Quest

Quest® Enterprise Reporter 3.5.2

Report Manager User 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 Report Manager User Guide
Updated - April 2025
Software Version - 3.5.2

Contents

Introducing the Report Manager . . . 7
Starting the Report Manager . . . 7
Finding Answers and Getting Help . . . 7
Checking Online Support . . . 8
Help Finding and Creating Custom Reports . . . 8
An Overview of the Report Manager Security . . . 8
Explaining My Reports, Published Reports, and the Report Library . . . 9
What are My Reports? . . . 9
What are Published Reports? . . . 10
What is the Report Library? . . . 10
Reports Included in Enterprise Reporter . . . 10
Active Directory Reports . . . 11
Active Directory Modernization Reports . . . 20
Change History Reports . . . 23
Computer Reports . . . 23
Enterprise Reporter System Reports . . . 27
Exchange Reports . . . 28
File Storage Analysis Reports . . . 30
Hybrid Reports . . . 39
Microsoft SQL Server Reports . . . 44
Microsoft 365 Reports . . . 45
NTFS Reports . . . 50
Registry Reports . . . 55
Security Explorer Remediation Reports . . . 56
Report Types Included in Enterprise Reporter . . . 59
Active Directory Report Types . . . 59
Microsoft Entra Report Types . . . 60
Azure Resource Report Types . . . 62
Common Objects Report Types . . . 64
Computer Report Types . . . 64
Exchange Report Types . . . 66
Exchange Online Report Types . . . 67
File Storage Analysis Report Types . . . 68
Microsoft Teams Report Types . . . 69
NTFS Report Types . . . 70
OneDrive Report Types . . . 70
Registry Report Types . . . 71
SharePoint Online Report Types . . . 71
SQL Server Report Types . . . 72
Configuring Global Settings (System Configuration) . . . 73
Configure Logging . . . 73
Credential Manager . . . 74
Database Settings . . . 74
Email settings . . . 74

Logon Configuration 74
Report Icon 74
Report Parameter Favourites 75
Server Error Notification 75
SSRS Server settings 75

Running and Scheduling Reports 76
Running Reports 76
Running Category Reports 76
Running Regular Reports 77
Running Reports or Exporting Reports to CSV and Other Formats from Different Containers 78
Entering Parameter Values 79
Searching for Parameter Values 80
Importing Parameter Values 81
Using Saved Parameters 82
Searching for a Report 83
Viewing Report Properties 83
Previewing a Report 84
Exporting a Report to Other Formats 84
Configuring a Default Email Server 86
Scheduling Reports 87
Creating a Schedule 88
Types of Schedules 92
Working with Schedules 94
Troubleshooting Scheduling Issues 98
Using the Credential Manager 98
Changing passwords using the Credential Manager 102
Changing account names using the Credential Manager 103
Organizing Reports 104
Working with Report Categories 105
Moving Reports 105
Copying Reports 105
Deleting Reports 106

Creating and Editing Reports 107
Editing Reports 107
Using My Reports 107
Changing the report icon 108
Modifying the Fields to be Included 109
Working with Report Parameters 112
Changing the Layout 120
Report Modification Example 121
Creating New Reports 122
Creating Report Layouts 124
Setting CSV File Export Options 125
Exporting and Importing Report Definitions 126

Report Designer Tips and Tricks 126
Report Bands 127
Binding a Data Field to a Control 128
Adding a Parameter Field to a Report Layout 128
Adding a New Grouping to a Report Layout 129
Adding a New Column to a Table 129
Formatting Rules:
Hiding or Showing a Field Based on Data Values 130
Creating a Calculated Field 130
Creating a Script to Run with a Report 131
Publishing Reports 132
Integrating with SSRS 132
Configuring SSRS 132
Publishing Reports to SSRS 133

Troubleshooting Issues with Enterprise Reporter 135
Troubleshooting connectivity issues 135
Restoring a connection to the Enterprise Reporter Server 136
Restoring a connection to the Enterprise Reporter database 136
Troubleshooting Connection Timeouts 136
Troubleshooting credential change failures 137
Auditing Report Manager Activity 137
Exporting Logs from the Report Manager 138
Exporting the Report Manager Logs 138
Viewing the Report Manager Logs 138
Resolving Issues in the Report Manager 138
What To Do if the Data in Your Report
is Not What You Expect 139
Other Issues 140
Viewing information about your Enterprise Reporter configuration 140
Troubleshooting Issues with SSRS 141

Appendix: PowerShell cmdlets 142
What is Microsoft Windows PowerShell? 142
What are cmdlets? 142
Registering Enterprise Reporter cmdlets 143
Adding the snap-ins automatically to new sessions 143
Enterprise Reporter cmdlets 144
Enabling Enterprise Reporter cmdlets 145
Loading the Enterprise Reporter cmdlets 146
Using cmdlets to manage clusters and nodes 146
Creating a cluster 147
Creating a node 147
Disabling a node 148
Enabling a node 148
Finding a node by name 149
Piping cmdlets 149
Finding a cluster by name 149

Disabling a cluster 150
Enabling a cluster 150
Using cmdlets to manage discoveries 151
Getting job information 151
Creating a job 153
Running a job 155
Scheduling a job 156
Deleting a job 157
Using cmdlets to run reports 157
Connecting to the server 158
Getting report information 158
Exporting a report definition 159
Importing a report definition to a category 159
Generating a report with data 160

Appendix: Log Viewer 161
Starting the Enterprise Reporter Log Viewer 161
Finding and opening log files 161
Viewing and searching log file entries 162
Filtering log file entries 163

About us 164
Technical support resources 164

1

Introducing the Report Manager

- Starting the Report Manager
- Finding Answers and Getting Help
- An Overview of the Report Manager Security
- Explaining My Reports, Published Reports, and the Report Library
- Reports Included in Enterprise Reporter
- Report Types Included in Enterprise Reporter
- Configuring Global Settings (System Configuration)

NOTE: Azure Active Directory is now Microsoft Entra ID.

Starting the Report Manager

The Report Manager is used to generate reports. You can run existing reports, or create your own custom reports. The reports use data collected by the Configuration Manager.

NOTE: To start the Report Manager, you must be a reporting administrator or a reporting user. Contact your Enterprise Reporter administrator for assistance.

To start the Report Manager

1. Click the **Start** menu and select **Quest** | **Report Manager**.
2. Type the name of the Enterprise Reporter 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 drop-down list for future use.
3. To connect to the database using SQL credentials, instead of the logged in user, click **Advanced**, then choose SQL Server Authentication and enter your user name and password.

   If you want to connect to the database using these credentials as the default, select Remember Credentials.
4. If necessary, type in the port number.
5. Click **Log In**.

Finding Answers and Getting Help

When using Enterprise Reporter, you can press F1 from any screen for help. The documentation included with Enterprise Reporter will open and display the section of documentation most relevant to the screen you are viewing.

The Help menu provided in Enterprise Reporter also addresses frequently asked questions related to the screen you are viewing. Clicking on any of the topics provided will display the related section of documentation.

See also:

- Checking Online Support
- Help Finding and Creating Custom Reports

Checking Online Support

Enterprise Reporter also provides a tool for searching knowledge articles and community discussions.

To search Online Support

1. Click the link for **Online Support** in the header bar of the console.
2. Select whether to search **Knowledge Articles**, **Community Discussions**, or both.
3. Enter a keyword or phrase in the text box.
4. Press **Enter** or click the search icon.
5. Click the link of any result to open the result in the Online Support portal.

   NOTE: Signing in to the Online Support portal is required to view premium knowledge articles.

Help Finding and Creating Custom Reports

The Quest Community contains the Enterprise Reporter Custom Reports Forum dedicated to help with custom reporting. The forum hosts discussions about editing reports in the Enterprise Reporter report library to create custom reports. Existing custom reports are available to download and edit. If none of the existing reports meet your needs, you will also find guidelines to request a custom report.

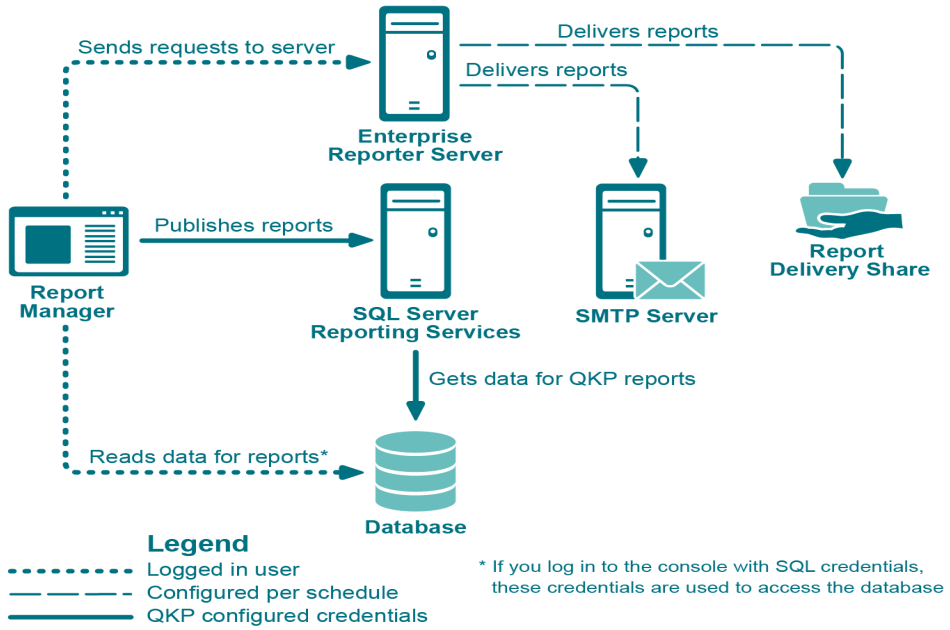
To search for custom reports

1. Click the link for the **Custom Report Community** in the toolbar of the console.
2. Click the link to review the **Existing Custom Reports** and download any that are appropriate.
3. If the appropriate report is not found, follow the link to the **Guidelines** to request a custom report.

An Overview of the Report Manager Security

The Report Manager needs to be able to access both the Enterprise Reporter server and the Enterprise Reporter database, as shown in Figure 1.

Figure 1. Credentials used to communicate in Enterprise Reporter



The logged in credentials need the following permissions in order to successfully run and create reports:

To log in to the Report Manager, the logged in user must be in the Reporter_Reporting_Admins or Reporter_Reporting_Operators security group. For more information, see the Quest Enterprise Reporter Installation and Deployment Guide.

To access the server, the logged in user must be a domain account.

- The account being used to access the database must have read access to the database to read reports, and write access to the database to publish reports. This account is chosen when you log in to the Report Manager. If you are using Windows® authentication, the account should already have these permissions because they must be in a security group in order to log in to the console. SQL accounts must be permissioned manually.

  SQL Authentication is supported for the Enterprise Reporter database.

Explaining My Reports, Published Reports, and the Report Library

Enterprise Reporter has three different report containers, each with its own intended use. They are shown in the treeview of the console. Each container can be expanded to show the categories and reports it contains.

See also:

- What are My Reports?
- What are Published Reports?
- What is the Report Library?

What are My Reports?

As you use Enterprise Reporter, you will find that there are reports that you use a lot, or reports that you want to customize. You can store these in the My Reports container. You decide what reports appear in My Reports by

copying them from other containers (see Copying Reports on page 105) or creating them from scratch (see Creating New Reports on page 122). My Reports is unique to each user, so different users will have different contents in their My Reports container. You can see your My Reports container on any computer that you are logged in to. You can create your own categories to keep these reports organized for easy access (see Working with Report Categories on page 105). Reports in this container may be scheduled (see Scheduling Reports on page 87).

What are Published Reports?

Reporting administrators can publish reports that will be useful to their users. When a report is added to the Published Reports container, it is visible to all reporting users the next time they open their console. These reports are generally customized to suit your environment. You can base a published report on a report from the library, or you can create a new report and publish it. If you are a reporting administrator, you can edit reports directly in Published Reports; however, it is recommended that you copy reports to My Reports for editing.

If you are a reporting user, you can fill in the parameters, run the reports from the published reports container, and copy them to My Reports (see Copying Reports on page 105) so they can be modified (see Editing Reports on page 107).

For example, you may want to run different versions of the same report. By creating several copies in My Reports and saving the parameter values, you can save yourself time. Reports in this container may also be scheduled (see Scheduling Reports on page 87).

What is the Report Library?

The Report Library is only visible to reporting administrators. It contains all available pre-defined reports included with Enterprise Reporter, organized by type of discovery. Reports in the library cannot be modified or moved, so you need to first copy them to My Reports or Published Reports if you would like to work with them. If reports in the library contain values in their parameters, those values will be included when the report is copied.

Reports Included in Enterprise Reporter

The reports included in Enterprise Reporter are located in the Report Library, and can only be seen by reporting administrators. The reports include the results of all discoveries that have been run on the server to which the console is connected. If you would like to customize a report, you need to create a copy in My Reports or Published Reports and modify it. If reports in the library contain values in their parameters, those values will be included when the report is copied.

See also:

- Active Directory Reports
- Active Directory Modernization Reports
- Change History Reports
- Computer Reports
- Enterprise Reporter System Reports
- Exchange Reports
- File Storage Analysis Reports
- Hybrid Reports
- Microsoft Entra Reports

- Microsoft SQL Server Reports
- Microsoft 365 Reports
- NTFS Reports
- Registry Reports
- Security Explorer Remediation Reports

Active Directory Reports

The following table describes the Active Directory reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. For each report, you must specify the domains on which you want to report.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 1. Active Directory Reports

Report Name	Description
Account Expiration Date	Shows the account expiration date for the selected accounts. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Account Operators	Shows the members of the account operators group for the selected domains. Contains a parameter to select the domains to be included in the report.
Accounts that can change any property of any user in the selected domains	Shows accounts that can change any property of any user in the selected domains. Includes any accounts that are permissioned through group membership. Contains a parameter to select the domains to be included in the report. You may also set the maximum recursion depth for this report. The folder level value will start from zero. Examining the path of C:\FolderA\FolderB, C:\ is 0 levels deep. FolderA is 1 level deep. FolderB is 2 levels deep.
Accounts that can change group membership of any group in the selected domains	Show accounts that can change group membership of any group in the selected domains. Includes accounts that are permissioned through group membership. Contains a parameter to select the domains to be included in the report. You may also set the maximum recursion depth for this report.
Accounts Where SID History Attribute Contains SID From Same Domain	Shows accounts whose SID History attribute contains an SID of another object in the same domain. Includes a parameter to select the domains and Organizational Units to be included in the report.
Active Directory Permissions	Shows all Active Directory permissions for the selected domains and Active Directory objects. Contains parameters to select the domains, organizational units, object types, objects, and accounts to be included in the report. Also includes the option to filter inherited or explicit permissions.

Table 1. Active Directory Reports

Report Name	Description
Active Directory Permissions for Account	Shows the Active Directory permissions for an account, including permissions derived through group membership. Contains parameters to select the account, domains, organizational units, object types, and objects to be included in the report. Also includes the option to filter inherited or explicit permissions.
Active Directory Permissions for Account with Membership	Shows the Active Directory permissions for an account, including permissions derived through group membership. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the account, domains, organizational units, object types, and objects to be included in the report. Also includes the option to filter inherited or explicit permissions.
All Accounts	Shows accounts of all types including trust accounts and InetOrgPerson accounts. Contains parameters to select the domains and account type to be included in this report.
All Names for Active Directory Users	Shows all the Active Directory names for the selected user accounts. Contains parameters to select the domains, organizational units and accounts to be included in the report.
Circular Nested Domain Groups	Shows information about groups which recursively contain themselves for the selected domains. Contains a parameter to select the domains to be included in the report.
Disabled Accounts	Shows all the disabled accounts for the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Accounts	Shows all the domain accounts for the selected domains. Contains parameters to select the domains, organizational units, accounts, and account scopes to be included in the report.
Domain Computer Information	Shows the domain computer information in selected domains. Contains parameters to select the domains, organizational units, and computers to be included in the report.
Domain Controller Information	Shows domain controller information for the selected domains. Contains parameters to select the domains, domain controllers, and organizational units to be included in the report.
Domain Groups	Shows all the domain groups for the selected domains. Contains parameters to select the domains, organizational units, domain groups, and group scopes to be included in the report. Also contains the option to include only security enabled groups.
Domain Groups and Members	Shows the group membership for the selected domains and groups. Contains parameters to select the domains, organizational units, and domain groups to be included in the report. Contains a parameter to include nested group memberships and options on how they are displayed in the report. For more information, see Searching for Parameter Values on page 80. Technical Documentation. Foreign groups only appear if they were included in the applicable discovery. For more information, see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.
Domain Groups with Probable Owners	Shows the domain groups for the selected domains and suggests the account that manages the highest percentage of members of each group as the probable group owner. Contains a parameter to select the domains to be included in the report.

Table 1. Active Directory Reports

Report Name	Description
Domain Groups without Members	Shows all the domain groups which do not have any members. Contains parameters to select the domains, organizational units, and domain groups to be included in the report.
Domain Sites	Shows all the sites for the selected domains. Contains parameters to select the domains and sites to be included in the report.
Domain Summary	Shows a domain summary for the selected domains. Summary information is only available if Active Direct discovery collections that include object counts for the selected domains have been completed. Contains parameters to select the domains and organizational units to be included in the report.
Domain Trusts	Shows all the trust relationships for the selected domains. Contains parameters to select the domains and trusts to be included in the report.
Domain Users	Shows all the domain users for the selected domains. Contains parameters to select the domains, organizational units, and accounts to be included in the report. Also contains the options to include only disabled or only locked domain user accounts.
Domain Users at Risk	Shows the users who match one or more of the selected risk factors and therefore may pose a security risk in the selected domains. Includes a summary of risk factors used as criteria for this report. Contains parameters to select the domains to be included in the report. Also contains the option to include users that: • have a password that never expires • have not logged on in the past _ days • have not changed their password in the past _ days • have a token group count of _ or higher • are a member of the Domain Admins group • are a member of the Enterprise Admins group • have password complexity disabled
Domain Users with Recent Logons	Shows users in the selected domains who have logged on in the selected time frame. Contains parameters to select the domains, organizational units, and users to be included in the report. Also contains the option to include users that have logged on in the past _ days.
Domain Users without Recent Logons	Shows users in the selected domains who have not logged on in the selected time frame. Contains parameters to select the domains, organizational units, and users to be included in the report. Also contains the option to include users that have not logged on in the past _ days.
Group Managed Service Accounts and Members	Shows all the group managed service accounts and their members for the selected domains. If you choose to include nested groups, membership of the group members is displayed. Contains parameters to select the domains, organizational units, and group managed service accounts to be included in the report.
Group Member Comparison	Shows the direct and indirect users that are members of the selected groups. Contains parameters to select up to 5 groups.
Group Membership by Domain Account	Shows all groups to which the selected domain accounts belong. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Group Membership Comparison	Compares the direct and indirect group memberships of the selected accounts. Contains parameters to select up to 5 accounts.

Table 1. Active Directory Reports

Report Name	Description
Locked Out Accounts	Shows all the locked out accounts for the selected domains.Contains a parameter to select the domains to be included in the report.
Managed Service Accounts	Shows all the managed service accounts for the selected domains. Contains parameters to select the domains, organizational units, and managed service accounts to be included in this report.
Managed Service Accounts and Members	Shows all the managed service accounts and their members for the selected domains. Contains parameters to select the domains, organizational units, and managed service accounts to be included in this report.
Member Servers	Shows the member server information for the selected domains.Contains parameters to select the domains and organizational units to be included in the report.
Published Printer Information	Shows published printer information for the selected domains.Contains parameters to select the domains and printers to be included in the report.
Published Share Information	Shows published share information for the selected domains. Contains parameters to select the domains and shares to be included in the report.
Recursive Group Membership by Domain Account	Shows recursive group membership for the selected domain accounts. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Remote Access Profile (RAS) Information	Shows RAS information for the selected user accounts. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Remote Control Settings Information	Shows terminal services remote control settings of the users for the selected domains. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Resultant Kerberos Configuration for Domains	Shows the resultant Kerberos GPO configuration for selected domains. Includes a parameter to select the domains to be included in the report.
Terminal Services Profile Information	Shows terminal services profile information of the users for the selected domains. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Users At Risk Of Token Bloat	Shows the users who are at risk of token bloat in the selected domains. You can select the number of security groups permitted for users in these domains. This report will only include groups from your selected domains. Contains a parameter to select the domains to be included in the report.
Users Not Logged On In The Past 30 Days	Shows users in the selected domains who have not logged on in the past 30 days. Contains a parameter to select the domains to be included in the report.
User That Have Never Logged On	Shows users in the selected domains who have never logged on. Contains a parameter to select the domains to be included in the report.
Users with An Exchange Mailbox	Shows Active Directory Users that have an Exchange mailbox as set by the Active Directory Connector. Contains parameters to select the domains, organizational units, and accounts to be included in the report.

Health Check | Active Directory

Table 1. Active Directory Reports

Report Name	Description
Accounts Where SID History Attribute Contains SID From Same Domain	Shows accounts whose SID History attribute contains an SID of another object in the same domain. Includes a parameter to select the domains and Organizational Units to be included in the report.
Active Directory Permissions - Dangerous permissions delegated	Shows all Active Directory permissions for the selected domains and Active Directory objects. These permissions can be used to attack Active Directory. For information about attack types, see https://attack.mitre.org/mitigations/M1015/
Active Directory Permissions - Domain Controller Owners	Shows all Active Directory permissions for the selected domains and Active Directory objects. The Domain Administrators group or the Enterprise Administrators group are set as owners for domain controllers. For details, see Privileged Account Management at https://attack.mitre.org/mitigations/M1026/
Active Directory Permissions for Account (Everyone)	Shows the Active Directory permissions for an account, including permissions derived through group membership. (Excluding Deny Permissions and Change Password permissions).
Active Directory Summary	Shows the summary of Active Directory Users and Groups for the selected domains. Contains a parameter to select the domains to be included in the report.
AdminSDHolder Permissions	Shows all Active Directory permissions for the selected domains and Active Directory objects. For more information see Protected Accounts and Groups in Active Directory at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory and Active Directory Configuration at https://attack.mitre.org/mitigations/M1015/
Domain Accounts (Users and Groups) with SID History Attribute not empty	Shows all the domain accounts for the selected domains which can leave accounts open to Access Token Manipulation: SID-History Injection attacks. Adversaries can use SID-History Injection to escalate privileges and bypass access controls. For details, see https://attack.mitre.org/techniques/T1134/005/
Domain Controllers by Site Name	Shows the domain controller per site for the selected domains. Contains parameters to select the domains and sites to be included in the report.
Domain Controllers with Global Catalog by Site Name	Shows the domain controller with global catalog per site for the selected domains. Contains parameters to select the domains and sites to be included in the report.
Domain Functional Level	Shows the domain functional level for the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Groups and Members (Pre-Windows 2000 Compatible Access)	Shows the group memberships for the selected domains and groups. If you include nested groups, the membership of the groups is displayed. For details, see https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-adts/7a76a403-ed8d-4c39-adb7-a3255cab82c5?redirectedfrom=MSDN and Exploitation of Remote Services https://attack.mitre.org/techniques/T1210/
Domain NetBIOS Name	Shows domain NetBIOS name for the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Sites without a Domain Controller	Shows domain sites that do not contain a domain controller for the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Sites without a Global Catalog	Shows domain sites that do not contain a global catalog for the selected domains. Contains a parameter to select the domains to be included in the report.

