries

2 Create a Discovery to Define the Data Collection

3 Run the Discovery to Collect the Data

4 Run the Reports

Setup Enterprise Reporter Microsoft Entra Applications for Microsoft 365 Discoveries

To collect from your tenant you must configure Enterprise Reporter Tenant applications using the Tenant Application Manager.

To setup Enterprise Reporter Microsoft Entra Applications for Microsoft 365 Discoveries

1 On the **Configuration** page of the Configuration Manager, select **Manage tenant applications**.

2 Click **Add**, enter the name of your Microsoft 365 tenant and click **OK**.

3 In the Tenant Application Manager, your tenant will display with four applications created – Quest Enterprise Reporter Microsoft Entra Discovery v2, Quest Enterprise Reporter Azure Resource Discovery, Quest Enterprise Reporter Microsoft Teams Discovery, SharePoint Online and Quest Enterprise Reporter OneDrive Discovery.

4 To configure each application, click the **Configure** link in the Application Status column.

5 Enter credentials for a global administrator account on the tenant and consent to the application permissions.

6 Ensure you configure each application. Once configured, the Configure link will change to **Reconfigure**.

7 Click **Close**.

Create a Discovery to Define the Data Collection

In a previous scenario, you have already configured a cluster and now have set up your Enterprise Reporter Tenant applications. You now need to set up discoveries for Microsoft Entra ID, Exchange Online, Microsoft Teams, SharePoint Online, and OneDrive. Discoveries define the targets from which data will be collected. Enterprise Reporter uses a “collect all” model. After you run a discovery you can run the reports that include the data that has been collected.

To create an Microsoft Entra ID discovery

1 On the Manage Discoveries page of the Configuration Manager, select **New Discovery | Microsoft Entra ID**.

2 On the Name page, enter **Microsoft Entra – [Tenant 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.

4 Select an account for the target tenant from the Credential Manager and click **Next**.

5 On the Scopes page, the target tenant will be displayed based on the account selected on the previous page. Since we previously configured your Enterprise Reporter Tenant application, no further configuration is required.

6 Select only the options necessary for the information you want to collect. Keep the following options: **Users**, **Groups**, **Contacts**, **Roles**, **Devices**, **Applications**, and **Service Principals**.

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 Exchange Online discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery | Exchange Online**.
2. On the Name page, enter **Exchange Online – [Tenant 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.
4. Select an account for the target tenant from the Credential Manager and click **Next**.
5. On the Scopes page, the target tenant will be displayed based on the account selected on the previous page. Since we previously configured your Enterprise Reporter Tenant applications, no further configuration is required.
6. Select only the options necessary for the information you want to collect. Keep the following options: **Mailboxes**, **Public Folders**, **Mail-Enabled Users**, **Contacts**, and **Distribution Groups**. Clear the option to **Collect group members**.
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 Microsoft Teams discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery | MS Teams**.
2. On the Name page, enter **Microsoft Teams – [Tenant 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.
4. Select an account for the target tenant from the Credential Manager and click **Next**.
5. On the Scopes page, the target tenant will be displayed based on the account selected on the previous page. Since we previously configured your Enterprise Reporter Tenant applications, no further configuration is required.
6. Select only the options necessary for the information you want to collect. Keep the following options: **Channels**, **Applications**, and **Files and Folders**.
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 SharePoint Online discovery

1. On the Manage Discoveries page of the Configuration Manager, select **New Discovery | SharePoint Online**.
2. On the Name page, enter **SharePoint Online – [Tenant 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.
4. Select an account for the target tenant from the Credential Manager and click **Next**.
5. On the Scopes page, the target tenant will be displayed based on the account selected on the previous page. Since we previously configured your Enterprise Reporter Tenant applications, no further configuration is required.
6. Select only the options necessary for the information you want to collect. Keep the following option: **Site Groups**.
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 OneDrive discovery

1. On the Manage Discoveries page of the Configuration Manager, select New Discovery | OneDrive.

2 On the Name page, enter **OneDrive – [Tenant 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.

4 Select an account for the target tenant from the Credential Manager and click **Next**.

5 On the Scopes page, the target tenant will be displayed based on the account selected on the previous page. Since we previously configured your Enterprise Reporter Tenant applications, no further configuration is required.

6 We want to collect all drives to understand usage by user. Select the option to **Collect all drives**.

7 To shorten collection time, select only the options you want to collect. Select the following options: **Folders and Files**.

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 that 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 each discovery and click **Run**.

2 To view the progress of each discovery in the cluster queue, click **View Queue**.

3 To see task progress, click the **Processing** link in the Status column.

Run the Reports

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 Microsoft Entra and Microsoft 365 reports require that the tenant name is entered.

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

The first report is found in the **Microsoft 365** report library:

- Microsoft 365 Overview – shows an overview of Microsoft 365 including Exchange Online, OneDrive, Microsoft Teams, and SharePoint Online.

The other two reports are found in the **Microsoft** report library:

- Microsoft Entra ID Summary– shows a summary of your Microsoft Entra ID
- Microsoft Entra Subscription Information – shows information on Microsoft Entra subscriptions

To run each report

1 Open the Report Manager by selecting **Start | Quest | 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 | Microsoft 365** and select your first report, Microsoft 365 Overview.

4 In the **Include the following tenants** parameter, type the tenant name and click **Add**.

- OR -

In the **Include the following tenants** parameter, click **Search**, locate and add the tenant, 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.

Repeat this process for the other reports.

A

About us

Quest Software creates technology and solutions that build the foundation for enterprise AI. Focused on data management and governance, cybersecurity and platform modernization, Quest helps organizations address their most pressing challenges and make the promise of AI a reality. Around the globe, more than 45,000 companies including over 90% of the Fortune 500 count on Quest Software. For more information, visit www.quest.com or follow Quest Software on X (formerly Twitter) and LinkedIn.

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.