Table 1. Active Directory Reports

Report Name	Description
FSMO Role Holders by Forest	Shows flexible single master operation (FSMO) role holders for the selected forests. Contains parameters to select the forests and domains to be included in the report.
Number of Domain Controllers	Shows the number of domain controllers for the selected domains. Contains a parameter to select the domains to be included in the report.
Number of Domains per Forest	Shows the number of domains for the selected forests. Contains a parameter to select the forests to be included in the report.
OU Structure	Shows the OU structure for the selected domains. Contains a parameter to select the domains to be included in the report.
Read-Only Domain Controllers	Shows read-only domain controllers for the selected domains. Contains a parameter to select the domains to be included in the report.
Size of Active Directory Database	Shows the size of the Active Directory database for the selected computers. Contains parameters to select the domain and organizational units to be included in the report.
Health Check | Computer	
Computer Services on Domain Controllers (Print Spooler)	Shows information about the services for the selected computers. (Enterprise Reporter Windows Server License must be available). More details at https://adsecurity.org/?p=4056
Disabled Computer Accounts	Shows disabled computer accounts for the selected domains. Contains parameters to select the domains and organizational units to be included in the report.
Domain Computers by Operating System	Shows domain computers per operating system for the selected domains. Contains parameters to select the domains, organizational units, and operating systems to be included in the report.
Domain Computers Having Constrained Delegation	Shows domain computers for selected domains that have constrained delegation.
Domain Computers Having SID History	Shows domain computers for selected domains that have some value specified in SID History attribute.
Domain Computers Having Unconstrained Delegation	Shows domain computers for selected domains having unconstrained delegation.
Domain Computers whose sAMAccountName Does Not End In a Dollar Sign	Shows domain computers for selected domains whose sAMAccountName does not end in a Dollar Sign.
Health Check | Group	
Domain Groups with Duplicate Display Names	Shows domain groups with duplicate display names in the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Groups with Only One Member	Shows domain groups with only one member for the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Groups without a Display Name	Shows domain groups without a display name for the selected domains. Contains a parameter to select the domains to be included in the report.
Privileged Domain Groups and Members	Shows the group memberships for the selected domains and groups. These privileged groups should have as few members as possible. DNSAdmins should have no members. If you include nested groups, the membership of the groups is displayed. For details, see Privileged Account Management https://attack.mitre.org/mitigations/M1026/

Table 1. Active Directory Reports

Report Name	Description
SID History Auditing Group available in Domain (Migration in Progress)	Shows if a SID History auditing group has been created in the domain.
Health Check | User	
Active Directory Permissions - Delegations for Accounts that cannot be resolved	Shows all active directory permissions for the selected domains and active directory objects. These permissions can be used for attacks. For details, see Active Directory Configuration https://attack.mitre.org/mitigations/M1015/
Built-in AD Administrator Account Usage	Shows native Administrator account in selected domains who have logged in selected timeframe.
Disabled Accounts	Shows disabled accounts for the selected domains. Contains parameters to select the domains and organizational units to be included in the report.
Domain User Accounts that are Sensitive and Cannot be Delegated	Shows all domain user accounts for selected domains that cannot be delegated.
Domain Users that will Expire in Next (N) Days	Shows domain users that will expire in next N days for the selected domains. Contains parameters to select the domains and the number of days to be included in the report.
Domain Users who do not require a password	Shows all domain users for selected domains who do not require a password.
Domain Users who do not require Kerberos Pre-Authentication	Shows all domain users for selected domains where the account is configured with the "Do not require Kerberos pre-authentication" option. Kerberos pre-authentication is a security feature which offers protection against password-guessing attacks. When you do not enforce pre-authentication, a malicious attacker can directly send a dummy request for authentication.
Domain Users with Duplicate Display Names	Shows domain users with duplicate display names in the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Users with Duplicate Email Addresses	Shows domain users with duplicate email addresses in the selected domains. Contains a parameter to select the domains to be included in the report.
Domain Users with weak DES encryption enabled	Shows all domain users for selected domains that have weak DES encryption enabled. DES is considered weak cryptography and is no longer enabled by default in Kerberos authentication.
Domain Users without a Display Name	Shows domain users without a display name for the selected domains. Contains parameters to select the domains and organizational units to be included in the report. Also contains the options to include only disabled or only locked domain user accounts.
Domain Users without a First Name	Shows domain users without a first name for the selected domains. Contains parameters to select the domains and organizational units to be included in the report. Also contains the options to include only disabled or only locked domain user accounts.
Domain Users without a Last Name	Shows domain users without a last name for the selected domains. Contains parameters to select the domains and organizational units to be included in the report. Also contains the options to include only disabled or only locked domain user accounts.
Exchange Mailbox Users with Duplicate Display Names	Shows exchange mailbox users with duplicate display names in at least two selected domains. Contains a parameter to select the domains to be included in the report.

Table 1. Active Directory Reports

Report Name	Description
Exchange Mailbox Users without a Display Name	Shows Active Directory users without a display name that have an Exchange mailbox. Contains parameters to select the domains, organizational units, and accounts to be included in the report.
Expired Accounts	Shows expired accounts for the selected domains. Contains a parameter to select the domains to be included in the report.
Golden Ticket Mitigation - Last Password Change for krbtgt account	Shows user password information for the krbtgt account. Attackers who have the krbtgt account password hash can forge Kerberos ticket-granting tickets (TGT), also known as a golden ticket. Golden tickets enable adversaries to generate authentication material for any account in Active Directory.
Privileged Accounts that are Sensitive and Cannot be Delegated	Shows all privileged accounts for selected domains that are configured with the "Account is sensitive and cannot be delegated" option.
Privileged Accounts that have Not Logged In	Shows privileged accounts in selected domains having unchanged passwords and have not logged in.
Privileged Accounts Vulnerable to the Kerberoast Attack	Shows all privileged user accounts that are vulnerable to the Kerberoast attack. Kerberoasting is an attack technique that attempts to crack the password of a service account within the Active Directory.
Privileged Accounts with Unchanged Passwords that Logged In	Shows privileged accounts in selected domains having unchanged passwords and have logged in.
User Account(s) that have Constrained Delegation	Shows all the domain users for the selected domains that have TRUSTED_FOR_AUTH_DELEGATION enabled. For details, see https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties
User Account(s) that have Unconstrained Delegation	Shows all the domain users for the selected domains that have TRUSTED_FOR_DELEGATION enabled. For details, see https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties
Users That Cannot Change the Set Password	Shows users that cannot change the set password for the selected domains. Contains parameters to select the domains and organizational units to be included in the report.
Users with Password Set to Never Expire	Shows users with password set to never expire for the selected domains. Contains parameters to select the domains and organizational units to be included in the report.
Migration Assessment	
Detailed Computer Information for Migration	Shows detailed information for the selected computers. The report includes the following sections to assist with migration efforts: for Local Groups, Local Administrators, Installed Software, Services, User Profiles, Shares and IP Addresses. Note: Computer detail information is only available if Computer and Active Directory collections that include the selected computers have been completed. Contains parameters to select the domains and computers to be included in the report.
Duplicate Domain Computers	Shows duplicate computers in the selected domains. Two or more domains must be specified. Contains a parameter to select the domains to be included in the report.
Duplicate Domain Groups	Shows duplicate groups in the selected domains. Two or more domains must be specified. Contains a parameter to select the domains to be included in the report.

Table 1. Active Directory Reports

Report Name	Description
Duplicate Domain Users	Shows duplicate users in the selected domains. Two or more domains must be specified. Contains a parameter to select the domains to be included in the report.
QMM Matching Computers	Shows computers that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source computer to the Extension Attribute 15 of the target computer. Contains parameters to select the source domain and the target domain for this report.
QMM Matching Groups	Shows groups that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source group to the Extension Attribute 15 of the target group. Contains parameters to select the source domain and the target domain for this report.
QMM Matching Users	Shows users that have been migrated (using Quest Migration Manager) from the selected source domain into the selected target domain by comparing the Object GUID of the source user to the Extension Attribute 15 of the target user. Contains parameters to select the source domain and the target domain for this report.
Passwords	
Accounts that can change or reset password for any user in the selected domains	Shows accounts that can change or reset the password of any user in the selected domains. Includes any accounts that are permissioned through group membership. Contains a parameter to select the domains to be included in the report. You may also set the maximum recursion depth for this report. The folder level value will start from zero. Examining the path of C:\FolderA\FolderB, C:\ is 0 levels deep. FolderA is 1 level deep. FolderB is 2 levels deep.
Domain Users with Changed Passwords	Shows all domain users who have changed their password in the selected time frame for the selected domains. Contains parameters to select the domains, organizational units, and users to be included in the report. Also contains the option to include users with passwords that have changed in the past _ days.
Domain Users with Expired Passwords	Shows all users with expired passwords for the selected domains. Contains parameters to select the domains, organizational units, and users to be included in the report.
Domain Users with Older Passwords	Shows all the users who have not changed their password in the selected time frame for the selected domains. Contains parameters to select the domains, organizational units, and users to be included in the report. Also contains the option to include users with passwords older than _ days.
Last Password Change and Logon for Domain Computers	Shows the last password change and last logon for computers in the selected domains. Contains parameters to select the domains, organizational units, and computers to be included in the report.
User Password Information	Shows user password information for the selected domains. Contains parameters to select the domains, organizational units, domain users, and accounts to be included in the report.

Active Directory Modernization Reports

The following table describes the Active Directory Modernization reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. For each report, you must specify the domains on which you want to report.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 2. Active Directory Modernization Reports

Report Name	Description
Assess and Remediate AD Configurations | Identify and Remediate AD Compromises	
DNS Server Information	Shows all the DNS settings for the selected DNS Servers.
Domain Computer Information	Shows domain computer information for the selected domains.
Domain Controller Advanced Auditing Policies	Shows the advanced auditing policies for the selected Domain Controller.
Domain Controller Computer Policies	Shows the computer policies for the selected Domain Controller.
Domain Controller Hot fix Information	Shows all the hotfixes and Windows updates applied to selected Domain Controller. When listing updates, the Operation field shows whether an installation or uninstallation was completed, and the Result field shows values such as, Succeeded, SucceededWithErrors, InProgress or NotStarted.
Domain Controller Information	Shows domain computer information for the selected domains.
Domain Controller Installed Features	Shows all installed features for the selected Domain Controller.
Domain Controller Installed Software Information	Shows all the installed software for the selected Domain Controller.
Domain Controller Services	Shows information about the services for the selected Domain Controller.
Domain Controller User Rights	Shows the user rights assignment for the selected Domain Controller.
Domain Functional Level	Shows the domain functional level for the selected domains.
Domain Groups	Shows all the domain groups for the selected domains.
Domain OU Structure	Shows the OU structure for the selected domains.
Domain Password Policy	Shows the password policy and account lockout policy for the selected domain.
Domain Sites	Shows all the sites for the selected domains.
Domain Summary	Shows a domain summary for the selected domains. Summary information is only available if Active Directory discovery collections that include object counts for the selected domains have been completed.
Domain Trusts	Shows all the trust relationships for the selected domains.
Domain Users at Risk	Shows the users who match one or more of the selected risk factors and therefore may pose a security risk in the selected domains. Includes a summary of risk factors used as criteria for this report.
User Password Information	Shows user password information for the selected users.

Table 2. Active Directory Modernization Reports

Report Name	Description
Users AdminSDHolder	Shows all Active Directory permissions for the selected domains and Active Directory objects. For more information see Protected Accounts and Groups in Active Directory at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory and Active Directory Configuration at https://attack.mitre.org/mitigations/M1015/.
Users All	Shows all the domain users for the selected domains.
Users Golden Ticket Mitigation - Last Password Change for krbtgt account	Shows user password information for the krbtgt account.
Users Privileged Accounts Vulnerable to the Kerberoast Attack	Shows all privileged user accounts that are vulnerable to the Kerberoast attack.
Users Privileged Accounts Vulnerable with Unchanged Passwords that Logged in	Shows privileged accounts in selected domains having unchanged passwords and have logged in.
Users with Older Passwords	Shows all the users who have not changed their password in the selected timeframe for the selected domains.
Assess and Remediate AD Configurations | Managed Risks from AD Trusts	
Domain Trusts	Shows all the trust relationships for the selected domains.
Identify and Manage Elevated Access | Identify and Manage Admin Accounts	
Active Directory Permissions - Dangerous permissions delegated	Shows all Active Directory permissions for the selected domains and Active Directory objects. These permissions can be used to attack Active Directory. For information about attack types, see https://attack.mitre.org/mitigations/M1015/.
Active Directory Permissions - Domain Controller Owners	Shows all Active Directory permissions for the selected domains and Active Directory objects. The Domain Administrators group or the Enterprise Administrators group are set as owners for domain controllers. For details, see Privileged Account Management at https://attack.mitre.org/mitigations/M1026/.
AdminSDHolder Permissions	Shows all Active Directory permissions for the selected domains and Active Directory objects. For more information see Protected Accounts and Groups in Active Directory at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory and Active Directory Configuration at https://attack.mitre.org/mitigations/M1015/.
Privileged Accounts that are Sensitive and Cannot be Delegated	Shows all privileged accounts for selected domains that are sensitive and cannot be delegated.
Privileged Accounts that have Not Logged In	Shows privileged accounts in selected domains that have not logged in the specified number of days.
Privileged Accounts Vulnerable to the Kerberoast Attack	Shows all privileged user accounts that are vulnerable to the Kerberoast attack.
Privileged Accounts with Unchanged Passwords that Logged In	Shows privileged accounts in selected domains having unchanged passwords and have logged in.

Table 2. Active Directory Modernization Reports

Report Name	Description
Privileged Domain Groups and Members	Shows the group memberships for the selected domains and groups. These privileged groups should have as few members as possible. DNSAdmins should have no members. If you include nested groups, the membership of the groups is displayed. For details, see Privileged Account Management https://attack.mitre.org/mitigations/M1026/
Identify and Manage Elevated Access | Identify and Manage Default Domain Groups	
Built-in AD Administrator Account Usage	Shows native Administrator account in selected domains who have logged in selected timeframe.
Privileged Domain Groups and Members	Shows the group memberships for the selected domains and groups. These privileged groups should have as few members as possible. DNSAdmins should have no members. If you include nested groups, the membership of the groups is displayed. For details, see Privileged Account Management https://attack.mitre.org/mitigations/M1026/.
Identify and Manage Elevated Access | Identify and Manage Resource Access	
Detailed Computer Information for Migration	Shows detailed information for the selected computers. The report includes the following sections to assist with migration efforts: Local Groups, Local Administrators, Installed Software, Services, User Profiles, Shares, and IP Addresses. Note: Computer detail information is only available if Computer and Active Directory collections that include the selected computers have been completed.
Manage Risks of Migrating SID History	
Accounts Where SID History Attribute Contains SID from Same Domain	Lists accounts whose SID History attribute contains an SID of another object in the same domain.
Domain Accounts (Users and Groups) with SID History Attribute not empty	Shows all the domain accounts for the selected domains which can leave accounts open to Access Token Manipulation: SID-History Injection. For details, see https://attack.mitre.org/techniques/T1134/005/.
SID History Auditing Group available in Domain (Migration in Progress)	Shows if a SID History auditing group has been created in the domain.
Tier 0 Object Reporting	
AdminSDHolder Permissions	Shows all Active Directory permissions for the selected domains and Active Directory objects. For more information see Protected Accounts and Groups in Active Directory at https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-c--protected-accounts-and-groups-in-active-directory and Active Directory Configuration at https://attack.mitre.org/mitigations/M1015/.
Domain Controller Information	Shows domain controller information for the selected domains.
Privileged Domain Groups and Members	Shows the group memberships for the selected domains and groups. These privileged groups should have as few members as possible. DNSAdmins should have no members. If you include nested groups, the membership of the groups is displayed. For details, see Privileged Account Management https://attack.mitre.org/mitigations/M1026/.
Privileged User Accounts	Shows the privileged accounts in selected domains.

Change History Reports

The following table outlines the change history reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. These reports show you changes over time to the selected objects, including additions, deletions, and changes to the properties.

Change history data must be enabled in the discovery that collected the data for the objects on which you want to report. If this data is not available in your report, contact your Enterprise Reporter administrator, or see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 3. Change History Reports

Report Name	Description
Active Directory Change History	Shows the changes made over time to the selected domains. Contains parameters to select the domains, changes, and date range to be included in the report.
Computer Change History	Shows the changes made over time to the selected computers. Contains parameters to select the domains, computers, changes, and date range to be included in the report.
Database Change History	Shows the changes made over time to the selected databases. Contains parameters to select the SQL Servers, instances, databases, changes, and date range to be included in the report.
Domain Group Membership Change History	Shows the changes made over time to domain group memberships. Contains parameters to select the domains, organizational units, groups, and date range to be included in the report.
Group Membership Change History	Shows the changes over time to group memberships. Contains parameters to select the group and date range to be included in the report. You must have group membership collection enabled in your discovery in order to have data for this report.
NTFS Change History	Shows the changes made over time to the selected NTFS objects (files, folders, and shares). Contains parameters to select the domains, computers, and date range to be included in the report.
Registry Change History	Shows the changes made over time to registry keys and values. Contains parameters to select the computers, changes, and date range to be included in the report.
SQL Server Change History	Shows the changes made over time to the selected SQL servers. Contains parameters to select the SQL Servers, instances, changes, and date range to be included in the report.

Computer Reports

The following table outlines the computer reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. For each report, you must specify the domains on which you want to report, and include at least one computer from one of the specified domains.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

TIP: If you include many or all computers in a selected domain, the amount of data in your report can result in a longer report generation time, and lengthy reports. You may find it helpful to create several smaller reports.

NOTE: If you are reporting on a NetApp filer, the available data is the general properties of the system, volumes, share, and group information.

Table 4. Computer Reports

Report Name	Description
All Installed Software Information	Shows all the installed software for the selected computers. Microsoft store applications are included. Contains parameters to select the domains, computers, and installed software to be included in the report.
Bitlocker Information	Shows the Bitlocker information for volumes on the selected computers. **Note:** Collecting information for encrypted volumes during discoveries is only possible if those volumes are unlocked. Contains parameters to select the domains, computers and volumes to be included in the report.
Computer Advanced Auditing Policies	Shows the computer advanced auditing policies for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer BIOS Information	Shows the BIOS information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Information	Shows computer information for the selected computers. Shows the general attributes of the selected computers, such as the operating system information. Contains parameters to select the domains, computers, types of servers, and operating systems to be included in the report.
Computer Network Adapter Information	Shows the network adapter information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Physical Memory Information	Shows the physical memory information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Policies	Shows the computer policies for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Security Identifiers (SIDs)	Shows computer security identifiers (SIDs) for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Security Options	Shows the computer security options for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Computer Services	Shows information about all installed services for the selected computers. Contains parameters to select the domains, computers, services, states, startup types, and accounts to be included in the report.
Computers With Less Than 1 GB of Free Disk Space	Shows all the computers with less than 1 GB of free disk space. Contains parameters to select the domains and computers to be included in the report.
Computers With Specific IP Address	Shows computer information for the selected IP addresses. Contains parameters to select the domains and IP addresses to be included in the report.

Table 4. Computer Reports

Report Name	Description
DNS Server Information	Shows all the DNS settings for the selected DNS Servers. Contains parameters to select the domains and computers to be included in the report.
Dynamic Host Configuration Protocol (DHCP) Service	Shows DHCP service information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Event Logs	Shows the event log settings for the selected computers. Contains parameters to select the domains, computers, and event logs to be included in the report.
Exchange Service	Shows Exchange Service information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Group Membership by Local Account	Shows all groups to which the selected computer accounts belong. Contains parameters to select the domains, computers, and accounts (user or group) to be included in the report.
Hotfixes and Updates	Shows all the hotfixes and Windows updates applied to selected computers. When listing updates, the Operation field shows whether an installation or uninstallation was completed, and the Result field shows values such as, Succeeded, SucceededWithErrors, InProgress or NotStarted.
Installed Software Information	Shows all the installed software for the selected computers. Contains parameters to select the domains, computers, and installed software to be included in the report.
Local Groups	Shows all the local groups for the selected computers. Contains parameters to select the domains, computers, and local groups to be included in the report.
Local Groups and Members	Shows the group memberships for the selected computers and groups. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the domains, computers, and local groups to be included in the report. Contains a parameter to include nested group memberships and options on how they are displayed in the report.
Local Users	Shows all the local users for the selected computers. Contains parameters to select the domains, computers, and user accounts to be included in the report. Also contains options to select locked/unlocked or disabled/enabled accounts.
Microsoft Store Application Information	Shows all the Microsoft store applications for the selected computers. Contains parameters to select the computers and Microsoft store applications to be included in the report.
Operating System Information	Shows operating system information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Printer Information	Shows the printer information for the selected computers. Contains parameters to select the domains, computers, printers, and printer statuses to be included in the report.
Remote Access Service	Shows Remote Access Service information for the selected computers. Contains parameters to include the domains and computers to be included in the report.
Scheduled Tasks	Shows the scheduled tasks for the selected computers. Contains parameters to select the domains, computers, and locations to be included in the report.
Server Features	Shows all the Windows Server Features for the selected computers.

Table 4. Computer Reports

Report Name	Description
Services Not Running as System Account	Shows all the services that are not running as the system account for the selected computers. Contains parameters to select the domains and computers to be included in the report. Contains hidden parameters to exclude, by default, account names containing the words “Local Service”, “System”, or “Network Service”.
Share Information	Shows the share information for the selected computers. Contains parameters to select the domains, computers, and type of shares to be included in the report.
User Profile Information	Shows all user profile information for the selected computers. Contains parameters to select the domains, computers, and users to be included in the report.
User Rights	Shows the user rights assignments for the selected computers. Contains parameters to select the domains, computers, user rights and accounts to be included in the report.
Volume Statistics	Shows the statistics for each volume for the selected computers. Contains parameters to select the domains, computers and volumes to be included in the report.
Windows Internet Name Service (WINS)	Shows WINS service information for the selected computers. Contains parameters to select the domains and computers to be included in the report.
Migration	
Detailed Computer Information for Migration	Shows detailed information for the selected computers. Report includes sections for Local Groups, Members of the Administrators group, Installed Software, Services, User Profiles, Shares, and IP Addresses to assist with migration efforts. **Note:** Computer detail information is only available if Computer and Active Directory collections that include the selected computers have been completed. Contains parameters to select the domains and computers to be included in the report.
Permissions	
Printer Permissions	Shows all the printer permissions for the selected computers and printers. Contains parameters to select the domains, computers, printers, and accounts to be included in the report.
Service Permissions	Shows all the service permissions for the selected computers and services. Contains parameters to select the domains, computers, services, and accounts to be included in the report.
Share Permissions	Shows the permissions for all shares on the selected computers. Contains parameters to select the domains, computers, shares, types of shares, and accounts to be included in the report.
Share Permissions for Account	Shows share permissions, including permissions derived through group membership, for the selected computers and the selected account. Contains parameters to select the account and its group membership, domains, computers, shares, and types of shares to be included in the report.

Table 4. Computer Reports

Report Name	Description
Share Permissions with Membership	Shows all the share permissions for the selected computers and shares. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the domains, computers, shares, types of shares, and accounts to be included in the report. If permissions are derived from membership in a group, the membership path of the permission is shown. You can filter the results by supplying a specific list of accounts to look for in the DACLs, and specific organizational units. Contains a parameter to include nested group memberships and options on how they are displayed in the report. For more information, see Searching for Parameter Values on page 80. Technical Documentation.
Shared Folder Permissions	Shows all NTFS permissions for the shared folders on the selected computers. **Note:** NTFS permission information is only available if NTFS discovery collections that include the selected shares have been completed. NTFS permissions have to be collected through the administrative share. Contains parameters to select the domains, computers, share, and account to be included in the report.

Enterprise Reporter System Reports

The following table outlines the Enterprise Reporter System reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 5. Enterprise Reporter System Reports

Report Name	Description
Enterprise Reporter Discoveries	Shows the collection discoveries for the selected discovery clusters. Contains a parameter to select the clusters to be included in the report.
Enterprise Reporter Discovery Clusters	Shows cluster and related node information for the selected discovery clusters. Contains a parameter to select the clusters to be included in the report.
Enterprise Reporter Discovery Errors	Shows discovery task errors for the selected discoveries. Contains a parameter to select the discoveries and the types of errors to be included in the report.
Enterprise Reporter Discovery Tasks	Shows the collection tasks for the selected discoveries. Contains a parameter to select the discoveries to be included in the report.

Exchange Reports

The following table outlines the Exchange reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. For each report, you must specify the organizations on which to report.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 6. Exchange Reports

Report Name	Description
Distribution Groups	
Distribution Group Details	Shows the detailed information of mail-enabled groups for the selected organizations. Mail-enabled groups include security and distribution group types. Membership filter information is shown when dynamic distribution groups are selected. Contains parameters to select the organizations, the distribution groups, or the type of distribution groups (static, dynamic, or unified) to be included in the report.
Distribution Group Membership by Account	Shows all mail-enabled distribution groups to which the selected accounts belong. Groups include security and distribution group types. Membership filters are displayed for dynamic groups. Contains parameters to select the organizations and the accounts to be included in the report.
Distribution Groups and Members	Shows all accounts that are members of the selected mail-enabled distribution groups. Groups include security and distribution group types. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the organizations and distribution groups to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Exchange	
Exchange Organization Overview	Shows a high-level summary of the information in your Exchange organization. You can drill to view detailed reports for each category in the report: • Mailboxes > Mailboxes Summary report • Mail-Enabled Users > Mail-Enabled Users report • Distribution Groups > Distribution Groups details report • Contacts > Mail Contacts report • Public Folders > Public Folders Summary report **Note:** This report includes system public folder information. • Servers > Exchange Server Details report
Mailboxes	
Exchange Mailboxes Overview	Shows a high-level summary of the number of mailboxes per server in your Exchange organizations. A bar chart displays the top 10 servers that contain the most mailboxes. You can drill down through the server name to view the Exchange Server Details report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Mailbox Delegates	Shows the mailboxes for the selected delegates.Contains parameters to select the organizations and mailbox delegates to be included in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.

Table 6. Exchange Reports

Report Name	Description
Mailbox Details	Shows detailed mailbox information for the selected servers. Contains parameters to select the organizations, servers, mailbox stores, and mailboxes to be included in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Mailbox Folder Details	Shows the mailbox folder information for the selected servers. Contains parameters to select the organizations, servers, mailbox stores, and mailboxes to be included in the report.
Mailboxes with Delegates	Shows the delegates for the selected mailboxes. Contains parameters to select the organizations, servers, and mailboxes to be included in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Permissions	
Mailbox Folder Permissions	Shows the mailbox folder permissions for the selected servers. Contains parameters to select the organizations, servers, mailbox stores, and mailboxes to be included in the report.
Mailbox Permissions	Shows the mailbox permissions for the selected servers. Contains parameters to select the organizations, servers, mailboxes, and types of permissions to be included in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Mailbox Permissions for Account	Shows the mailbox permissions for an account, including permissions derived through group membership. Contains parameters to select the account, organizations, servers, mailboxes, permission inheritance, and types of permissions. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Mailbox Permissions with Membership	Shows the permissions for the selected servers and mailboxes. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select organizations, servers, mailboxes, permission inheritance, and types of permissions. Also contains a parameter to include nested group memberships and options for how they are displayed in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Public Folder Permissions	Shows all folder permissions for the selected servers and public folders. Contains parameters to select the organizations, servers, public folders, accounts, and types of permissions to be included in the report. Also includes the options to exclude specific public folders and to filter inherited or explicit permissions. Contains hidden parameters to include, by default, only Exchange servers running the Mailbox server role, and to exclude, by default, system public folder information.
Public Folder Permissions for Account	Shows folder permissions, including permissions derived through group membership, for the selected account and the selected folders. Contains parameters to select the account, organizations, servers, public folders, permission inheritance, and types of permissions. Contains hidden parameters to include, by default, only Exchange servers running the Mailbox server role, and to exclude, by default, system public folder information.
Public Folder Permissions with Membership	Shows the folder permissions for the selected servers and folders. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the organizations, servers, public folders, permission inheritance, and types of permissions. Also contains a parameter to include nested group memberships and options for how they are displayed in the report. Contains hidden parameters to include, by default, only Exchange servers running the Mailbox server role, and to exclude, by default, system public folder information.
Public Folders	

Table 6. Exchange Reports

Report Name	Description
Exchange Public Folders Overview	Shows a high-level summary of the number of public folders per server in your Exchange organizations. You can drill down through the server names to view detailed reports. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role. **Note:** This report includes system public folder information.
Public Folder Details	Shows public folder details for the selected servers. Contains parameters to select the organizations, servers, and public folders to be included in the report. Contains hidden parameters to include, by default, only Exchange servers running the Mailbox server role, and to exclude, by default, system public folder information.
Servers	
Exchange Server Details	Shows Exchange server details. Includes computer attributes and volume information if computer discoveries have been completed for the selected servers. Contains parameters to select the organizations and servers to be included in the report. **Note:** The section containing the physical computer information and matching pie chart is only available if Computer discovery collections that include the selected servers have been completed.
Users and Contacts	
Mail Contacts	Shows the details for mail contacts in the selected organizations. Contains parameters to select the organizations and mail contacts to be included in the report.
Mail-Enabled Users	Shows the details for mail-enabled users in the selected organizations. Contains parameters to select the organizations and mail-enabled users to be included in the report.

File Storage Analysis Reports

The following table outlines the File Storage Analysis reports included in Enterprise Reporter. If you are a report user, your administrator may have made some of these reports available in Published Reports.

These reports use information collected from discoveries running over time to assist administrators with data life cycle management by providing storage assessments that can be used for storage planning and pre-migration assessments. Detailed reports provide historical information about resources such as servers, shares, volumes, folders, files, home directories and users.

The File Storage Analysis category displays a default Category Report in the report pane. For more information on setting the parameters of this report, see Running Category Reports on page 76.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

See also:

- File Categories
- Folder Categories

Days Until Critical Capacity

Some File Storage Analysis reports include an estimated number of Days Until Critical Capacity. This estimate is calculated using the following formulae:

- W = Sum U / Sum D
  Based on the most recent 25% of discoveries.
- Y = ((Rt * C/100) – Ru) / W

Where:

U = Used Space Changed between last two runs
D = No. of Days between the last two runs
W = Weighted Average
Y = Days until critical capacity
Rt = Recent Total Size
Ru = Recent Used Size
C = Critical Capacity Percent

The calculation is restricted to the discovery runs in the last 1 year. If the last discovery run is more than a year ago, **No data found** is displayed in the report.

Table 7. File Storage Analysis Reports

Report Name	Description
File Storage Analysis Overview	Shows a high-level summary of storage information for your network and highlights immediate storage needs to be addressed. The overview is based on all completed file storage analysis discoveries. You can drill down through the server name, categories, extensions and users to view more detailed reports. Contains a parameter to specify the percentage of used space that indicates critical capacity for this report.
Capacity Planning	
Capacity Planning	Shows storage growth and highlights any areas of critical capacity across your enterprise. **NOTE:** Growth trends are based on historical collections. If multiple collections are not available for comparison, growth projections are not available. This report is useful for evaluating your enterprise when capacity planning and for assessing servers during migration projects. It serves as an integral part of storage administration activities. You can drill down through the server name and the user name to view more detailed reports. A line graph displays the total enterprise growth by displaying the total amount of used space for all servers.
Server Capacity	Shows server capacity information. You can specify the percentage of used space that determines if a server is reaching critical capacity. You can drill down through the server name to view the Server Details report. **NOTE:** Estimated Days Until Critical Capacity indicates how many days it is expected to take for the server to reach the value set as critical capacity (a default of 80%) based on the current analysis of data increase per day. This report highlights servers that may be running out of disk space so that action can be taken. You can also use this report during server consolidation project planning to determine which servers to migrate first. A bar chart displays the top 10 servers sorted by days until critical capacity and indicates the percentage of used and free disk space.
Server Details	Shows server details with volume and share usage information for the selected servers. You can drill down through the logical disk or the share name to view detailed reports. This report is useful for determining your consolidation approach and for capacity planning. A pie chart displays the percentage of used and free disk space. Contains a parameter to select the server to be included in this report.

Table 7. File Storage Analysis Reports

Report Name	Description
Server Growth	Shows server growth information for the selected server. Growth details are sorted by dates of discovery runs. **NOTE:** Growth trends are based on historical collections. If multiple collections are not available for comparison, growth projections are not available. This report allows you to track the percentage of used space over time for servers and provides a snapshot of used and available space for each time the discovery was run. This report is useful for evaluating servers when planning migration projects and serves as an integral part of server administration. Contains parameters to select the server and the number of weeks/months/years to be included in the report.
Server Summary by Domain	Shows the total, used, and free disk space on each server in the selected domains. Servers are grouped by domain and sorted by server name. You can drill down through the server name to view the Server Details report. The Server Summary by Domain report is of critical importance when planning your consolidation projects since it provides the data volume information you can use to determine the scope of a consolidation project. Contains a parameter to select the domain to be included in the report.
Top Volumes	Shows top volumes sorted by used space. You can drill down through the server name and the logical disk name to view more detailed reports. A bar chart helps you visually compare the used space on the volumes. Contains a parameter to select the number of volumes to included in the report.
Volume Capacity	Shows volume capacity information. You can specify the percentage of used space that is used to determine if a volume is reaching critical capacity. You can drill down through the server name and the logical disk name to view more detailed reports. Identifying the volumes can help you create capacity projections, determine critical volumes for file cleanup or archiving activities, or plan an approach for server consolidation projects. A bar chart indicates the top 10 volumes sorted by days until critical capacity and indicates the percentage of used and free space. Contains a parameter to specify the percentage of used space that indicates critical capacity for the report.
Volume Details	Shows the volume details for the selected servers. You can also drill down through the logical disk to view a file summary for the volume. This report helps with ongoing capacity planning such as identifying volumes where disk space optimizations (cleanup, compression, or file offloading) are required. You can also use this report during server consolidation project planning to determine which servers and volumes to migrate first. A pie chart displays the percentage of used and free disk space. Contains parameters to select the servers and volumes to be included in the report.
Files and Folders	
File Categories	Shows details on the file categories that are used to group files in Enterprise Reporter. Lists the default types of files contained in each category. A file category contains various types of files or other file categories. Contains a parameter to select the file category to be included in the report.
File Category Details	Shows the file extensions that are included in the selected category on the selected servers. Categories are sorted by size. You can drill down through a file extension to view the File Information by Extension report. This report is useful for determining exactly what type of files are using storage space when you plan for future storage allocation. A bar chart displays the top 10 file extensions in the category based on size. Contains parameters to select the server and the file category to be included in the report.

Table 7. File Storage Analysis Reports

Report Name	Description
File Summary	Shows file summary information for the selected servers and volumes. You can drill down through the section titles to view more detailed reports. This report is useful for estimating migration schedules since the time needed to migrate data in large files is significantly less than the time needed to migrate the same amount of data in small files. A bar chart displays the number of files in each file size grouping. Another bar chart displays the actual space consumed by the files in each file size grouping. Contains the parameters to select the server and the volume to be included in the report.
Files by Category	Shows files grouped into pre-defined categories that are sorted by size. You can drill down through the file category name to view a detailed report of files in the category. This report is useful for identifying the files that you want to remove or migrate to a different storage location. A bar chart displays the categories sorted by size. Contains parameters to select the server and the category to be included in the report.
Folder Categories	Shows details on the folder categories that are used to group folders in Enterprise Reporter. Lists the default folder paths contained in each category and describes the types of files typically found in the folders.
Folders by Category	Shows folders grouped in pre-defined categories that are sorted by used space. This report is useful for identifying groups of folders that you want to remove or migrate to a different storage location. A bar chart displays the amount of used space per category. Contains parameters to select the server and the folder category to be included in the report.
Storage Cleanup	Shows storage areas across your enterprise where you can potentially reclaim space through data cleanup or by migrating files to different storage locations. The report is based on all completed server discoveries. You can also drill down through the server name to view more detailed reports. Note: This information is only available if NTFS discoveries have been completed with the duplicate file collection option enabled. This report is useful for assessing your current storage needs prior to migration and as a part of regular data cleanup operations. A pie chart displays the total amount of space recommended for cleanup on all servers.
Top File Extensions	Shows top file extensions sorted by size. You can drill down through any file extension to view the File Information by Extension report. A bar chart displays up to the top 10 file extensions sorted by size. Contains a parameter to select the number of file extensions to be included in the report.
Home Directories	
Home Directory Details	Shows home directory details for the selected servers. This report can be used for planning home directory updates by identifying the users who are consuming space on the server. Contains the parameters to select the servers and the accounts to be included in the report.
Home Directory Summary	Shows home directory summary information. The report is based on all completed server discoveries. You can drill down through the server name or the number of home directories to view more detailed reports. A bar chart displays the total amount of space used by home directories on each server.
Top Home Directories	Shows top home directories sorted by size. You can drill down through the server name to view the Server Details report. This report can be used to prepare for home directory migrations, to maintain storage quotas, and for storage management activities. A bar chart displays the top home directories sorted by size. Contains a parameter to select the number of home directories to be included in the report.

Table 7. File Storage Analysis Reports

Report Name	Description
Shares	
Share Details	Shows share details for the selected servers. This report can be used during server consolidation project planning to determine which server shares to migrate first. Contains parameters to select the servers and the shares to be included in the report.
Share File Details	Shows file details for the selected shares. This report is valuable when planning for data reorganization or preparing for storage consolidation. **NOTE:** Share file detail information is only available if Computer and NTFS permission discovery collections that include the selected shares have been completed. Contains parameters to select the server and the share to be included in the report.
Share Summary	Shows share summary information. The report is based on all completed server discoveries. You can drill down through the server name or the number of shares to view more detailed reports. This report is useful for ongoing share management as well as preparing for share migration in server consolidation projects. A bar chart displays the total amount of space used by shares on each server.
Top Shares	Shows top shares sorted by size. You can drill down through the server name and the share name to view more detailed reports. This report is useful for ongoing data assessment, for planning server consolidation projects, or for determining if specific users are outside acceptable levels of disk space usage. A bar chart displays the top 10 shares sorted by size. Contains a parameter to select the number of shares to include in the report.
Users	
Top Users	Shows the top users using the most space. This report is useful for analyzing user storage needs and for quota management activities. A bar chart displays up to the top 10 users sorted by size. Contains a parameter to select the number of users to be included in the report.
User Growth	Shows user storage growth over time. User growth details are sorted by dates of discovery runs. **NOTE:** Growth trends are based on historical collections. If multiple collections are not available for comparison, growth projections are not available. This report is useful for identifying users with the fastest growing storage needs over time. The report provides a snapshot of the amount of storage used by the user each time the discovery was run. Use the report to evaluate user storage needs when planning consolidation projects and as an integral part of user storage management activities. A line graph shows the size of storage over time for the user on the server. Contains parameters to select the user, server, and number of weeks/months/years to be included in the report.

File Categories

The following table outlines the file extensions that are grouped into each file category.

Table 8. File Categories

File Category Name	Category Description	File Extensions	
Against Policy	Files Categories from this table that violate the enterprise file storage policy.	Media Files	Wasted Space Files
All Media Files	File Categories from this table that contain image, audio, video, or internet information.	Graphic Files Internet Files	Movie Files Sound Files
Application Files	Files that contain executables and assemblies.	.app .bat .cgi .com .exe	.jar .pif .vb .wsf
Compressed Files	Files that are compressed using ZIP compression.	.7z .rar	.zip .zipx
Data Files	File types used to identify formatted data.	.csv .dat .gbr .sdf	.tar .vcf .xml
Database Files	File types used to identify database queries, data, and log files.	.accdb .db .dbf	.mdb .pdb .sql
Disk Image Files	File types used to identify virtual disks and disk images.	.bin .cue .iso	.mdf .vcd
Document Files	File types created by the Microsoft Office® suite of programs.	.doc .docx .indd .mdb .odb .odt .pages .pct .pdf .pps	.ppt .pptx .rtf .tex .txt .wpd .wps .xls .xlsx
Email Files	File types used to identify messages and indexes created by various email programs.	.eml .idx .mbx .msg	.pab .pst .wab

Table 8. File Categories

File Category Name	Category Description	File Extensions	
Graphic Files	File types produced by graphic software tools, digital photo software, and software that captures documents as electronic images.	.ai	.pic
		.al	.png
		.al3	.pnp
		.al4	.ps
		.al5	.psd
		.bmp	.pspimage
		.eps	.pxr
		.flm	.raw
		.gif	.rle
		.icd	.sct
		.jpe	.swf
		.jpg	.tga
		.pcd	.thm
		.pct	.tif
		.pcx	.tiff
		.pdd	.vda
		.pdf	.vst
		.pdp	
Movie Files	File types used to identify digital animation files, interactive audio/visual files, and media player files.	.asf	.mpg
		.asx	.qt
		.avi	.ram
		.m1v	.rm
		.m4v	.rmx
		.mov	.rt
		.mp2	.smi
		.mp4	.swf
		.mpa	.viv
		.mpe	.vob
		.mpeg	.wmv
Paging Files	Files used to define virtual memory settings for the server.	hiberfil.sys	pagefile.sys
Sound Files	Files types used to identify digital and audio files.	.afic	.mp3
		.agp	.mp4
		.aif	.mpa
		.aiff	.pps
		.au	.ra
		.iff	.snd
		.jpa	.wav
		.m3u	.wax
		.m4a	.wma
		.mid	.wvx

Table 8. File Categories

File Category Name	Category Description	File Extensions	
System Files	File types used to identify by operating system files such as driver files and image files.	.cab .cpl .cur .dll .dmp	.drv .ico .lnk .sys
Temporary Files	File types used to identify temporary files.	.bak .dmp .log	.tmp ~$*.*
Unknown File Extensions	File extensions that are not categorized.		
Wasted Space	File Categories from this table that may be needlessly using storage space.	Temporary Files	Movie Files
Web Files	File types that identify web site files such as html files, cascading style sheet files, browser cookie files, and graphic files.	.asp .aspx .cer .cfm .csr .css .htm	.html .js .jsp .mht .php .rss .xhtml

Folder Categories

The following table outlines the folder paths that are grouped into each folder category.

Table 9. Folder Categories

Folder Category Name	Category Description	Folder Paths
Applications	Folders typically used to store application program files and settings.	\Applications \Program Files \Program Files (x86)
Exchange Data	Folders that contain Microsoft Exchange Server messaging data files.	\Exchsrvr \Program Files\Exchsrvr \Program Files\Microsoft\Exchange Server
Home Directories	Folders that contain user home directories.	\Home \Users
Operating System	Folders that contain Microsoft Windows operating system files.	\Windows \WINNT \WINNT351 \WINNT4 \WINNT40 \WINNT5
Oracle Database Data	Folders that contain Oracle database data files.	\OraData \OraNT \OraWin95

Table 9. Folder Categories

Folder Category Name	Category Description	Folder Paths
Recycle Bin	Folder that temporarily stores deleted files and folders before they are permanently erased.	\$Recycle.Bin
Share Point Portal	Folders that contain Microsoft SharePoint Portal Server document management data files.	\Program Files\Common Files\Microsoft Shared\MSSearch \Program Files\Common Files\Microsoft Shared\Web Storage System \Program Files\SharePoint Portal Server
SQL Server	Folders that contain Microsoft SQL Server files such as database engine, client components, and data files.	\MSSQL \MSSQL2000 \MSSQL6 \MSSQL7 \Program Files\Microsoft SQL Server
SQL Server Database	Folders that contain Microsoft SQL Server data files.	\MSSQL\Data \MSSQL2000\Data \MSSQL6\Data \MSSQL7\Data \Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL15.MSSQLSERVER\MSSQL\DATA \Program Files\Microsoft SQL Server\MSSQL16.MSSQLSERVER\MSSQL\DATA

Table 9. Folder Categories

Folder Category Name	Category Description	Folder Paths
Temporary Data	Folders that are used to store temporary files.	\Temp \Windows\Temp \WINNT\Temp
Web	Folders that contain files used in web sites.	\InetPub

Hybrid Reports

The following table outlines the Hybrid reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 10. Hybrid Reports

Report Name	Description
Exchange Hybrid Migrated Mailbox Permissions with Membership	Shows the permissions for the mailboxes migrated to Microsoft 365 in an Exchange hybrid environment. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, mailboxes, and mailbox types to be included in the report. Also includes the option to filter inherited or explicit permissions.
Exchange Hybrid Migrated Mailboxes	Shows mailboxes that have been migrated to Microsoft 365 in an Exchange hybrid environment. Contains parameters to select the tenants and mailboxes to be included in the report.
OneDrive and NTFS File and Folder Permissions for Account	Shows OneDrive and NTFS file and folder permissions for the selected synchronized domain account. OneDrive and NTFS file and folder permissions are only available if the Microsoft Entra ID, OneDrive, and NTFS collections have been completed. Account information will only be available if synchronization is enabled between the OneDrive and On-premises environments at the time of collection. **Note:** No wildcard support available. Contains a parameter to select the synchronized domain account to be included in the report.
OneDrive and NTFS File and Folder Permissions for Account with Group Membership	Shows OneDrive and NTFS file and folder permissions for the selected synchronized domain account including permissions derived through group membership. OneDrive and NTFS file and folder permissions are only available if the Microsoft Entra ID, OneDrive, and NTFS collections have been completed. Account information will only be available if synchronization is enabled between the OneDrive and On-premises environments at the time of collection. **Note:** No wildcard support available. Contains a parameter to select the synchronized domain account to be included in the report.

Microsoft Entra Reports

NOTE: Azure Active Directory has been renamed to Microsoft Entra ID. The structure of the report library has been revised to reflect this change. Please republish the reports in the report library to implement this update.

The following table describes the Microsoft Entra reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 11. Microsoft Entra Reports

Report Name	Description
Entra ID	
Microsoft Entra Application Information	Shows all the applications for the selected tenants. Contains parameters to select the tenants and applications to be included in the report. Also contains a parameter to include only native applications.
Microsoft Entra Application Permissions	Shows the application permissions for the selected tenants. Contains parameters to include tenants and applications to be included in the report. Also contains a parameter to include only native applications.
Microsoft Entra Application Service Principals	Shows all the applications for the selected tenants. Contains parameters to include the tenants, applications, and service principals to be included in the report.
Microsoft Entra Contact Information	Shows all the contacts for the selected tenants. Contains parameters to select tenants and contacts to be included in the report. Also contains a parameter to include only contacts connected with on-premises Active Directory.
Microsoft Entra Deleted Users	Shows deleted users for the selected tenants. Contains a parameter to select the tenants to be included in the report.
Microsoft Entra Device Information	Shows all devices for the selected tenants. Contains parameters to select tenants and devices to be included in the report. Also contains a parameter to include only devices connected with on-premises Active Directory.
Microsoft Entra Domain Information	Shows all the domains for the selected tenants. Contains parameters to select tenants and domains to be included in the report. Also contains a parameter to include only verified domains.
Microsoft Entra Group Information	Shows all the groups for the selected tenants. Contains parameters to select tenants and groups to be included in the report. Also contains a parameter to include only groups connected with on-premises Active Directory.
Microsoft Entra Group Membership for Identity	Shows all groups to which the selected entities belong. Contains parameters to select the tenants and identities to be included in the report.
Microsoft Entra Groups and Members	Shows the group memberships for the selected tenants. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants and groups to be included in the report.
Microsoft Entra Groups Connected with On-Premises Active Directory	Shows all the Microsoft Entra groups whose identity information is synchronized with on-premises directories for the selected tenants. Contains parameters to select tenants and groups to be included in the report.
Microsoft Entra Groups with Dynamic Membership	Shows all the groups with dynamic memberships for the selected tenants. Contains parameters to select tenants and groups to be included in the report.

Table 11. Microsoft Entra Reports

Report Name	Description
Microsoft Entra Identities	Shows all the Microsoft Entra identities for the selected tenants. Contains parameters to select tenants and identity types to be included in the report.
Microsoft Entra Identities with Connected On-Premises Status	Shows the on-premises connection status for the selected identities, identity types, and tenants. Contains parameters to select tenants, identities, and identity types to be included in the report.
Microsoft 365 Groups	Shows all the Microsoft 365 groups for the selected tenants. Contains parameters to select tenants and groups to be included in the report.
Microsoft Entra Orphaned Groups	Shows groups without owners for the selected tenants. Contains parameters to select tenants and groups to be included in the report.
Microsoft Entra Privileged Roles for User	Shows the assigned roles for the selected users. Contains parameters to select tenants and users to be included in the report. This report displays role names that differ from those displayed in the Microsoft Entra Admin Center. **Microsoft Entra Admin Center Role Name -- Report Role Name** • Global administrator -- Company administrator • Password administrator -- Helpdesk administrator • Skype for Business Service administrator -- Lync Service administrator
Microsoft Entra Roles and Members	Shows all the roles and their members for the selected tenants. Contains parameters to select tenants and roles to be included in the report. This report displays role names that differ from those displayed in the Microsoft Entra Admin Center. **Microsoft Entra Admin Center Role Name -- Report Role Name** • Global administrator -- Company administrator • Password administrator -- Helpdesk administrator • Skype for Business Service administrator -- Lync Service administrator
Microsoft Entra Security Groups	Shows all the security groups for the selected tenants. Contains parameters to select tenants and groups to be included in the report.
Microsoft Entra Service Principal Assignments with Members	Shows the service principal assignments for the selected tenants. If you choose to include nested groups, membership of the assignment is displayed. Contains parameters to select the tenants and service principals to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Microsoft Entra Service Principals	Shows all the service principals for the selected tenants. Contains parameters to select the tenants and service principals to be included in the report. Also contains a parameter to include service principals with a registered application on the tenant.
Microsoft Entra ID Summary	Shows a summary information with statistics for the selected tenants. Contains a parameter to select the tenants to be included in the report. Each tenant includes a table summarizing the number of users, groups, contacts, and service principals as well as statistics for Microsoft Entra users, groups, roles, and application service principals.
Microsoft Entra User Devices	Shows all the users and their devices for the selected tenants. Contains parameters to select tenants and users to be included in the report.
Microsoft Entra User Information	Shows all the users for the selected tenants. Contains parameters to select tenants and users to be included in the report. Also contains parameters to include only enabled users or only users connected with on-premises Active Directory.

Table 11. Microsoft Entra Reports

Report Name	Description
Microsoft Entra Users Connected with On-Premises Active Directory	Shows all Microsoft Entra users whose identity information is synchronized with on-premises directories for the selected tenants. Contains parameters to select tenants and users to be included in the report.
Microsoft Entra Users Flagged for Risk	Shows all the users for the selected tenants that are flagged as at risk. Contains parameters to select the tenants, risks updated within the past (N) days, and risk levels to be included in the report.
Microsoft Entra Users with Multi-Factor Authentication Information	Shows users with multi-factor authentication information for the selected tenants. Contains parameters to select the tenants, users, and multi-factor authentication statuses to be included in the report.
Microsoft Entra Global Administrators with Multi-Factor Authentication Disabled	Shows global administrators that do not have multi-factor authentication enabled or enforced on the selected tenants. Contains a parameter to select the tenants to be included in the report. Contains hidden parameters to include, by default, company administrators and users with multi-factor authentication status set to disabled.
Microsoft Entra Managers with Direct Reports	Shows all the direct reports for the selected managers. Contains parameters to select the tenants and Microsoft Entra managers to be included in the report.
Microsoft Entra Tenant Information	Shows general information for the selected tenants. Contains a parameter to select tenants to be included in the report.
Microsoft Entra Tenant Password Reset Policies	Shows password reset policy information for the selected tenants. Contains parameters to select the tenants to be included in the report.
Microsoft Entra Tenant User Settings	Shows Microsoft Entra tenant level user settings for selected tenants. Contains a parameter to select tenants to be included in the report.
Circular Nested Microsoft Entra Groups	Shows information about groups which recursively contain themselves for the selected Microsoft Entra tenants. Contains a parameter to select the tenants to be included in the report.
Azure Resources	
Azure Classic Disk Information	Shows general information for the classic disks on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, virtual machines, and classic disks to be included in the report.
Azure Classic Storage Account Information	Shows general information for the classic storage accounts on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and storage accounts to be included in the report.
Azure Classic Virtual Machine Information	Shows information for the classic virtual machines on the selected tenant. Contains parameters to select the tenants, subscriptions, resource groups, and classic virtual machines to be included in the report.
Azure Classic Virtual Machine with Networking Information	Shows classic virtual machines with networking information on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and classic virtual machines to be included in the report.
Azure Disk Information	Shows general information for the disks on the selected tenants. Contains parameters to select tenants, subscriptions, resource groups, and disks.
Azure IP Configuration Information	Shows IP configuration resources on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and IP configurations to be included in the report.
Azure Network Interface Information	Shows network interfaces on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and network interfaces to be included in the report.
Azure Network Security Group Information	Shows general information for the network security groups on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and network security groups.

Table 11. Microsoft Entra Reports

Report Name	Description
Azure Resource Group Information	Shows general information for the resource groups on the selected tenants. Contains parameters to select tenants and subscriptions to be included in the report.
Azure Resource Information	Shows general information for the resources for the selected tenants. Contains parameters to select tenants, subscriptions, resource groups, and resource types to be included in the report.
Azure Resource Subscription Information	Shows general information for the resource subscriptions for the selected tenants. Contains a parameter to select tenants to be included in the report.
Azure Resource Summary	Shows a summary of the azure resources on the selected tenants. Contains a parameter to select the tenants to be included in the report.
Azure Storage Account Information	Shows general information for the storage accounts on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and storage accounts to be included in the report.
Azure Virtual Machine Drive Information	Shows information for the virtual machine drives on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and virtual machines to be included in the report.
Azure Virtual Machine Information	Shows information for virtual machines on the selected tenant. Contains parameters to select the tenants, subscriptions, and resource groups, and virtual machines to be included in the report.
Azure Virtual Machine with Networking Information	Shows virtual machines with networking information on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and virtual machines to be included in the report.
Azure Virtual Machines	Shows all types of virtual machines including classic and standard on the selected tenants. Contains a parameter to select the tenants to be included in the report.
Azure Virtual Network Information	Shows virtual networks on the selected tenants. Contains parameters to select the tenants, subscriptions, resource groups, and virtual networks to be included in the report. Also contains a parameter to include whether the virtual machine protection flag has changed.
Resources | Access Control	
Azure Resource Access Control for Identity	Shows resource access control, including access derived through group membership, for the selected resources and the selected identity. Contains parameters to select the identity, tenants, subscriptions, resource groups, and resources to be included in the report.
Azure Resource Access Control with Membership	Shows permissions for the resources on the selected tenants. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, subscriptions, resource groups, resource, and roles to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Azure Resource Group Access Control for Identity	Shows resource group access control, including access derived through group membership, for the selected resource groups and the selected identity. Contains parameters to select the identity, tenants, subscriptions, and resource groups to be included in the report.
Azure Resource Group Access Control with Membership	Shows permissions for the resource groups on the selected tenants. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, subscriptions, resource groups, and roles to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.

Table 11. Microsoft Entra Reports

Report Name	Description
Azure Resource Subscription Access Control for Identity	Shows resource subscription access control, including access derived through group membership, for the selected subscriptions and the selected identity. Contains parameters to select the identity, tenants, and subscriptions, to be included in the report.
Azure Resource Subscription Access Control with Membership	Shows permissions for the resource subscriptions on the selected tenants. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, subscriptions, and roles to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Subscriptions and Licenses	
Microsoft Entra Licensed Users for Department	Shows licensed users for the selected departments. Contains parameters to select tenants, users, and departments to be included in the report.
Microsoft Entra Licensed Users with Service Plans	Shows licensed users with service plan information for the selected tenants. Contains parameters to select tenants and users to be included in the report.
Microsoft Entra License Information	Shows subscription information for the selected tenants. Contains parameters to select tenants and licenses to be included in the report.
Microsoft Entra Service Plan Usage	Shows service plan usage information for the selected tenants. Contains parameters to select tenants and service plans to be included in the report.
Microsoft Entra Users without a License	Shows all users without a license for the selected tenants. Contains parameters to select tenants and users to be included in the report.

Microsoft SQL Server Reports

The following table outlines the Microsoft SQL Server reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 12. Microsoft SQL Server Reports

Report Name	Description
Databases	
SQL Database Objects	Shows all SQL database objects. Contains parameters to select the SQL servers, SQL instances, and SQL databases to be included in the report.
SQL Databases	Shows all SQL databases. Contains parameters to select the SQL servers, SQL instances, and SQL databases to be included in the report.
Jobs	
SQL Server Job Information	Shows information for the jobs on the selected SQL servers. Contains parameters to select the SQL servers and database jobs to be included in the report.
Permissions	

Table 12. Microsoft SQL Server Reports

Report Name	Description
Account Permissions for SQL Database Objects	Shows the direct or indirect database object permissions for the selected accounts. Contains parameters to select the AD or SQL Login accounts, SQL servers, SQL instances, SQL databases, and object types to be included in the report.
SQL Database Object Permissions	Shows all SQL Server® database objects and their permissions. Contains parameters to select the SQL servers, SQL instances, SQL databases, object types, permission types, and object permissions to be included in the report.
SQL Database Schema Permissions	Shows all database schemas and their assigned permissions on the database. Contains parameters to select the SQL servers, SQL instances, SQL databases, schemas, owners, permission types, and schema permissions to be included in the report.
SQL Server Instance Permissions	Shows SQL Server instance permissions for the selected instances. Contains parameters to select the SQL servers and SQL instances to be included in the report.
Roles and Users	
SQL Database Role Membership	Shows membership for each SQL Server role. Contains parameters to select the SQL servers, SQL instances, SQL databases, and SQL roles to be included in the report.
SQL Database Role Membership by Account	Shows all database roles of which the selected accounts are direct or indirect members. Contains parameters to select the AD or SQL Login accounts, SQL servers, SQL instances, and SQL databases to be included in the report.
SQL Database Users	Shows all SQL database users. If you choose to expand groups, membership of the groups is displayed. Contains parameters to select the SQL servers, SQL instances, SQL databases, and SQL database users to be included in the report. Contains a parameter to include nested group memberships and options on how they are displayed in the report. For more information, see Searching for Parameter Values on page 80. Technical Documentation.
SQL Logins	Shows all SQL logins. Contains parameters to select the SQL servers, SQL instances, SQL login types, and SQL logins to be included in the report.
SQL Server Role Membership by Account	Shows all server roles of which the SQL Server® logins are direct or indirect members. Contains parameters to select the AD or SQL Login accounts, SQL servers, SQL instances, and SQL roles to be included in the report.

Microsoft 365 Reports

The following table outlines the Microsoft 365 reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters. For more information, see how To enter a parameter value on page 79.

NOTE: Whenever OneDrive reports provide a parameter for filtering the report by drive, you may specify “Organization” or “Anonymous” to include documents with internal links (organization) or public links (anonymous).

Table 13. Microsoft 365 Reports

Report Name	Description
Microsoft 365 Overview	Shows a high-level overview for the selected Microsoft 365 tenants. Overview includes summary information for Microsoft Entra ID, Exchange Online, OneDrive, Microsoft Teams, and SharePoint Online. Contains a parameter to select the tenants to be included in the report.
Exchange Online	
Exchange Online Summary	Shows a summary of your Exchange Online organization for the selected Microsoft 365 tenants. System public folders are excluded from this report. Contains a parameter to select the tenant to be included in the report.
Exchange Online | Groups	
Mail-Enabled Dynamic Groups	Shows the dynamic groups for the selected Microsoft 365 tenants. Membership rules will be shown for dynamic groups. Contains parameters to select the tenants and groups to be included in the report.
Mail-Enabled Group Information	Shows the detailed information of mail-enabled groups for the selected Microsoft 365 tenants. Mail-enabled groups include security and distribution group types. Contains parameters to select the tenants and groups to be included in the report.
Mail-Enabled Group Membership by Identity	Shows all mail-enabled groups to which the selected identities belong. Groups include security and distribution group types. Contains parameters to select the tenants and identities to be included in the report.
Mail-Enabled Groups and Members	Shows all identities that are members of the selected mail-enabled groups. Groups include security and distribution group types. Contains parameters to select the tenants and groups to be included in the report. Contains a hidden parameter to include only Azure users with User Type set to Guest.
Exchange Online | Mailboxes and Public Folders	
Mailbox Delegates	Shows the mailboxes for the selected delegates.Contains parameters to select the tenants and mailbox delegates to be included in the report.
Mailbox Folder Information	Shows the mailbox folder information for the selected Microsoft 365 tenants. Contains parameters to select the tenants and mailboxes to be included in the report.
Mailbox Information	Shows the detailed mailbox information for the selected Microsoft 365 tenants. Contains parameters to select the tenants and mailboxes to be included in the report.
Mailbox Size Information	Shows the mailbox size information for the selected Microsoft 365 tenants. Contains parameters to select the tenants and mailboxes to be included in the report.
Mailboxes With Delegates	Shows the mailbox delegates for the selected Microsoft 365 tenants. Contains parameters to select the tenants and mailboxes to be included in the report.
Mailboxes With Recent Logons	Shows the mailboxes in the selected tenants that have logged on in the selected time frame. Contains parameters to select the tenants, mailboxes, and time frame to be included in the report.
Public Folder Information	Shows the detailed public folder information for the selected Microsoft 365 tenants. Contains parameters to select the tenants and public folders to be included in the report.
Exchange Online | Permissions	
Mailbox Folder Permissions	Shows the mailbox folder permissions for the selected tenants. Contains parameters to select the tenants and mailboxes to be included in the report.

Table 13. Microsoft 365 Reports

Report Name	Description
Mailbox Permissions for Identity	Shows the mailbox permissions for an identity, including permissions derived through group membership. Contains parameters to select the identity and its group memberships, tenants, mailboxes, and types of mailboxes to be included in the report. Also includes the option to filter inherited or explicit permissions.
Mailbox Permissions with Membership	Shows the mailbox permissions for the selected Microsoft 365 tenants. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, mailboxes. and types of mailboxes to be included in the report. Also includes the option to filter inherited or explicit permissions. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Public Folder Permissions for Identity	Shows all public folder permissions for an identity, including permissions derived through group membership for the selected Microsoft 365 tenants. System public folders are excluded from this report. Contains parameters to select the identity and its group membership, tenants, and public folders to be included in the report.
Public Folder Permissions with Membership	Shows the public folder permissions for the selected Microsoft 365 tenants. If you choose to include nested groups, membership of the groups is displayed. System public folders are excluded from this report. Contains parameters to select the tenants and public folders to be included in the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Exchange Online | Users and Contacts	
Mail Contacts	Shows the details for mail contacts in the selected Microsoft 365 tenants. Contains parameters to select the tenants and mail contacts to be included in the report.
Mail-Enabled Users	Shows the details for mail-enabled users in the selected Microsoft 365 tenants. Contains parameters to select the tenants and mail-enabled users to be included in the report.
Microsoft 365 Active Users	
Microsoft 365 Active Users	Shows which Microsoft 365 product licenses are being used by which users in your organization.
Microsoft Teams	
Microsoft Dysfunctional Teams	Shows any Microsoft Teams with no owners and/or one member or less.
Microsoft Team Applications Information	Shows all the Microsoft Team Applications for the selected tenants. Contains parameters to select the tenants, teams, and applications to be included in the report.
Microsoft Team Channels Information	Shows all the Microsoft Team Channels for the selected tenants. Contains parameters to select the tenants, teams, and channels to be included in the report.
Microsoft Team Files and Folders Information	Shows file and folder information for the selected tenants and drives. Contains parameters to select the tenants, teams, drives, and files and folders to be included in the report. Contains a parameter to select the files and folders to be excluded from the report.
Microsoft Teams for Identity	Shows all teams to which the selected identities belong. Contains parameters to select the tenants and identities to be included in the report.
Microsoft Team Members	Shows all the members of the Microsoft Teams for the selected tenants. Contains parameters to select the tenants and teams to be included in the report.

Table 13. Microsoft 365 Reports

Report Name	Description
Microsoft Team Owners Information	Shows all the Microsoft Team Owners for the selected tenants. Contains parameters to select the tenants and teams to be included in the report.
Microsoft Team Settings Information	Shows all the Microsoft Teams for the selected tenants. Contains parameters to select the tenants and teams to be included in the report.
Microsoft Teams Organization Settings	Shows the Microsoft Teams Organization Settings for the selected tenants. This includes settings for External access, Guest call access, Guest meeting access, Guest messaging access, and Teams settings.
Microsoft Teams Privacy Information	Shows the privacy information of the selected Microsoft Teams for the selected tenants, teams, channels, private teams options, and private channels options.
Microsoft Teams Summary	Shows a summary of Microsoft Teams for the selected Microsoft 365 tenants. Contains a parameter to select the teams to be included in the report.
Microsoft Teams Tabs	Shows the Microsoft Teams tabs for the selected channels, teams, and tenants. Contains parameters to select tenants, teams, channels, and tabs to be included in the report.
Microsoft Teams with Guest Members	Shows only Microsoft Teams with guest members for the selected tenants. The information is based on all completed Microsoft Teams and Microsoft Entra ID discoveries. Contains parameters to select the tenants to be included in the report.
Microsoft Teams Policy	
Microsoft Teams Application Permission Policies	Shows the Microsoft Teams Application Permission Policies for the selected tenant. The policies are Global for the tenant and Tenant apps for applied to specific applications.
Microsoft Teams Calling Policies	Shows the Microsoft Teams Calling Policies for the selected tenants. The policies include Allow Calling, Allow Calling Prevent Forwarding to Phone, Allow Calling Prevent Toll Bypass, Disallow Calling and Global.
Microsoft Teams Meeting Policies	Shows the Microsoft Teams Meeting Policies for the selected tenants. The policies include settings for All Off, All On, Default, Global, Kiosk, Restricted Anonymous Access and Restricted Anonymous no Recording.
Microsoft Teams Messaging Policies	Shows the Microsoft Teams Messaging Policies for the selected tenants. The policies include Default, Global and any created policies in use.
Microsoft Teams Team and Channel Policies	Shows the Microsoft Teams Team and Channel Policies for the selected tenants. The policies are Default and Global.
Microsoft Teams User Policies	Shows some Microsoft Teams Policies for the selected users.
OneDrive	
OneDrive Configuration Settings	Shows OneDrive configuration settings for the selected tenants. Contains parameters to select the tenants to be included in the report.
OneDrive File and Folder Information	Shows file and folder information for the selected tenants and drives. Contains parameters to select the tenants, drives, and files and folders to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.
OneDrive File and Folder Information Grouped by Parent Path	Shows the information for all files and folders grouped by parent path. Contains parameters to select the tenants, drives, and folders to be included in the report. Contains a parameter to select the folders to be excluded from the report.
OneDrive File and Folder Link Information	Shows the link information for shared files and folders on the selected drives. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.

Table 13. Microsoft 365 Reports

Report Name	Description
OneDrive Files and Folders with Access Links	Shows the files and folders that have internal or external access links. Contains parameters to select the tenants and drives to be included in the report.
OneDrive Files and Folders with an Anonymous Access Link	Shows the files and folders that have an anonymous access link for outside the organization. Contains parameters to select the tenants and drives to be included in the report.
OneDrive Files and Folders with an Organization Access Link	Shows the files and folders that have an access link for inside the organization. Contains parameters to select the tenants and drives to be included in the report.
OneDrive Files and Folders with No Access Links	Shows the files and folder that have no access links for the selected drives. Contains parameters to select the tenants and drives to be included in the report.
OneDrive Quotas	Shows the quota information for the selected tenants and drives. Contains parameters to select the tenants and drives to be included in the report. Contains a parameter to select the drives to be excluded from the report.
OneDrive Quotas for Department	Shows the quota information for the selected departments and tenants. Contains parameters to select the tenants and departments to be included in the report.
OneDrive Summary	Shows a summary of OneDrive for the selected Microsoft 365 tenants.
OneDrive Users	Shows all Microsoft 365 users using OneDrive for the selected tenants. Contains parameters to select the tenants to be included in the report.
OneDrive | Permissions	
OneDrive File and Folder Access Link Permissions	Shows the access link permissions for the selected files and folders. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.
OneDrive File and Folder Owner Permissions	Shows owner permissions for files and folders on the selected tenants. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.
OneDrive File and Folder Permissions	Shows owner permissions for all files and folders on the selected tenants and drives. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.
OneDrive File and Folder Permissions for Identity	Shows file and folder permissions, including permissions derived through group membership, for the selected paths and selected identity. Contains parameters to select the identity and its group members, tenants and drives to be included in the report.
OneDrive File and Folder Permissions that are Different	Shows permissions that are different from parent folder permissions on the selected tenants and drives. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report.
OneDrive File and Folder Permissions with Membership	Shows the permissions for all files and folders on the selected tenants and drives. If you choose to include nested groups, membership of the groups is displayed. Contains parameters to select the tenants, drives, and folders and files to be included in the report. Contains a parameter to select the folders and files to be excluded from the report. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
SharePoint Online	
SharePoint Online Access Control Settings	Shows the access control settings for the selected tenants. Contains a parameter to select the tenants to be included in the report.

Table 13. Microsoft 365 Reports

Report Name	Description
SharePoint Online Configuration Settings	Shows the configuration settings for the selected tenants. Contains a parameter to select the tenants to be included in the report.
SharePoint Online Microsoft 365 Group Sites	Shows all Microsoft 365 group sites for the selected SharePoint Online Tenants. Contains parameters to select the tenants and sites to be included in the report.
SharePoint Online Permissions for Identity	Shows the SharePoint Online permissions for the selected identity in the selected tenants and sites. Contains parameters to select the identity, tenants, sites, and roles to be included in the report.
SharePoint Online Sharing Policies	Shows the sharing policies for the selected tenants. Contains parameters to select the tenants to be included in the report.
SharePoint Online Site Administrators	Shows all site administrators for the selected SharePoint Online Tenants and sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Site Group Information with Members	Shows all site groups and their members for the selected SharePoint Online Tenants and sites. Contains parameters to select the tenants, site collections, sites, and site groups to be included in the report.
SharePoint Online Site Sharing	Shows the sharing settings for the selected tenants and sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Site Permissions	Shows the site permissions for the selected tenants and sites. Contains parameters to select the tenants, site collections, sites, and roles to be included in the report.
SharePoint Online Sites without an Microsoft 365 Group	Shows all sites without an Microsoft 365 group for the selected tenants. The report will not include subsites for the sites. Contains parameters to select the tenants, site collections, and sites to be included in the report.
SharePoint Online Summary	Shows a summary of SharePoint Online for the selected Microsoft 365 tenants. Contains a parameter to select the tenants to be included in the report.

NTFS Reports

The following table outlines the NTFS reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports. For each report, you must include at least one computer, and one path on that computer. Once you have included a path, you can exclude part of the path.

TIP: If you include many or all computers or paths, the amount of data processed for your reports can result in a longer report generation time and lengthy reports. You may find it helpful to create several smaller reports.

Wildcard usage: You can use wildcards when specifying computers, paths and owners. Use an asterisk (*) for multiple characters, or a question mark (?) for a single character.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 14. NTFS Reports

Report Name	Description
File and Folder Summary	Shows the total number of files and folders collected per computer. Contains a parameter to select the computers to be included in the report.
NTFS Object Attributes	Shows the general file and folder information for the selected computers and paths. This report combines the General File Information and General Folder Information reports for your convenience. Contains parameters to select the computers, paths, and owners to be included in the report. Contains a parameter to select the paths to be excluded from the report.
Files	
Compressed Files	Shows compressed files on the selected computers. Contains a parameter to select the computers to be included in the report.
Duplicate File Details	Shows duplicate files on the selected computers. Contains a parameter to select the computers to be included in the report.
Extended File Information	Shows the extended file information (including the file owner) for the selected computers and paths. Contains parameters to select the computers, folders, and file extensions to be included in the report.
File Details	Shows file details for the selected computers and paths. Contains parameters to select the computers, folders, and files to be included in the report.
File Information by Extension	Shows files on the selected computers grouped by file extension. Contains parameters to select the computers, folders and file extensions to be included in the report.
Files Created in Last (N) Days	Shows all files created in last (N) days for the selected computers grouped by date created. Contains parameters to select the computers, number of days, folders, and file extensions to be included in the report.
Files Created in Last (N) Days grouped by Parent Path	Shows all files created in last (N) days for the selected computers grouped by parent path. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Created within Date Range	Shows all files created within the specified date range for the selected computers grouped by date created. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.
Files Created within Date Range grouped by Parent Path	Shows all files last accessed in last (N) days for the selected computers grouped by date last accessed. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.
Files Larger than a Specific Size	Shows all files for the selected computers that are larger than a specific size grouped by parent path. Contains parameters to select the computers, file size, folders, and extensions to be included in the report.
Files Last Accessed in Last (N) Days	Shows all files last accessed in the last (N) days for the selected computers grouped by date last accessed. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Last Accessed in Last (N) Days grouped by Parent Path	Shows all files last accessed in last (N) days for the selected computers grouped by parent path. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Last Accessed within Date Range	Shows all files last accessed within the specified date range for the selected computers grouped by date last accessed. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.

Table 14. NTFS Reports

Report Name	Description
Files Last Accessed within Date Range grouped by Parent Path	Shows all files last accessed within the specified date range for the selected computers grouped by parent path. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.
Files Modified in Last (N) Days	Shows all files modified in last (N) days for the selected computers grouped by date modified. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Modified in Last (N) Days grouped by Parent Path	Shows all files modified in last (N) days for the selected computers grouped by parent path. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Modified within Date Range	Shows all files modified within the specified date range for the selected computers grouped by date modified. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.
Files Modified within Date Range grouped by Parent Path	Shows all files modified within the specified date range for the selected computers grouped by parent path. Contains parameters to select the computers, date range, folders, and file extensions to be included in the report.
Files Older Than (N) Days	Shows files that have not been accessed in a selected period on the selected computers. Contains parameters to select computers, number of days, folders, and file extensions to be included in the report.
Files Older Than a Year	Shows files that have not been accessed in a year on the selected computers. Contains parameters to select computers, folders, and file extensions to be included in the report.
Files with Long Paths	Shows details for files with a path greater than 255 characters. Contains a parameter to select the computers to be included in the report.
General File Information	Shows general file information for the selected computers and paths — including the file attributes, date and time information, path, and size. Contains parameters to select computers, folders, and file extensions to be included in the report.
General File Information by Folder Depth	Shows the general file information filtered by folder depth. Contains parameters to select the computers, folder depth, folders, and file extensions to be included in the report. The starting folder level and subsequent depth are determined by the collection options and how the paths are stored. Your Administrator may be collecting files and folders through the administrative share or a network share. You can choose the level of folder depth to include. The folder level value will start from zero. Examining the path of C:\FolderA\FolderB, C:\ is 0 levels deep. FolderA is 1 level deep. FolderB is 2 levels deep.
Orphaned Files	Shows files on the selected computers with unknown ownership. Contains a parameter to select the computers to be included in the report.
Folders	
Aggregate Folder Size	Shows the aggregate folder size for the computers and included paths. Contains parameters to select the domains, computers and paths to be included in the report. Contains a parameter to select the paths to be excluded from the report.

Table 14. NTFS Reports

Report Name	Description
Extended Folder Information	In addition to the general folder information, shows the folder owner for the selected computers and paths. Contains parameters to select the computers and paths to be included in the report. Contains a parameter to select the paths to be excluded from the report.
Folder Information with Number of Files	Shows folders for the selected computers with a file count for each folder. Contains parameters to select the computers and paths to be included in the report. Contains a parameter to select the paths to be excluded from the report.
Folders Created in Last (N) Days	Shows all folders created in last (N) days for the selected computers grouped by date created. Contains parameters to select the computers and the number of days to be included in the report.
Folders Created in Last (N) Days grouped by Parent Path	Shows all folders created in last (N) days for the selected computers grouped by parent path. Contains parameters to select the computers and the number of days to be included in the report.
Folders Created within Date Range	Shows all folders created within the specified date range for the selected computers grouped by date created. Contains parameters to select the computers and the date range to be included in the report.
Folders Created within Date Range grouped by Parent Path	Shows all folders created within the specified date range for the selected computers grouped by parent path. Contains parameters to select the computers and the date range to be included in the report.
Folders Modified in Last (N) Days	Shows all folders modified in last (N) days for the selected computers grouped by date modified. Contains parameters to select the computers and the number of days to be included in the report.
Folders Modified in Last (N) Days grouped by Parent Path	Shows all folders modified in last (N) days for the selected computers grouped by parent path. Contains parameters to select the computers and the number of days to be included in the report.
Folders Modified within Date Range	Shows all folders modified within the specified date range for the selected computers grouped by date modified. Contains parameters to select the computers and the date range to be included in the report.
Folders Modified within Date Range grouped by Parent Path	Shows all folders modified within the specified date range for the selected computers grouped by parent path. Contains parameters to select the computers and the date range to be included in the report.
General Folder Information	Shows general folder information for the selected computers and paths — including the folder attributes, date and time information, path, and size. Contains parameters to select the computers and paths to be included in the report. Contains a parameter to select the paths to be excluded from the report.
General Folder Information by Folder Depth	Shows the general folder information filtered by folder depth. Contains parameters to select the computers, paths, and folder depth to be included in the report. Contains a parameter to select the paths to be excluded from the report. The starting folder level and subsequent depth are determined by the collection options and how the paths are stored. Your Administrator may be collecting folders through the administrative share or a network share. You can choose the level of folder depth to include. The folder level value will start from zero. Examining the path of C:\FolderA\FolderB, C:\ is 0 levels deep. FolderA is 1 level deep. FolderB is 2 levels deep.
General Folder Information grouped by Parent Path	Shows the general folder information for the selected computers grouped by parent path. Contains a parameter to select the computers to be included in the report.

Table 14. NTFS Reports

Report Name	Description
General Folder Information grouped by Size	Shows the general folder information for the selected computers grouped by size. Contains a parameter to select the computers to be included in the report.
Permissions	
File and Folder Permissions Differences with Membership	Shows the parent and child permission differences between the selected files and folders. Contains parameters to select the computers, paths, and permission differences to be included in this report. Contains a parameter to include nested group memberships and options on how they are displayed in the report. Also contains an option to include folders only.
File and Folder Permissions with Differences	Shows the parent and child permission differences between the selected files and folders. Contains parameters to select the computers, paths, and permission differences to be included in this report. Also contains options to include folders only or only files and folders with permissions that differ from the parent.
File Permissions	Shows the list of ACEs in the DACL for all files on the selected computers and paths. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both. You can filter the results by supplying a specific list of accounts to look for in the DACLs, and specific organizational units.
File Permissions for Account	Shows file permissions for the selected account, including permissions derived through group membership. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both.
File Permissions with Membership	Shows the list of ACEs in the DACL for all files on the selected computers and paths, including the first level of group members for any group given permissions. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both. Contains a parameter to include nested group memberships and options on how they are displayed in the report. For more information, see Searching for Parameter Values on page 80. Technical Documentation. You can filter on specific groups.
Files by Owner	Shows all files for the selected computers and owners.
Files or Folders with Permissions that Contain Deleted Accounts	Shows the permissions of the files or folders that contain deleted accounts. Contains parameters to select the computers, paths, and permissions to be included in the report. Contains a hidden parameter that includes deleted accounts.
Folder Permissions	Shows the list of ACEs in the DACL for all folders on the selected computers and paths. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both. You can filter the results by supplying a specific list of accounts to look for in the DACLs, and specific organizational units.
Folder Permissions for Account	Shows folder permissions for the selected account, including permissions derived through group membership. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both.

Table 14. NTFS Reports

Report Name	Description
Folder Permissions with Membership	Shows the list of ACEs in the DACL for all folders on the selected computers and paths, including the first level of group members for any group given permissions. You can choose to show only permissions inherited from a parent, only explicit permissions or to show both. You can filter the results by supplying a specific list of accounts to look for in the DACLs. You can choose whether or not you want to include the members of the Domain Users group. Since this can be a very large group, you may wish to exclude it. If you have included the Domain Users group, this report can take longer to generate. Contains a parameter to include nested group memberships and options on how they are displayed in the report. For more information, see Searching for Parameter Values on page 80. Technical Documentation. You can filter on specific groups.
Folders by Owner	Shows all folders for the selected computers and owners.
Groups with No Permissions on Any Computer	Shows groups that do not have permissions, or permissions derived through group membership, for any of the files or folders on any of the selected computers. If the selected computers are in more than one domain, all groups from those domains will be verified. If a group has permissions on any of the selected computers, that group will be excluded from the report. When there are 2 (or more) computers from the same domain (for example, Computer A and Computer B), all groups in their domain are analyzed and the results will be as follows: If a group has permission on Computer A but not on Computer B, it will not be in the report. If a group does not have permission on either Computer B or on Computer A, it will not be in the report. If a group does not have permission on either Computer A or on Computer B, it will be in the report.
Groups with No Permissions on Files or Folders	Shows groups that do not have permissions, or permissions derived through group membership, for any of the files or folders on the selected computers. If the selected computers are in more than one domain, all groups from the domains will be verified. If a group does not have any permissions on more than one of the selected computers, that group will be shown under each of those computers.
User Permissions on Folders	Shows the user permissions on the selected folders including permissions derived through group membership.

Registry Reports

The following table outlines the Registry reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Table 15. Registry Reports

Report Name	Description
Registry Keys and Values	Shows the registry keys and their associated values for selected computers. Contains parameters to select the domains, computers, and keys to be included in the report.
Registry Permissions	Shows all registry permissions for the selected computers. Contains parameters to select the domains, computers, keys, and accounts to be included in the report.

Security Explorer Remediation Reports

The following table outlines the Security Explorer Remediation reports included in the Report Library. If you are a report user, your administrator may have made some of these reports available in Published Reports.

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

NOTE: Security Explorer must be installed on the same computer as the Report Manager.

Table 16. Security Explorer Remediation Reports

Report Name	Description
Active Directory	
Active Directory Permissions for Account with Actions	Shows the Active Directory permissions for an account, including permissions derived through group membership. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select the domains, organizational units, object types, and permissions to be included in the report. You can choose to show only permissions inherited from a parent, only explicit permissions, or to show both.
Active Directory Permissions for Account with Membership and Actions	Shows the Active Directory permissions for an account, including permissions derived through group membership. If you choose to include nested groups, membership of the groups is displayed. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select the domains, organizational units, object types, and objects to be included in the report. You can choose to show only permissions inherited from a parent, only explicit permissions, or to show both. Also contains a parameter to include nested group memberships and options for how they are displayed in the report.
Active Directory Permissions with Actions	Shows all Active Directory permissions for the selected domains and Active Directory objects. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select the domains, organizational units, object types, objects, and accounts to be included in the report. You can choose to show only permissions inherited from a parent, only explicit permissions, or to show both.

Table 16. Security Explorer Remediation Reports

Report Name	Description
Domain Groups and Members with Actions	Shows group memberships for the selected domains and groups. If you choose to include nested groups, membership of the groups is displayed. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, organizational units, and domain groups. Also contains a parameter to include nested group memberships and options on how they are displayed in the report.
Domain Groups with Probable Owner with Actions	Shows the domain groups with members for the selected domains and suggests the account that manages the highest percentage of members as the probable group owner. Click any link in the report to open Security Explorer and manage the group's membership and properties. Contains a parameter to select the domains to be included in the report.
Domain Users with Actions	Shows domain users for the selected domains. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, organizational units, and accounts. Also contains options to include only disabled or locked domain user accounts.
Group Managed Service Accounts and Members with Actions	Shows all the managed service accounts and their members for the selected domains. Contains parameters to select the domains, organizational units, and managed service accounts to be included in the report.
Managed Service Accounts and Members with Actions	Shows all the managed service accounts and their members for the selected domains. If you choose to include nested groups, membership of the group members is displayed. Contains parameters to select the domains, organizational units, and group managed accounts to be included in the report.
Computer	
Local Groups and Members with Actions	Shows the group memberships for the selected computers and groups. If you choose to include nested groups, membership of the groups is displayed. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, computers, and local groups. Also contains a parameter to include nested group memberships and options on how they are displayed in the report.
Local Users with Actions	Shows local users for the selected computers. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select the domains, computers, accounts, and the status of accounts. If you want to report on all included users regardless of their account status (locked/unlocked, disabled/enabled), choose No value specified.
Printer Permissions with Actions	Shows printer permissions for the selected computers and printers. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, computers, printers, and accounts.
Service Permissions with Actions	Shows service permissions for the selected computers and services. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, computers, services, and accounts.
Share Permissions with Actions	Shows share permissions for the selected computers and shares. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, computers, shares, type of shares, and accounts.
Exchange	

Table 16. Security Explorer Remediation Reports

Report Name	Description
Mailbox Permissions with Actions	Shows mailbox permissions for the selected servers. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select organizations, servers, mailbox stores, mailboxes, and types of permissions to be included in the report. Contains a hidden parameter to include, by default, only Exchange servers running the Mailbox server role.
Public Folder Permissions with Actions	Shows folder permissions for the selected servers and public folders. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select organizations, servers, public folders, accounts, and types of permissions to be included in the report. Also includes the options to exclude specific public folders and to filter inherited or explicit permissions. Contains hidden parameters to include, by default, only Exchange servers running the Mailbox server role, and to exclude, by default, system public folder information.
Microsoft SQL Server	
SQL Database Object Permissions with Actions	Shows SQL database objects and their permissions. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select SQL servers, instances, and databases. Also contains parameters to select object types, permission types, and object permissions.
SQL Database Schema Permissions with Actions	Shows database schemata and their assigned permissions in the database. Click any link in the report to open Security Explorer and manage the object's permissions.Contains parameters to select SQL servers, instances, databases, and object permissions.
NTFS	
File Permissions with Actions	Shows file permissions for the selected computers and paths. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select computers, paths, accounts, and organizational units. Also contains options to show only permissions inherited from a parent, only explicit permissions, or both.
Files by Owner with Actions	Shows files for the selected computers and owners. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select computers and owners to be included in the report.
Folder Permissions with Actions	Shows folder permissions for the selected computers and paths. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select computers, paths, accounts, and organizational units. Also contains an option to show only permissions inherited from a parent, only explicit permissions, or both.
Folders by Owner with Actions	Shows folders for the selected computers and owners. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select computers and owners to be included in the report.
Registry	
Registry Permissions with Actions	Shows registry permissions for the selected computers. Click any link in the report to open Security Explorer and manage the object's permissions. Contains parameters to select domains, computers, keys, and accounts to be included in the report.

Report Types Included in Enterprise Reporter

The report types included in Enterprise Reporter are used to determine what fields can be included in each report. A report can only contain fields from one report type. For more information on editing existing reports, see Editing Reports on page 107. For more information on creating new reports, see Creating New Reports on page 122.

The following tables outline each category of report types included in Enterprise Reporter Report Manager.

See also:

- Active Directory Report Types
- Microsoft Entra Report Types
- Azure Resource Report Types
- Common Objects Report Types
- Computer Report Types
- Exchange Report Types
- Exchange Online Report Types
- File Storage Analysis Report Types
- Microsoft Teams Report Types
- NTFS Report Types
- OneDrive Report Types
- Registry Report Types
- SQL Server Report Types
- SharePoint Online Report Types

Active Directory Report Types

Table 17. Active Directory Report Types

Report Type	Description
Account Membership	Provides information on domain accounts and the groups of which they are a member. Contains fields for the domain group member as well as its related domain and organizational unit.
Accounts	Provides information on accounts in an Active Directory domain. Contains fields for the domain account as well as its related domain and organizational unit. Domain accounts can be users and groups.
Change History	Provides a list of changes made over time to all objects collected in an Active Directory domain. Contains fields for the domain, domain change history, and change history details.
Computers	Provides information on computers in an Active Directory domain. Contains fields for the domain computer as well as its related domain and organizational unit. Contains only information retrieved from Active Directory. For physical computer fields, please select the Computer | Computer report type.
Contacts	Provides information on contacts in an Active Directory domain. Contains fields for the domain contact as well as its related domain and organizational unit.

Table 17. Active Directory Report Types

Report Type	Description
Deleted Objects	Provides information on objects in the Deleted Objects Container in an Active Directory domain. Contains fields for the deleted object as well as its related domain.
Domain Controllers	Provides information on domain controllers in an Active Directory domain. Contains fields for the domain controller as well as its related domain and organizational unit.
Domain Group Membership Change History	Provides information on group membership changes in a domain. Contains fields for Domain, Domain Group, Domain OU, and Common Change History.
Domains	Provides information on an Active Directory domain.
Group Members	Provides information on domain groups and their members. Contains fields for the domain group, its related domain and organizational unit as well as the member accounts. Domain user and domain group fields are available for the member account as well as an option to expand the membership.
Groups	Provides information on groups in an Active Directory domain. Contains fields for the domain group as well as its related domain and organizational unit.
Object Permissions	Provides permission information on Active Directory objects. Contains fields for the domain object, the permission, the permissioned account as well as its related domain and organizational unit. Domain user and domain group fields are available for the permissioned account.
Organizational Units	Provides information on organizational units in an Active Directory domain. Contains field for the domain object and the domain organizational unit.
Published Printers	Provides information on printers published in an Active Directory domain. Contains fields for the printer as well as its related domain and organizational unit.
Published Shares	Provides information on shares published in an Active Directory domain. Contains fields for the share as well as its related domain and organizational unit.
Service Account Members	Provides information on service accounts and their members in an Active Directory domain. Contains fields for the domain service account, it's related domain and organizational unit as well as the related member accounts.
Service Accounts	Provides information on service accounts in an Active Directory domain. Contains fields for the domain service account as well as its related domain service account members that have the permission to retrieve password.
Sites	Provides information on sites in an Active Directory domain. Contains fields for the domain site and its related domain.
Trusts	Provides information on trusts in an Active Directory domain. Contains fields for the domain trust and its related domain.
Users	Provides information on users in an Active Directory domain. Contains fields for the user as well as its related domain and organizational unit.

Microsoft Entra Report Types

The following table outlines the report types that are available for Microsoft Entra reports. Many of these report types can be extended to include additional fields. When editing a report, in the Available Fields area, the option to extend the report type is indicated by a special folder icon next to object names underlined in blue. You can right click the object names to see the available type of account objects that can be added. For detailed steps on extending the report type, see To extend a report type on page 110.

Table 18. Microsoft Entra Report Types

Report Type	Description
Microsoft Entra Application Permissions	Provides information on Microsoft Entra Tenant Application Permissions. Contains fields for Microsoft Entra Tenant, Microsoft Entra Application, Microsoft Entra Application Permission, and Microsoft EntraIdentity.
Microsoft Entra Application Service Principals	Provides information on Microsoft Entra Tenant Applications' Service Principals. Contains fields for Microsoft Entra Tenant, Microsoft Entra Application, and Microsoft Entra Service Principal.
Microsoft Entra Applications	Provides information on Microsoft Entra Tenant Applications. Contains fields for Microsoft Entra Tenant and Microsoft Entra Applications.
Microsoft Entra Contacts	Provides information on Microsoft Entra tenant contacts. Contains fields for Microsoft Entra Tenant and Microsoft Entra Contact.
Microsoft Entra Device Members	Provides information on Microsoft Entra tenant device members. Contains fields for Microsoft Entra Tenant, Microsoft Entra Device, and Microsoft Entra Device Member.
Microsoft Entra Devices	Provides information on Microsoft Entra tenant devices. Contains fields for Microsoft Entra Tenant and Microsoft Entra Device.
Microsoft Entra Domains	Provides information on Microsoft Entra tenant domains. Contains fields for Microsoft Entra Tenant and Microsoft Entra Domain.
Microsoft Entra Group Members	Provides information on Microsoft Entra tenant group members. Contains fields for Microsoft Entra Tenant, Microsoft Entra Group, and Microsoft Entra Group Member.
Microsoft Entra Groups	Provides information on Microsoft Entra tenant groups. Contains fields for Microsoft Entra Tenant and Microsoft Entra Group.
Microsoft Entra Identities	Provides information on Microsoft Entra tenant identities. Contains fields for Microsoft Entra Tenant and Microsoft Entra Identity.
Microsoft Entra Identity Membership	Provides information on Microsoft Entra tenant identity membership. Contains fields for Microsoft Entra Tenant, Microsoft Entra Identity, and Microsoft Entra Group.
Microsoft Entra Identity Roles	Provides information on Microsoft Entra tenant identity roles. Contains fields for Microsoft Entra Tenant, Microsoft Entra Identity, and Microsoft Entra Role.
Microsoft Entra Risky Users	Provides information on risky users in Microsoft Entra ID. Contains fields for Microsoft Entra Tenant, Microsoft Entra Risky User, and Microsoft Entra User.
Microsoft Entra Roles	Provides information on Microsoft Entra tenant roles. Contains fields for Microsoft Entra Tenant, Microsoft Entra Role, and Microsoft Entra Role Member.
Microsoft Entra Service Plan Users	Provides information on Microsoft Entra tenant service plan users. Contains fields for Microsoft Entra Tenant, Microsoft Entra Subscription, Microsoft Entra Service Plan, and Microsoft Entra User.
Microsoft Entra Score Controls	Provides information on Microsoft Entra Secure Score. Contains fields for TenantId, Created Date Time, Current Score, and Max Score.
Microsoft Entra Secure Score	Provides information on Microsoft Entra Secure Score. Contains fields for Identity Secure Score Id, Action Type, Action Url, Control Category, Deprecated, Implementation Cost, Last Modified DateTime, Current Control Score, Max Control Score, Rank, Remediation, Remediation Impact, Service, Tier, Title, and UserImpact.
Microsoft Entra Service Principal Members	Provides information on Microsoft Entra tenant service principal members. Contains fields for Microsoft Entra Tenant, Microsoft Entra Service Principal, and Microsoft Entra Service Principal Member.

Table 18. Microsoft Entra Report Types

Report Type	Description
Microsoft Entra Service Principals	Provides information on Microsoft Entra tenant service principals. Contains fields for Microsoft Entra Tenant and Microsoft Entra Service Principal.
Microsoft Entra Tenant Service Plans	Provides information on Microsoft Entra tenant service plans. Contains fields for Microsoft Entra Tenant, Microsoft Entra Subscription, and Microsoft Entra Service Plan.
Microsoft Entra Tenant Subscriptions	Provides information on Microsoft Entra tenant subscriptions. Contains fields for Microsoft Entra Tenant and Microsoft Entra Subscription.
Microsoft Entra Tenants	Provides information on Microsoft Entra tenants. Contains fields for Microsoft Entra Tenant and for Microsoft Entra ID and on-premises Password Protection settings.
Microsoft Entra User Subscriptions	Provides information on Microsoft Entra tenant user subscriptions. Contains fields for Microsoft Entra Tenant, Microsoft Entra User, Microsoft Entra Service Plan, the Microsoft Entra Subscription.
Microsoft Entra Users	Provides information on Microsoft Entra tenant users. Contains fields for Microsoft Entra Tenant and Microsoft Entra User.

Azure Resource Report Types

The following table outlines the report types that are available for Azure reports. Many of these report types can be extended to include additional fields. When editing a report, in the Available Fields area, the option to extend the report type is indicated by a special folder icon next to object names underlined in blue. You can right click the object names to see the available type of account objects that can be added. For detailed steps on extending the report type, see To extend a report type on page 110.

Table 19. Azure Resource Report Types

Report Type	Description
Azure Classic Disk Resource	Provides information on Azure Classic Disk Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, and Azure Resource Classic Disk.
Azure Classic Network Security Group	Provides information on Azure Classic Network Security Group Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Classic Network Security Group, and Azure Resource Network Security Group Security Rule.
Azure Classic Storage Account Resource	Provides information on Azure Classic Storage Account Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, and Azure Resource Classic Storage Account.
Azure Classic Virtual Machine Drives	Provides information on drives connected to Azure Classic Virtual Machine Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Classic Virtual Machine, and Azure Classic Virtual Machine Drives.
Azure Classic Virtual Machine Networking Resource	Provides information on Azure Classic Virtual Machine Networking Resources. Contains fields for Azure Resource Subscription, Azure Resource Group, Azure Resource Classic Virtual Machine, Azure Resource Classic Network Security Group, and Azure Resource Classic Virtual Network.
Azure Classic Virtual Machine Resource	Provides information on Azure Classic Virtual Machine Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, and Azure Resource Classic Virtual Machine.

Table 19. Azure Resource Report Types

Report Type	Description
Azure Classic Virtual Network Resource	Provides information on Azure Classic Virtual Network Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Classic Virtual Network, and Azure Resource Classic Subnet.
Azure Disk Resource	Provides information on Azure Disk Resources. Contains fields for Azure Resource Subscriptions, Azure Resource Resource Groups, and Azure Resource Disk.
Azure IP Address	Provides information on Azure Network Interface Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Groups, Azure Resource IP Address.
Azure IP Configuration	Provides information on Azure IP Configuration. Contains fields for Azure Resource Subscription, Azure Resource Resource Groups, Azure Resource IP Configuration, Azure Resource IP Address, and Azure Resource Subnet.
Azure Network Interface	Provides information on Azure Network Interface Resources. Contains fields for Azure Resource Subscription, Azure Resource Groups, Azure Resource Network Interface, and Azure Resource IP Configuration.
Azure Network Interface Resource	Provides information on Azure Network Interface Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Network Interface, Azure Resource Network Security Group, Azure Resource IP Configuration, Azure Resource Public IP Address, Azure Resource Subnet, Azure Resource Virtual Network.
Azure Network Security Group Resource	Provides information on Azure Network Security Group Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Network Security Group, Azure Resource Network Security Group Security Role.
Azure Resource Access Control	Provides information on Azure Resource access control. Contains fields for Azure Resource Subscription, Azure Resource Group, Azure Resource, and Azure Resource Role Assignment.
Azure Resource Groups	Provides information on Azure Resource Groups. Contains fields for Azure Resource Subscription.
Azure Resource Resource Group Access Control	Provides information on Azure Resource Group access control. Contains fields for Azure Resource Subscription, Azure Resource Group, and Azure Resource Role Assignment.
Azure Resource Subscription Access Control	Provides information on Azure Resource Subscription access control. Contains fields for Azure Resource Subscription, and Azure Resource Resource Role Assignment.
Azure Resource Subscriptions	Provides information on Azure Resource Subscriptions.
Azure Resources	Provides information on Azure resources. Contains fields for Azure Resource Subscription, and Azure Resource Group Group.
Azure Storage Account Resources	Provides information on Azure Storage Account Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group,and Azure Resource Storage Account.
Azure Subnet	Provides information on Azure Subnet. Contains fields for Azure Resource Subscription, Azure Resource Groups, and Azure Resource Subnet.
Azure Virtual Machine Networking Resources	Provides information on Azure Virtual Machine Networking Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Virtual Machine, Azure Resource Network Interface, Azure Resource Network Security Group, Azure Resource IP Configuration, Azure Resource Public IP Address Azure Resource Subnet, and Azure Resource Virtual Network.

Table 19. Azure Resource Report Types

Report Type	Description
Azure Virtual Machine Resource	Provides information on Azure Virtual Machines. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, and Azure Resource Virtual Machine.
Azure Virtual Network	Provides information on Azure Virtual Network Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Groups, Azure Resources Virtual Network, and Azure Resource Subnet.
Azure Virtual Network Resource	Provides information on Azure Virtual Network Resources. Contains fields for Azure Resource Subscription, Azure Resource Resource Group, Azure Resource Virtual Network, Azure Resource Subnet.

Common Objects Report Types

Table 20. Common Objects Report Types

Report Type	Description
Accounts	Provides information on accounts. Accounts can be users, groups, computers, or contacts.
Change History	Provides a list of changes made over time to group memberships.

Computer Report Types

Table 21. Computer Report Types

Report Type	Description
Account Membership	Provides information on computer accounts and the groups of which they are a member. Contains fields for the computer group member and its related computer and group.
Addresses	Provides information on computer IP addresses. Contains fields for the IP address and its related computer.
Advanced Auditing	Provides information on computer advanced audit policy configuration settings. Contains fields for the policy and its related computer. Fields are organized into advanced audit policy categories for simpler selection. When Advanced Audit Policy Configuration settings are being used the "Force audit policy subcategory settings to override audit policy category settings" policy setting must be enabled, this field is available in Security Options Audit.
All Installed Software	Provides information on all the installed software on a computer (including Microsoft Store applications). Contains fields for the installed software and its related computer.
Change History	Provides a list of changes made over time to all computer objects collected. Contains fields for the change history and its related computer.
Computer	Provides information on physical computers.
DNS Zones	Provides information on DNS zones for a computer. Contains fields for the DNS zone and its related computer.
Event Logs	Provides information on event logs for a computer. Contains fields for the event log configuration and its related computer.
Hotfixes	Provides information on hotfixes on a computer. Contains fields for the hotfix and its related computer.

Table 21. Computer Report Types

Report Type	Description
Installed Software	Provides information on the installed software on a computer. Contains fields for the installed software and its related computer.
Local Group Members	Provides information on local groups and their members. Contains fields for the local group, its related computer and the group member as well as an option to expand group membership.
Local Groups	Provides information on local groups on a computer. Contains fields for the local group and its related computer.
Local Users	Provides information on local users on a computer. Contains fields for the local user and its related computer.
Microsoft Store Applications	Provides information on the Microsoft Store applications on a computer. Contains fields for the Microsoft Store application and its related computer.
Network Configuration	Provides information on the network configuration of a computer. Contains fields for the network adapter as well as its related network protocol and computer.
Printer Permissions	Provides permission information on computer printers. Contains fields for the computer, the printer, the permission, the owner, and the permissioned account.
Printers	Provides information on printers on a computer. Contains fields for the printer and its related computer.
Profile Information	Provides user profile information on a computer. Contains fields for the profile and its related computer.
Security Options	Provides information on security options on a computer. Contains fields for each security option and its related computer. Fields are organized into security option categories for simpler selection.
Security Policies	Provides information on computer security policies including audit, lockout and password policies. Contains fields for the security policy and its related computer.
Service Permissions	Provides permission information on computer services. Contains fields for the computer, the service, the permission, the owner, and the permissioned account.
Services	Provides information on services on a computer. Contains fields for the service as well as its related service account and computer.
Service with Dependencies	Provides information on services on a computer including the service dependencies. Contains fields for the service as well as its related service dependencies, service account and computer.
Share Permissions	Provides permission information on shares on a computer. Contains fields for the computer, the share, the permission, the owner, and the permissioned account. Domain user, domain group, local user and local group fields are available for the permissioned account including organizational unit. **Note:** Domain user and domain group information only available if an Active Directory® collection has been completed.
Share Permissions with Nested Accounts	Provides permission information on shares on a computer. Contains fields for the computer, the share, the permission, the owner, and the permissioned account as well as an option to expand the accounts membership.
Shares	Provides information on shares on a computer. Contains fields for the share and its related computer.

Table 21. Computer Report Types

Report Type	Description
User Rights	Provides information on user rights on a computer including the accounts assigned user rights. Contains fields for the user right as well as its related assigned accounts and computer.
Volumes	Provides information on the volumes on a computer. Contains fields for the volume and its related computer.

Exchange Report Types

Table 22. Exchange Report Types

Report Type	Description
Distribution Group Members	Provides detailed information for Distribution Group Members. Contains fields for Exchange Organization, Distribution Group, and Distribution Group Member.
Distribution Groups	Provides detailed information for Distribution Groups. Contains fields for Exchange Organization and Distribution Group.
Mail Contacts	Provides detailed information for Mail Contacts. Contains fields for Exchange Organization and Mail Contact.
Mailbox Delegates	Provides detailed information on Mailbox Delegates. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Mailbox Account, and Mailbox Delegate.
Mailbox Folder Permissions	Provides detailed information for Mailbox Folder Permissions. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Account, Mailbox Folder, the permission, and the permissioned account.
Mailbox Folder Permissions with Nested Accounts	Provides detailed information for Mailbox Folder Permissions with Nested Accounts. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Mailbox Folder, the permission, the permissioned account, and an option to expand the account's membership.
Mailbox Folders	Provides detailed information for Mailbox Folders. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Mailbox Folder, and Account.
Mailbox Permissions	Provides detailed information for Mailbox Permissions. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Account, the permission, and the permissioned account.
Mailbox Permissions with Nested Accounts	Provides detailed information for Mailbox Permissions with Nested Accounts. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, Account, the permission, the permissioned account, and an option to expand the account's membership.
Mailbox Store Permissions	Provides detailed information for Mailbox Store Permissions. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, the permission, and the permissioned account.
Mailbox Store Permissions with Nested Accounts	Provides detailed information for Mailbox Store Permissions with Nested Accounts. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, the permission, the permissioned account, and an option to expand the account's membership.
Mailbox Stores	Provides detailed information for Mailbox Stores. Contains fields for Exchange Organization, Exchange Server, and Mailbox Store.
Mailboxes	Provides detailed information for Mailboxes. Contains fields for Exchange Organization, Exchange Server, Mailbox Store, Mailbox, and Account.

Table 22. Exchange Report Types

Report Type	Description
Mail-Enabled Users	Provides detailed information for Mail-Enabled Users. Contains fields for Exchange Organization and Mail-Enabled User.
Organization Permissions	Provides detailed information for Organization Permissions. Contains fields for Exchange Organization, the permission, and the permissioned account.
Organization Permissions with Nested Accounts	Provides detailed information for Organization Permissions with Nested Accounts. Contains fields for Exchange Organization, the permission, the permissioned account, and an option to expand the account's membership.
Public Folder Permissions	Provides detailed information for Public Folder Permissions. Contains fields for Exchange Organization, Exchange Server, Public Folder, Mailbox, Account, Public Folder Store, the permission, and the permissioned account.
Public Folder Permissions with Nested Accounts	Provides detailed information for Public Folder Permissions with Nested Accounts. Contains fields for Exchange Organization, Exchange Server, Public Folder, Mailbox, Account, Public Folder Store, the permission, the permissioned account, and an option to expand the account's membership.
Public Folders	Provides detailed information for Exchange Public Folders. Contains fields for the Exchange Organization, Exchange Server, Public Folder, Mailbox, Account, and Public Folder Store. **Note**: Public Folder Mailboxes and Public Folder Stores only exist for certain versions of Exchange.
Server Permissions	Provides detailed information for Exchange Server Permissions. Contains fields for Exchange Organization, Exchange Server, the permission, and the permissioned account.
Server Permissions with Nested Accounts	Provides detailed information for Exchange Server Permissions. Contains fields for Exchange Organization, Exchange Server, the permission, the permissioned account, and an option to expand the account's membership.
Servers	Provides detailed information for Exchange Servers. Contains fields for Exchange Organization and Exchange Server.

Exchange Online Report Types

Table 23. Exchange Online Report Types

Report Type	Description
Mail Contacts	Provides detailed information for Mail Contacts. Contains fields for Exchange Online Tenant and Mail Contact.
Mailbox Delegates	Provides detailed information on Mailbox Delegates. Contains fields for Exchange Online Tenant, Mailbox, and Mailbox Delegate.
Mailbox Folder Permissions	Provides detailed information for Mailbox Folder Permissions. Contains fields for Exchange Online Tenant, Mailbox, and Mailbox Folder.
Mailbox Folders	Provides detailed information for Mailbox Folders. Contains fields for Exchange Online Tenant, Mailbox, Mailbox Folder, and Account.
Mailbox Permissions	Provides detailed information for Mailbox Permissions. Contains fields for Exchange Online Tenant, Mailbox, the permission, and the permissioned identity.
Mailboxes	Provides detailed information for Mailboxes. Contains fields for Exchange Online Tenant and Mailbox.
Mail-Enabled Group Members	Provides detailed information for Mail-Enabled Group Members. Contains fields for Exchange Online Tenant, Mail-Enabled Group, and Mail-Enabled Group Member.

Table 23. Exchange Online Report Types

Report Type	Description
Mail-Enabled Groups	Provides detailed information for Mail-Enabled Groups. Contains fields for Exchange Online Tenant and Mail-Enabled Group.
Mail-Enabled Users	Provides detailed information for Mail-Enabled Users. Contains fields for Exchange Online Tenant and Mail-Enabled User.
Public Folder Permissions	Provides detailed information for Public Folder Permissions. Contains fields for Exchange Online Tenant, Public Folder, Mailbox, the permission, and the permissioned identity.
Public Folders	Provides detailed information for Exchange Public Folders. Contains fields for the Exchange Online Tenant, Public Folder, and Mailbox.

File Storage Analysis Report Types

Table 24. File Storage Analysis Report Types

Report Type	Description
File Category Details	Provides the most recent information on file distribution by category. Contains fields for the file category name, description, file count and size.
File Category History	Provides historical information on file distribution by category. Contains fields for the file category name, description, file count and size.
File Date Details	Provides the most recent information on file distribution by last access date. Contains fields for the server, file date details, volume detail, and file date.
File Date History	Provides historical information on file distribution by last access date. Contains fields for server, file date history, volume history, and file date.
File Extension Detail	Provides the most recent information on file distribution by file extension. Contains fields for the server, volume detail, file extension detail, and file extension.
File Extension History	Provides historical information on file distribution by file extension. Contains fields for the server, volume history, file extension history, and file extension.
File Size Details	Provides the most recent information on file distribution by size. Contains fields for the server, file size details, volume detail, and file size.
File Size History	Provides historical information on file distribution by size. Contains fields for the server, file size history, volume history, and file size.
Folder Category Details	Provides the most recent information on a folder category.Contains fields for the server, folder category details, volume detail, and lookup folder category.
Folder Category History	Provides historical information on a folder category. Contains fields for the server, folder category history, volume history, and lookup folder category.
Home Directory Details	Provides the most recent information on a server's home directories. Contains fields for the server, home directory details, account, and volume detail.
Home Directory History	Provides historical information on a server's home directories. Contains fields for the server, home directory history, account, and volume detail.
Owner Details	Provides the most recent information on file or folder owner. Contains fields for the server and owner details.
Owner History	Provides historical information on file or folder owner. Contains fields for the server and owner history.
Server Details	Provides the most recent information on a server. Contains fields for the server and server details.

Table 24. File Storage Analysis Report Types

Report Type	Description
Server History	Provides the historical information on a server. Contains fields for the server and server history.
Share Details	Provides the most recent information on a server's shares. Contains fields for the server and share details.
Share History	Provides historical information on a server's shares. Contains fields for the server and share history.
Volume Details	Provides the most recent information on a server's volumes. Contains fields for the server and volume details.
Volume History	Provides historical information on a server's volumes. Contains fields for the server and volume history.

Microsoft Teams Report Types

Table 25. Microsoft Teams Report Types

Report Type	Description
Teams and Settings	Provides information on Microsoft Teams and its settings. Contains fields for Teams Tenant and Teams Identity.
Teams App Permission Policies	Provides information on Microsoft Teams App Permission Policies. Contains fields for Teams Tenant and Teams App Permission Policies.
Teams Applications	Provides information on Microsoft Team Applications. Contains fields for Teams Tenant, Teams Identity, and Teams Application.
Teams Calling Policies	Provides information on Microsoft Teams Calling Policies. Contains fields for Teams Tenant and Teams Calling Policies.
Teams Channels	Provides information on Microsoft Team Channels. Contains fields for Teams Tenant, Teams, Teams Identity, and Teams Channel.
Teams Drive Items	Provides information on Microsoft Team Drive Items. Contains fields for Teams Tenant, Teams Identity, Teams Drive, Teams Drive Item, Created By, and Last Modified By.
Teams Meeting Policies	Provides information on Microsoft Teams Meeting Policies. Contains fields for Teams Tenant and Teams Meeting Policies.
Teams Members	Provides information on Microsoft Teams members. Contains fields for Teams Tenant, Teams Identity, and Teams Member.
Teams Messaging Policies	Provides information on Microsoft Teams Messaging Policies. Contains fields for Teams Tenant and Teams Messaging Policies.
Teams Organization Settings	Provides information on Microsoft Teams organization-wide settings. Contains fields for Teams Client, External Access, Guest Calling, Guest Meeting, and Guest Messaging settings.
Teams Tabs	Provides information on Microsoft Teams Tabs. Contains fields for Teams Tenant, Teams Identity, Teams Channel, and Teams Tab.
Teams Team and Channel Policies	Provides information on Microsoft Teams Team and Channel Policies. Contains fields for Teams Tenant and Teams Team and Channel Policies.
Teams User Policies	Provides information on Microsoft Teams User Policies. Contains fields for Teams Tenant, Teams User Identity, Teams Team and Channel Policies.

NTFS Report Types

Table 26. NTFS Report Types

Report Type	Description
Change History	Provides a list of changes made over time to files and folders collected. Contains fields for the computer, NTFS Change History, and Change Data.
Duplicate File Details	Provides the most recent information on duplicate files. Contains fields for the duplicate file and its related computer.
File and Folder Information	Provides information on files and folders on a computer. Contains fields for the file or folder and its related computer.
File and Folder Permission Differences	Provides parent and child permission differences on files and folders on a computer. Contains fields for the computer, the file or folder, the permission and the type of difference from the parent permission.
File and Folder Permission Differences with Nested Accounts	Provides parent and child permission differences on files and folders on a computer. Contains fields for the computer, the file or folder, the permission and the type of difference from the parent permission as well as an option to expand the account's membership.
File and Folder Permissions	Provides permission information on files and folders on a computer. Contains fields for the computer, the file or folder, the permission and the permissioned account. Domain user, domain group, local user and local group fields are available for the permissioned account including organizational unit. **Note:** Domain user and domain group information only available if an Active Directory® collection has been completed.
File and Folder Permissions with Nested Accounts	Provides permission information on files and folders on a computer. Contains fields for the computer, the file or folder, the permission and the permissioned account as well as an option to expand the accounts membership.
File Information	Provides information on files on a computer. Contains fields for the file and its related computer.
Folder Information	Provides information on folders on a computer. Contains fields for the folders and its related computer.
Folders with File Information	Provides detailed information on folders and optional files on a computer. Contains fields for the Computer, NTFS Share, NTFS Folder, and NTFS File.

OneDrive Report Types

The following table outlines the report types that are available for OneDrive reports. Many of these report types can be extended to include additional fields. When editing a report, in the Available Fields area, the option to extend the report type is indicated by a special folder icon next to object names underlined in blue. You can right click the object names to see the available type of account objects that can be added. For detailed steps on extending the report type, see To extend a report type on page 110.

Table 27. OneDrive Report Types

Report Type	Description
Configuration Settings	Provides configuration settings information for OneDrive. Contains fields for the tenant and settings.
Drive Information	Provides information on drives on OneDrive. Contains fields for the tenant, drive, and drive owner.

Table 27. OneDrive Report Types

Report Type	Description
Drive Permissions	Provides permission information on drives on OneDrive. Contains fields for the tenant, drive, permission, and permissioned identity set. User, device, and application fields are available for the permissioned identity set.
File and Folder Information	Provides information on files and folders on OneDrive. Contains fields for the tenant, drive, file or folder, and identity sets (Created By and Last Modified By). User, device, and application fields are available for the identity sets.
File and Folder Permissions	Provides permission information on files and folders on OneDrive. Contains fields for the tenant, drive, file or folder, permission, and permissioned identity set. User, device, and application fields are available for the permissioned identity set.
File and Folder Permissions Differences	Provides parent and child permission differences on files and folders on OneDrive. Contains fields for the tenant, drive, file or folder, permission, permissioned identity set, and if permissions differ from the parent permission.
File Information	Provides information on files on OneDrive. Contains fields for the tenant, drive, file and identity sets (Created By and Last Modified By). User, device, and application fields are available for the identity sets.
Folder Information	Provides information on folders on OneDrive. Contains fields for the tenant, drive, folder and identity sets (Created By and Last Modified By).User, device, and application fields are available for the identity sets.

Registry Report Types

Table 28. Registry Report Types

Report Type	Description
Change History	Provides a list of changes made over time to registry keys and values. Contains fields for Computer, Registry Change History, and Change Data.
Keys and Values	Provides information on registry keys and their values on a computer. Contains fields for the registry key as well as its value and related computer.
Permissions	Provides permission information on registry keys on a computer. Contains fields for the computer, the registry key, the permission and the permissioned account.

SharePoint Online Report Types

Table 29. SharePoint Online Report Types

Report Type	Description
SharePoint Online Configuration Settings	Provides information on SharePoint Online configuration settings. Contains fields for SharePoint Online Tenant and SharePoint Online Configuration Setting.
SharePoint Online Policies	Provides information on SharePoint Online Policies. Contains fields for SharePoint Online Tenant and SharePoint Online Policy.
SharePoint Online Settings and Policies.	Provides information on SharePoint Online Settings and Policies. Contains fields for SharePoint Online Tenant, SharePoint Online Configuration Settings, and SharePoint Online Tenant Policy.

Table 29. SharePoint Online Report Types

Report Type	Description
SharePoint Online Site Group Members	Provides information on SharePoint Online site group members. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Site Group, and SharePoint Online Site Group Member.
SharePoint Online Site Groups	Provides information on SharePoint Online site groups. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, and SharePoint Online Group.
SharePoint Online Site Permissions	Provides information on SharePoint Online site permissions. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Role Assignment Set, SharePoint Online Role Assignment, SharePoint Online Permission, and Azure Identity.
SharePoint Online Site Users and Azure Group Members	Provides information on SharePoint Online site administrators. Contains fields for the site and its related Azure Groups as well as the member accounts. Contains fields for the site user information at includes if the user is site administrator or if the user is primary admin. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, SharePoint Online Site, SharePoint Online Site User, Azure Identity, Azure Group, and Azure Group member.
SharePoint Online Sites	Provides information on SharePoint Online sites. Contains fields for SharePoint Online Tenant, SharePoint Online Site Collection, and SharePoint Online Site.

SQL Server Report Types

Table 30. SQL Server Report Types

Report Type	Description
Database	Provides information on databases on a SQL Server. Contains fields for the database and its related SQL Server.
Database Change History	Provides a list of changes made over time to databases collected.
Database Object	Provides information on database objects on a SQL Server. Contains fields for the database objects and its related database and SQL Server.
Database Object Permission	Provides permission information on database objects on a SQL Server. Contains fields for the SQL Server, the database, the database object, the permission, the grantor and the grantee.
Database Role	Provides information on database roles on a SQL Server. Contains fields for the role and its related SQL Server and database.
Database Role Membership	Provides information on databases roles and their members. Contains fields for the SQL Server, the database, the database role and the role members.
Database Role Membership by Account	Provides information on databases roles and their members. Contains fields for the role member name and membership path.
Database Schema	Provides information on database schemas on a SQL Server. Contains fields for the schema and its related SQL Server and database.
Database Schema Permission	Provides permission information on database schemas on a SQL Server. Contains fields for the SQL Server, the database, the database schema, the permission and the principal account.
Database User	Provides information on database users on a SQL Server. Contains fields for the SQL Server, the database, the user and the SQL Server Login. **Note:** Extended account information is only available if an Active Directory collection has been completed.

Table 30. SQL Server Report Types

Report Type	Description
Job	Provides information on server jobs on a SQL Server. Contains fields for the job and its related SQL Server.
Login	Provides information on SQL Logins on a SQL Server. Contains fields for the login, its related SQL Server, and the account. **Note:** Extended account information is only available if an Active Directory collection has been completed.
Permission for Database Objects	Provides permission information on database objects on a SQL Server. Contains fields for the SQL Server, the database object and the permission.
Permissions for SQL Server Instances	Provides permission information on SQL Server instance. Contains fields for the SQL Server, the permission, the grantor, and the grantee.
Role	Provides information on server roles on a SQL Server. Contains fields for the server role and its related SQL Server.
Role Membership	Provides information on SQL Server roles and their members. Contains fields for the SQL Server, the role and the members.
SQL Server	Provides information on a SQL Server.
SQL Server ACEs	Provides permission information on a SQL Server. Contains fields for the SQL Server the permission, the grantor and the grantee.
SQL Server Change History	Provides a list of changes made over time to SQL Servers collected.
SQL Server Role Membership by Account	Provides information on SQL Server roles and their members. Contains fields for the role member name and membership path.

Configuring Global Settings (System Configuration)

There are several global settings available on the System Configuration page that you can set to manage Enterprise Reporter.

Configure Logging

Each user of Report Manager can configure the amount of logging information that is collected from each Report Manager computer. Quest recommends using the default setting of Debug to collect as much information as possible. The following logging levels are available:

- **Debug**

  This is the most verbose logging level (maximum volume setting).

- **Information**

  The Information level is typically used to output information that is useful to the running of ER.

- **Warning**

  Warning is often used for showing when exceptional behavior has occurred. These can usually be handled without issue.

- **Error**

  Error is used to log all unexpected errors.

- **Fatal**

Fatal is reserved for special exceptions/conditions causing a failure of a component (console or server) with the ER product.

- **Off**

  This turns off logging completely. This setting is not recommended.

Credential Manager

There are many communication channels in Enterprise Reporter, involving different sets of credentials. You can manage credentials for use throughout the system using the Credential Manager. For more information, see Using the Credential Manager on page 98.

Database Settings

You can increase the timeouts for the Enterprise Reporter server. Connection Timeout controls how long the server has to establish a connection to the database, the Command Timeout controls the amount of time available for processing a command on the database, and the Report Command Timeout controls the amount of time allowed for report generation.

For more information, see Troubleshooting Connection Timeouts on page 136.

Email settings

If you are a reporting administrator, you can configure default settings for sending email. Setting default email settings makes it easier for reporting users to set up delivery of reports by email.

You can either configure a default SMTP server or, for OAuth2 authentication, you can configure Exchange Online. For Exchange Online, you must register an app for Enterprise Reporter in the Microsoft Entra Admin Center. For more information about default email settings, see Configuring a Default Email Server on page 86.

Logon Configuration

Enterprise Reporter can be configured to bypass the login screen. This eliminates the need to enter the server and port information.

To bypass the login screen

1. Open the System Configuration page.
2. Click **Manage bypass of the login screen**.
3. Optionally, enable **Show the login dialog at startup**.
4. Click **OK**.

Report Icon

Report administrators can configure a custom icon for report headers. There is an option for all new reports to use the icon automatically. Reports that have custom layouts may need to have their layout adjusted to accommodate the custom icon. For more information, see Changing the report icon on page 108.

Report Parameter Favourites

You can configure Enterprise Reporter to save your favorite parameter values within each report type. Your favorites can then be loaded when running reports that contain these parameters.

For more information, see how To enter a parameter value on page 79.

Server Error Notification

Enterprise Reporter can be configured to display or suppress a login notification indicating that the Enterprise Reporter server has unexpectedly restarted since the last login.

To configure server error notification

1. On the System Configuration page, click **Manage server error notification**.
2. Select **Do not show server restarted error** to suppress the notification.
3. Click OK.

SSRS Server settings

SSRS is a cross product online reporting platform. Once SSRS is deployed, you can configure Enterprise Reporter to enable publishing. Reports can then be published, allowing users to generate reports using a web browser instead of the Report Manager. For more information, see Configuring SSRS on page 132.

2

Running and Scheduling Reports

- Running Reports
- Configuring a Default Email Server
- Scheduling Reports
- Using the Credential Manager
- Organizing Reports

Running Reports

This section outlines how to run reports, work with parameters, find reports, view report properties, preview a report, and export a report.

See also:

- Running Category Reports
- Running Regular Reports
- Running Reports or Exporting Reports to CSV and Other Formats from Different Containers
- Entering Parameter Values
- Searching for Parameter Values
- Importing Parameter Values
- Using Saved Parameters
- Searching for a Report
- Viewing Report Properties
- Previewing a Report
- Printing a Report
- Exporting a Report to Other Formats

Running Category Reports

Category reports run and display in the report pane when the category is selected in the treeview of the Report Manager. You will find categories equipped with default category reports in Active Directory, File Storage Analysis and Exchange. For more information, see on page 27 and File Storage Analysis Reports on page 30.

Showing and Applying Category Report Parameters

To show and apply category report parameters

1 While viewing the category report, click **Show Parameters** in the toolbar.

The parameters and a Hide Parameters button are displayed, and the toolbar is hidden.

2 Enter the parameter values.

For more information, see Entering Parameter Values on page 79.

- OR -

Click **Hide Parameters** to hide the parameters and display the toolbar.

3 If the parameters have changed, click **Refresh Report** to apply the current parameters.

Change the Category Report View

To change the category report view

- While viewing the category report, click the View button to view the list of category reports.

  - OR -

  While viewing the list of category reports, click the View button to view the category report.

Navigating Within a Category Report

To navigate within a category report

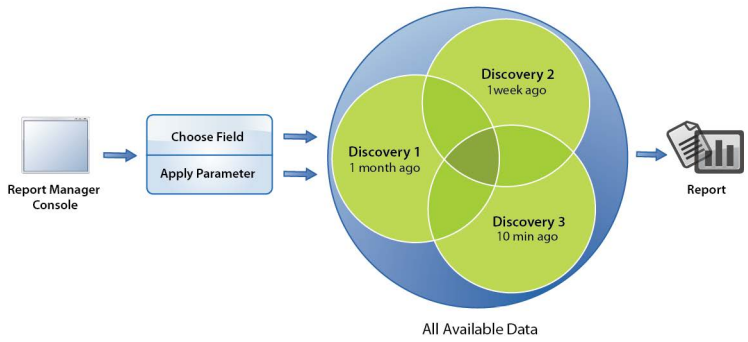
1 While viewing the category report, click on links within the report to drill down and view more specific information in associated reports.

2 Click the Next Report or Previous Report buttons in the toolbar to navigate between reports you have viewed.

Running Regular Reports

When you run a report, it returns data based on the most recent data collected by the discoveries, the selected fields, defined parameters, 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. Figure 2 outlines the source of the data for your report.

Figure 2. Relationship between collected data and a report



Because you are running reports on previously collected data, it may be important to understand the age of the data. Data may come from different discoveries, which were run at different times. Users of the Report Manager may not be aware of when and in what configuration data was collected, as discoveries are administered in the Configuration Manager.

For example, in Figure 2, the generated report relies on data collected by three different discoveries, with different ages of data. If it is important to know how fresh data is, you can add a timestamp to your report. For more information, see Indicating Data Age on a Report on page 111.

When reports contain date and time values, they are always expressed in the local time zone of the console where the report was generated. You can display this time zone on the report by modifying its layout. For more information, see Changing the Layout on page 120.

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

Printing a Report

Running Reports or Exporting Reports to CSV and Other Formats from Different Containers

The procedure for running a report, exporting a report to a raw, unformatted CSV file, or exporting to other formats is the same, no matter what container the report is in. The Report Details view provides a breadcrumb trail to make it easy to navigate back through report categories and containers.

TIP: Only administrators can run reports from the library. It is recommended that you run reports from the My Reports or Published Reports containers.

To run a report or export a report

1 Click a container or category, locate the report card, and click the report name.

- OR -

Expand the treeview as necessary, and select the report.

2 If necessary, in the Report Details view, enter the parameter values.

NOTE: A report cannot be run until all parameter cards have green check marks beside them. Optional parameters have a green check mark, but a required parameter will have a red x until you enter a valid parameter value.

For more information on entering parameters, see Entering Parameter Values on page 79.

3 Click **Run Report**.

The report is displayed to the screen for printing (see Printing a Report on page 84) or exporting to other formats (see Exporting a Report to Other Formats on page 84).

- OR -

Click **Export to CSV.** For more information, see Setting CSV File Export Options on page 125.
Provide a name and location for the file, and click **Save**.
Click **Yes** to open the file or click **No** to return to your report.

NOTE: If your organization has SSRS deployed, you may be able to run reports online. A reporting administrator must publish the reports first. For more information, see Publishing Reports to SSRS on page 133.

- OR -

Click **Export to...** For more information, see Exporting a Report to Other Formats on page 84.
Select a format for the resulting file.
Click **Export Options**, set the appropriate options, and click **OK**.
Provide a name and location for the file, and click **Save**.

Entering Parameter Values

When you run a report, parameter cards are used to filter the data and make your reports more meaningful. These parameter cards are added by the report author, who can be identified on the General tab of the Report Properties. For more information, see Types of Parameters on page 113. All parameters must have a green check mark icon beside them, satisfying the parameter requirements, before you can view the report.

Some parameters are required; you must enter values in these in order to run the report. The parameter type is indicated in the top right corner of the parameter card. Required parameters that you have not yet filled in are indicated by a red X icon. Once you have entered an acceptable value, a green check mark is displayed.

The action you take to enter a parameter value depends on both the type of operator and the type of field you are working with. For example, a field that contains numbers, combined with the *Between* operator, requires you to enter two values, one higher than the other. A field that contains a date and the *Not in the last* operator requires you to either type in or use the spin control to enter a number of days.

You can import parameter values from a file with one entry per line. You can merge the imported values with existing values or over-write the existing values. For more information, see Importing Parameter Values on page 81.

You can also save your favorite parameter values in the **System Configuration** tab with the **Report Parameter Favorites** option. When running or scheduling reports, you can then load the favorite parameter values you have configured.

You can choose whether to enter values in an optional parameter. Optional parameters have a green check mark icon regardless of whether a value is provided.

NOTE: Some optional parameters have an additional option to allow you to include all results, effectively ignoring the parameter. For example, using the optional parameter that allows you to select the type of permission you want to include (using the Equals operator), you can:

- Filter the report on specific permission types (provide a value for the parameter)
- Report on objects with no permissions (leave the parameter blank)

Include all permissions in the report (select the Include all results check box)

Once you have entered parameter values, they can be edited, deleted, or sorted. The height of the parameter window can also be expanded to make it easier to view and manage parameter values.

To enter a parameter value

1 On the parameter card, click the text box and type the value.

NOTE: Some parameters support the use of wildcard characters such as entering an asterisk * for multiple characters, or a question mark ? for a single character. For more details on which types of parameters support wildcards, see Parameter Operators on page 114.

- OR -

If there is a search icon or a filtered search icon, click and search for the value. For more information, see Searching for Parameter Values on page 80.

- OR -

If you want to load parameter values from a text file with one entry per line, click the **Import values from file icon**, select the file and click **Open**. For more information, see Importing Parameter Values on page 81.

- OR -

If favorite parameters have been configured, click **Load Parameter Favorites** under the Manage Parameters heading to the left of the parameter cards.

NOTE: You may configure your favorite parameter values in the **System Configuration** tab using the **Report Parameter Favorites** option.

2 Select a value using the list, radio buttons, or other user controls.

If the parameter has a list, it indicates that you can choose from values populated from existing data. As you type, Enterprise Reporter automatically searches for the closest match from this list. Date parameters provide a second arrow that shows a calendar you can use to select a date.

3 If there is an option to expand nested group members, you can specify how they are displayed in the report. For more information, see Searching for Parameter Values on page 80.

To edit a parameter value

1 Double-click on the parameter value to be edited.

- OR -

Right-click the selected values and select **Edit**.

2 Modify the value of the parameter.

3 Click **OK**.

To delete a parameter value

1 Click on the parameter value to be deleted.
To select multiple parameters, press Ctrl during selection.

2 Click **Delete**.

- OR -

Right-click the selected values and select **Delete** from the menu.

To sort parameter values

1 Once the parameter values have been added, click the **Sort** icon once to sort the values in ascending alphabetical order.

2 Optionally, click the **Sort** icon again to change to descending alphabetical order.

To resize the parameter window

1 Click the Resize icon to increase the height of the parameter window.

2 Click the Resize icon again to decrease the height of the parameter window to its original size.

Searching for Parameter Values

In order to properly define your report, you must choose the values to include in your report. Enterprise Reporter helps with this task by providing a list of currently available values, based on the data that has been collected in your environment. By selecting from a list instead of typing in a value, you can be sure that data exists, and that you have entered the value correctly.

Because there can be large amounts of collected data available, you can search the collected database for the parameter value for any string field. You can enter search phrase, or use the * wildcard character to help narrow down the results. Only the first 500 results are returned; in this case, you need to provide a more refined search term.

When searching for parameter values, parameters will contain the option to display search results filtered by previous parameters when possible. For example, if you have already selected a domain for a report, then subsequent parameters will have the option to display only the results from that domain.

When a parameter is specific to selecting groups or users to be included in the report, when possible, the search results page will contain the option to Show only Groups or to Show only Users. Selecting either option will filter out all other objects thus making specific Groups or Users easier to find.

To search for a parameter value

1 For any string parameter, click the **Search** icon or the **Filtered Search** icon.

Anything you have typed in the parameter value text box becomes the search term.

2 Optionally, enter a search phrase and click **Search.**

When no search phrase is provided, all results are returned.

If you have used the **Filtered Search** icon, the search results will be filtered based on the contents of previous parameters.

3 Optionally, select **Show only Groups** if it is available.

- OR -

Optionally, select **Show only Users** if it is available.

4 Select the value or values you want to include in the report, and click **Add**.

5 Click **OK**.

Importing Parameter Values

You can create a text file of parameter values that you can later import into reports when running them. This option can be especially helpful when there are many parameter values to select every time you run a report or when there is a specific group of parameter values that is the same for every report you run.

The plain text file must have a file extension of .TXT and each parameter value must be on a separate line within the file. The following examples outline how you can import account names, computer names, and file or folder paths when running various reports.

Account Names

When running a Domain Accounts report, you can import a file with account names. Each account name must be on a separate line and must be fully qualified as in the following examples.

HAL-TEST\Abby

HAL-TEST\Grace

HAL-TEST\Nevaeh

HAL-TEST\Brayden

HAL-TEST\PJ

HAL-TEST\Angela

Computer Names

When running a Computer Information report, you can import a file with the computer names for the computer parameter. Each computer name must be on a separate line and must be fully qualified as in the following examples.

HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT

HAL-TEST-SQL.HAL-TEST.DEV.HAL.CA.QSFT

HAL-TEST-DC.HAL-TEST.DEV.HAL.CA.QSFT

HAL-TEST-ITSS.HAL-TEST.DEV.HAL.CA.QSFT

HAL-TEST-EXCHG.HAL-TEST.DEV.HAL.CA.QSFT

HAL-TEST-NODE0.HAL-TEST.DEV.HAL.CA.QSFT

File/Folder Paths

When running a Folder Permissions report, you can import a file with the specific paths for the path parameter. Each path must be on a separate line.

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\Financials Report.rtf

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\HR\AMER\Payroll.rtf

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\HR\EMEA\Employee List.rtf

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\Sales\Financials Report.rtf

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\Sales\Q3 Sales.rtf

\\HAL-TEST-SRV.HAL-TEST.DEV.HAL.CA.QSFT\Financials\Sales\Sales Graph.bmp

Using Saved Parameters

Once you have parameters entered, you can save them as the default parameters for that report. If you already had default parameters saved, they are overwritten with the new values.

When you display the Report Details view, the parameters are already entered, so you can run the report with the default parameters or edit them as needed. If you edit parameters, you can return to the current default parameters at any time.

To save default parameters

1. Open the Report Details view for the report. For more information, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78.
2. Enter parameters as needed. For more information, see Entering Parameter Values on page 79.
3. Click **Save parameters as default**.

   The parameters overwrite any current default parameters.

To restore default parameters

1. Open the Report Details view for report. For more information, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78.
2. Click **Restore default parameters**.

The Expand Nested Groups Parameter

Some reports have a parameter that allows you to expand nested group members and specify how they are displayed in the report. The five ways you can handle nested groups and their members are as follows:

- Do not expand nested group membership
- Expand inline including members of Domain Users group
- Expand inline excluding members of Domain Users group
- Expand in subreport including members of Domain Users group
- Expand in subreport excluding members of Domain Users group

Optionally you can add more fields for the nested group members to be displayed in the report and save it for future use.

To add more nested group member fields when running a report

1. When running a report, click **Add Fields** at the Expand Nested Groups parameter.

2 Select the fields you want from the available fields list, and click **Add**. For more information, see Modifying the Fields to be Included on page 109.

3 Click **OK**.

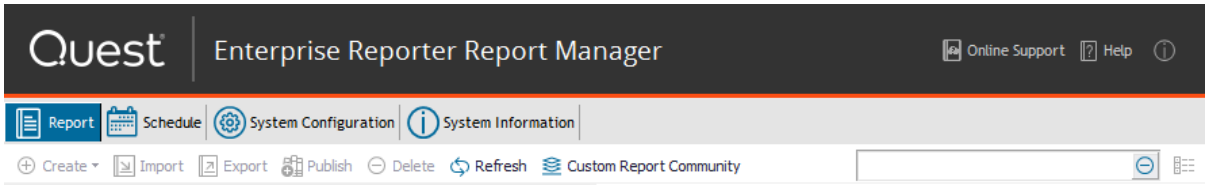
4 Complete all required fields.

5 Optionally, click **Save parameters as default** to save the fields for the next use of this report.

6 Continue with running or exporting this report as usual. For more information, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78.

Searching for a Report

You can search for reports based on the report name, the author, and text in the report description. Searching is performed within the selected container or category. As you type in the search field, your report list is dynamically narrowed down.



If you type more than one word, the Report Manager looks for either of the words—it creates an OR condition. If you want to search for a phrase, enclose it in quotations. For example, if you search for Boston Office, you will see all reports that have Boston and all reports that have Office. If you search for "Boston Office", you will see all reports that have that exact phrase.

To search for reports

1 Click the container or category you want to search.

2 In the search box, type a phrase.

To clear a search

- Clear the contents of the search box.

  - OR -

  Click on a different container or category.

Viewing Report Properties

If you want to see how a report was designed, you can open the Edit Report dialog box and examine the settings. If the report is in the Library, you can view the properties but cannot make any changes. If the report is in Published Reports, you can view the properties but only reporting administrators can make changes. See Editing Reports on page 107 for more information on modifying the report definition.

To see the settings used in creating the report

1 Display a report list by clicking a report container or category, then locate the report card and, in My Reports, click **Edit**; otherwise, click **Properties**.

  - OR -

  Expand the treeview until you locate the report, then right-click the report and, in My Reports, click **Edit Report**; otherwise, click **Properties**.

  - OR -

Expand the treeview until you locate the report, select the report and on the Report Details page under Manage Report, in My Reports or Published Reports, click **Edit Report**; otherwise, click **Properties**.

2 Click each tab to view the General, Fields, Parameters, Query, and Layout pages.

Previewing a Report

Preview is a quick way to see what your report will look like. It returns a shortened version of the report, without prompting for parameter values.

To preview a report

1 Click a report container.

- OR -

Expand a report container and select the category containing the report.

2 On the report card for the report, click **Preview**.

3 Examine the report and then close the window.

If there is no data in the report, it is possible the relevant data has not yet been collected. For more information, see your Enterprise Reporter administrator or see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.

Printing a Report

Once you run a report, you can print the entire report, or just specific pages.

To print a report

1 Run the report.
For more information, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78.

You can change the paper size, margins and orientation by clicking Page Setup.

2 Click the **Print** button.

3 If necessary, select a printer, set a page range, or a number of copies.

4 Click **Print**.

Exporting a Report to Other Formats

Before or after running a report, you can export it to one of the following formats:

- PDF
- HTML
- MHT
- RTF
- Excel
- CSV (with formatting)
  This option exports a CSV file that contains formatted information (such as title and description information). For more information on exporting to a raw, unformatted CSV file, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78 and Setting CSV File Export Options on page 125.
- Text file
- Image File (includes all common image formats).

- You can also email your report in any format directly from the report window.

The procedure for exporting a report to a raw, unformatted CSV file, or exporting to other formats is the same, no matter what container the report is in.

TIP: Only administrators can run reports from the library. It is recommended that you run reports from the My Reports or Published Reports containers.

To export a report without running the report

1. Click a container or category, locate the report card, and click the report name.

   - OR -

   Expand the treeview and select the report.

2. If necessary, in the Report Details view, enter the parameter values.

   NOTE: A report cannot be exported until all parameter cards have green check marks beside them. Optional parameters have a green check mark, but a required parameter will have a red x until you enter a valid parameter value.

   For more information about entering parameters, see Entering Parameter Values on page 79.

3. In the sidebar, click **Export to CSV.** For details, see Setting CSV File Export Options on page 125.

   1. Provide a name and location for the file and click **Save**..
   2. Click **Yes** to open the file or click **No** to return to your report.

   NOTE: If your organization has SSRS deployed, you may be able to run reports online. A reporting administrator must publish the reports first. For more information, see Publishing Reports to SSRS on page 133.

   - OR -

   1. In the sidebar, click **Export to...**
   2. Select a format for the resulting file.
   3. Click **Export Options**, set the appropriate options, and click **OK**.
   4. Provide a name and location for the file and click **Save**.

To export a report after running the report

1. Click a container or category, locate the report card, and click the report name.

   - OR -

   Expand the treeview as necessary, and select the report.

2. If necessary, in the Report Details view, enter the parameter values.

   NOTE: A report cannot be exported until all parameter cards have green check marks beside them. Optional parameters have a green check mark, but a required parameter will have a red x until you enter a valid parameter value.

   For more information on entering parameters, see Entering Parameter Values on page 79.

3. In the sidebar, click **Run report**. and wait for the report to finish.
4. Click the **Export** drop-down to display export options.
5. Click the **Export To** drop-down to display a list of formats.

   To email a report, click the **Email-As** drop-down or arrow to display a list of formats.

6. Select a format.
7. Set the export options and click **OK**.
8. Provide a name and location for the file, and click **Save**.

9 Click **Yes** to open the file.

- OR -

Click **No** to return to your report.

Configuring a Default Email Server

If you are a reporting administrator, and want to make it easier for reporting users to set up email in Enterprise Reporter, you can configure default email settings. There are two options for email settings:

- You can configure a default SMTP server that reporting users can select when setting up report delivery. You can provide a server that uses anonymous connections or one that uses authentication. Users can provide their own credentials when they create a schedule.
- If you need OAuth2 authentication for sending email, you can configure an Exchange Online connection to send reports by email. To use Exchange Online, you must register an application for Enterprise Reporter with Microsoft Entra ID, using certificate-based authentication. For details see “Registering an Application for Exchange Online Email Delivery” in the *Configuration Manager User Guide*.

To configure a default SMTP server for email

1 On the Report Manager **System Configuration** tab, click **Configure email settings used by Enterprise Reporter**.

2 For service type, select **SMTP**.

3 Enter the Host server name or IP address.

4 Enter the Host port number.

5 Select a user account with credentials required to access the mail server by clicking the ellipsis (...) to open the Credential Manager. For more information, see Using the Credential Manager on page 98.

If you need to remove the credentials, click **Clear**.

6 To test the connection, enter the email address to be used as the sender when testing the connection of the Host configuration.

7 To test the connection, enter the email addresses to be used as the recipient when testing the connection of the Host configuration.

8 To test the Host configuration, press **Click to test your connection**.

9 Optionally, you can adjust the **Attachment Size Limit** to accommodate the size (in MB) of email attachments that will be sent by email.

10 Click **OK**.

To configure an Exchange Online connection for email

1 On the Report Manager **System Configuration** tab, click **Configure email settings used by Enterprise Reporter**.

2 For service type, select **Exchange Online**.

3 Enter the following information for the app that has been registered in Microsoft Entra ID for Enterprise Reporter:

- **Application (client) ID:** The application (client) ID for the Microsoft Entra ID application created for Enterprise Reporter email notifications.
- **Directory (tenant) ID:** The directory (tenant) ID for the Microsoft Entra ID application created for Enterprise Reporter email notifications.
- **Certificate Thumbprint:** The certificate thumbprint for the certificate that was uploaded to the registered app.

- **Cloud instance**: Select the type of cloud instance to use for notifications - Azure Cloud (default), US Government Cloud L4, or US Government Cloud L5 (DoD).

For details about how to register an application in Microsoft Entra ID, see “Registering an Application for Exchange Online Email Delivery” in the *Configuration Manager User Guide*.

4 Optionally, you can adjust the **Attachment Size Limit** to accommodate the size (in MB) of email attachments that will be sent by email.

5 Click **OK**.

Scheduling Reports

You can create a schedule, or a series of schedules, to run reports. Once you have created a schedule, you can add reports and set the parameters for the reports. You can also view a calendar showing when the reports will run based on the schedule.

When you are deciding how often to run reports, make sure you understand how often the data on which you are reporting is collected. Your reporting interval needs to be at least the size of the data collection interval, or there will not be any new information in the reports. For more information on data freshness, see Running Reports on page 76. Each schedule card has the option to disable or enable the schedule if the need arises. The Schedule page also contains the option to sort all reports within each schedule by name or by type.

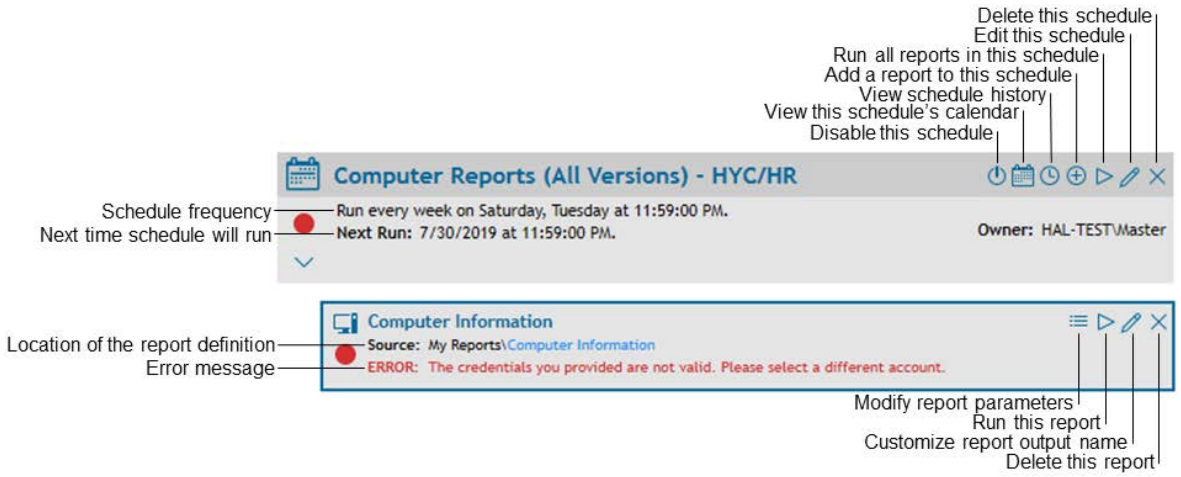
NOTE: Reports can be scheduled from the My Reports container. Reporting Administrators can also schedule reports from the Published Reports container.

When you add a report to a schedule, a link is maintained between the originating report and the scheduled version. Any changes to the report definition and layout will be reflected in all scheduled versions. The originating report path is indicated on the scheduled report card.

NOTE: If you change the parameters in the originating report, the scheduled versions are not updated. If you want to use the new parameters, remove the reports from any schedules, and add the new version. For more information, see Removing Reports from a Schedule on page 96 and Adding Reports to a Schedule on page 95.

You can add the same report to a single schedule more than once, or to different schedules. This allows you to schedule different versions of the report by providing different parameter values. In order to help you keep track of the various versions, you can provide a description of the parameter values. This description also appears on the scheduled report card. Figure 3 shows this information on the scheduled report card.

Figure 3. A scheduled report card



See also:

- Creating a Schedule
- Types of Schedules
- Working with Schedules
- Types of Schedules

Creating a Schedule

The first step in scheduling reports is to create a schedule. One schedule can be used for many reports. Reports can be deposited in a file share you specify, can be emailed to selected users, or can be distributed using both methods.

NOTE:

- You must provide credentials to generate and deliver reports. Ensure these credentials have write access to the target share. If you want to allow all users of the Report Manager to have access to the target share, you can permission the Reporter_Reporting_Operators and/or the Reporter_Reporting_Admins groups. If you use an account that is not a member of either of these groups, you must manually give the account permission to read the database; otherwise no reports are generated.
- Users that only have the Reporter_Reporting _Operators role cannot modify or schedule reports that are located in Published Reports. To create a schedule and send a report to a location or through email, users need to copy the report from Published reports and place it into My Reports. For complete details on roles and their associated permissions, see the section on role-based security in the Installation and Deployment Guide.

See also:

- Delivering Scheduled Reports by Email

To create a schedule

1. On the Schedule tab, click **New Schedule**.
2. Give your schedule a unique name.
3. Enter the schedule details.

   For more information, see Types of Schedules on page 92.
4. Select an account from the Credential Manager.

   If the account you want is not on the list, click Add and enter the account, then select it from the list. For more information, see Using the Credential Manager on page 98.
5. Select the format for your report.

   For more information on these formats, see Exporting a Report to Other Formats on page 84. Not all formats are available for scheduled reports.
6. Optionally, click **Export Options** and set options such as the Export Mode and the Page Range.
7. Optionally, select **Send report to share** to deposit the finished report to a share.

   Type, select one of the 10 most recent entries from the pull-down menu, or browse to the share path where the reports are to be delivered.

   If you are typing, use the form \\servername\share.

   You can filter in the browser to make it easier to locate a particular share.
8. Optionally, select **Send Email** to email a copy of the report.

   You must specify the From details for the sender and at least one recipient by typing in the email addresses or by selecting one of the 10 most recent entries from the pull-down menu. If you have configured email to use Exchange Online, the send address must be an Exchange Online account.

You can also modify the Subject and Body of the email message.

For more information on setup and configuration, see Delivering Scheduled Reports by Email on page 89. For more information on customizing the message, see Modifying Scheduled Email Messages on page 90.

You can select **Attach report to email** to send the report as an attachment.

If you opt to send attachments, you can also select Do not attach reports with empty data results to avoid sending empty reports.

If you opt to send attachments, you can also select **Do not attach reports with empty data results** to avoid sending empty reports.

9 Click **OK**.

10 Optionally, click calendar icon to display a calendar showing the schedule visually.

Delivering Scheduled Reports by Email

You can choose to have all of the reports on a schedule delivered by email. Reports can also be delivered to a network share, since some organizations do not allow certain file types to be sent, and restrict the size of attachments.

To configure email, you must provide either an SMTP email server or an Exchange Online connection.

- For on-premises email delivery, your administrator might have provided a default SMTP email server for you to use. Otherwise, you must enter the server name and port number. Unless the SMTP server is configured to accept anonymous connections, you must also provide valid credentials for the SMTP server.
- For Exchange Online, you need the Application (client) ID, Directory (tenant) ID, Certificate Thumbprint, and cloud instance for the application that is registered with Microsoft Entra ID. You must use an account that is an Exchange Online account on the tenant to which you are connecting.

The same SMTP server or Exchange Online connection is used for all schedules. If you change the SMTP server or Exchange Online connection setting on one schedule, all other schedules are automatically updated.

If you select the **Attach email to report** option, Enterprise Reporter attempts to email the reports as an attachment. If your email setup does not allow for this and you have selected the **Save to share** option, the email will have a link to the share on which the reports are located.

To set up email delivery of reports

1 Create or edit a schedule. For more information, see Creating a Schedule on page 88.

2 Optionally, select **Send report to share** to deposit the finished report to a share.

Type or browse to the share path where the reports are to be delivered. If you are typing, use the form \\servername\share. You can filter in the browser to make it easier to locate a particular share.

3 Select **Send Email**.

You can select **Attach report to email** to send the report as an attachment. If you opt to send attachments, you can also select **Do not attach reports with empty data results** to avoid sending empty reports.

4 If this is your first schedule, select **Configure the mail server**.

If you make changes to the mail server configuration (SMTP or Exchange Online), all schedules will be updated. For more information, see Configuring a Default Email Server on page 86.

5 In the **From** field, type the sender email address or select one of the 10 most recent entries from the pull-down menu. Note that if Exchange Online is being used, you must select an Exchange Online account for the tenant you are using.

6 In the **To**, **CC**, and **BCC** fields, type the recipient email addresses, separated by a comma or semicolon. You can also select from the 10 most recent entries from the pull-down menu.

7 Optionally, type a subject that indicates the purpose of the reports being emailed. If the Subject field is left blank, the default subject from the template is used.

8 Optionally, modify the Body of the email message.

For more information, see Modifying Scheduled Email Messages on page 90.

9 Click **OK**.

To configure your mail server for all schedules

1 Create or edit a schedule.

2 If necessary, select **Send Email**.

3 Click **Configure mail server**. There are two ways to configure email notification: SMTP and Exchange Online.

- If your administrator has configured a default email SMTP server, or if you have previously configured an SMTP server for a schedule, the fields are filled in.
- If your administrator has configured email to use Exchange Online, or if you have previously configured an Exchange Online for a schedule, the fields are filled in.

  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 Enter the required configuration information following the steps found in Configuring a Default Email Server on page 86.

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

5 Test your connection.

6 Click **OK**.

Modifying Scheduled Email Messages

When scheduling reports, one of the Delivery options is to Send Email. When the Send Email option is selected, the Default SchedulingTemplate.xml template is automatically loaded into the Body field as the default message. For more information, see Modifying Scheduled Email Templates on page 91.

You may modify the email message for this schedule, but it is important to note that the email template contains variables and tags that control the content and layout of the email message.

The following options may be used anywhere within the body of the message.

Table 31. Scheduled Email Message Global Variables

Variable	Content
{%report_schedule%}	schedule name
{%network_path%}	path location of scheduled reports
{%filename%}	name of the file containing scheduled reports

Table 32. Scheduled Email Message Formatting Tags

Tag	HTML Layout Equivalent
<body></body>	<body></body>
<static></static>	

To create a section that will be repeated for every report in the schedule, use <repeat> and </repeat> to indicate the beginning and the end of the section.

The following variables and tags may be used anywhere within the repeating section:

Table 33. Scheduled Email Message Repeating Section Variables

Variable	Content
{%name%}	name of report
{%description%}	description of report

Table 34. Scheduled Email Message Repeating Section Formatting Tags

Tag	HTML Layout Equivalent
<row></row>	<tr></tr>
<plaintext></plaintext>	<td></td>
<dynamictext></dynamictext>	<td></td>

An example of an email message using all available variables and tags is shown below.

```
<Body>
    <static>The report schedule "{%REPORT_SCHEDULE%}" has successfully completed. The following reports can be found in this location:
        <link>{%NETWORK_PATH%}</link>
    </static>
    <repeat>
        <row>
            <plaintext>Report Name:</plaintext>
            <dynamictext>{name%}</dynamictext>
        </row>
        <row>
            <plaintext>Description:</plaintext>
            <dynamictext>{description%}</dynamictext>
        </row>
        <row>
            <plaintext>Filename:</plaintext>
            <dynamictext>{%filename%}</dynamictext>
        </row>
    </repeat>
</Body>
```

Modifying Scheduled Email Templates

You can choose to have all of the reports on a schedule delivered by email. For more details, see Delivering Scheduled Reports by Email on page 89. The success, failure, or attachment size of the scheduled reports determines which email template is used.

The templates are located in the following directory on the computer where the Enterprise Reporter server is installed:

- Program Files\Quest\Enterprise Reporter\Server\EmailTemplates

Email templates are provided for the following four scenarios:

- A schedule completes successfully and the total size of all reports is less than the maximum of 500KB.
  `DefaultSchedulingTemplate.xml`
  `DefaultSchedulingTemplate.xslt`
- A schedule does not complete successfully.
  `FailureTemplate.xml`
  `FailureTemplate.xml`
- The total size of all reports exceeds the maximum of 500KB so no reports are attached.
  `DefaultSchedulingTemplate.xml`
  `DefaultSchedulingTemplate.xslt`
- A schedule is partially complete because one or more reports fail.
  `PartialCompleteTemplate.xml`
  `PartialCompleteTemplate.xslt`

You can use any XML editor to modify the templates (.xml) and their corresponding email style files (.xslt). Some prior knowledge of XML and Extensible Stylesheet Language Transformation will be helpful. For more information, see Email Template Structure (.xml) on page 92.

TIP: Given the precise nature of the content formatting, using an XML editor to validate changes to the email templates and their style files is recommended.

Email Template Structure (.xml)

The template files contain tags such as <EmailTemplate>, <Subject> and <Body>. The attributes and textual content of these tags may be modified. For example, to change the subject of an email template, open the applicable template file and change the content between <Subject> and </Subject>.

To add more information to the email messages, the following tags can be repeated within the same template:

- <static>
- <repeat>
- <plaintext>
- <dynamictext>

Text between the `{%....%}` tags must remain unaltered as they control relative content embedded in the email messages as they are generated. For more information, see Modifying Scheduled Email Messages on page 90.

Modifying the Maximum File Size for an Email Attachment

The default maximum file size for Enterprise Reporter e-mail attachments is 1MB. You can increase the maximum attachment size to accommodate larger reports by modifying the Enterprise Reporter configuration.

How to modify the maximum file size for an email attachment

1. Open the Enterprise Reporter Report Manager.
2. Click the **System Configuration** tab.
3. Click **Configure SMTP server used by Enterprise Reporter** under Email Settings.
4. Enter an **Attachment Size Limit** (in megabytes) that accommodates your reports.
5. Click **OK**.

Types of Schedules

There are various types of schedules you can create; one-time, daily, weekly, monthly, yearly, or for specific months.

NOTE: All times are stored in local time. They will be adjusted when your local time changes, such as for Daylight Savings Time.

See also:

- Run Your Schedule Once
- Run Your Schedule on a Daily Interval
- Run Your Schedule on Specified Days of the Week
- Run Your Schedule on a Specified Day of the Month
- Run Your Schedule Yearly

Run Your Schedule Once

This allows you to run your schedule a single time, at a date and time you provide.

To schedule a single run

1. In the Settings area of the Create Schedule dialog box, click **Run Once**.
2. In the Start Date field, select the element you want to change, and use the spin arrows to change the value.

Run Your Schedule on a Daily Interval

You can run your schedule every day, or at an interval you choose. For example, if you set the interval to two days, starting on the 22nd day of the month, it will run on the 24th, 26th, 28th and 30th.

The schedule resets at the beginning of the month, so if you have a daily schedule it runs on the first of the month, and then at the set interval. In the above example, after the run on the 30th, the next scheduled runs are the 1st and 3rd of the following month.

To schedule a daily run

1. In the Settings area of the Create Schedule dialog box, click **Daily**.
2. In the Start Date field, click the drop-down arrow, and use the calendar to select the date and time.

   - OR -

   In the Start Date field, select the element you want to change, and use the spin arrows to change the value.
3. Set the interval for your daily run.

Run Your Schedule on Specified Days of the Week

You can set any number of days of the week, and your schedule will run at the set time on those days.

To schedule a weekly run

1. In the Settings area of the Create Schedule dialog box, click **Weekly**.
2. In the Start Date field, click the drop-down arrow, and use the calendar to select the date and time.

   - OR -

   In the Start Date field, select the element you want to change, and use the arrows to change the value.
3. Select the days on which you want your schedule to run.

Run Your Schedule on a Specified Day of the Month

You can select a certain day of the month to run your schedule. This can either be a calendar day, such as the 1st day of the month, or it can be described, such as the last Friday of the month.

To schedule a monthly run

1 In the Settings area of the Create Schedule dialog box, click **Monthly**.

2 In the Start Date field, click the drop-down arrow, and use the calendar to select the date and time.

- OR -

In the Start Date field, select the element you want to change, and use the arrows to change the value.

3 Select the day of the month on which you want your schedule to run.

- OR -

Select the weekly interval and day of the month.

Run Your Schedule Yearly

You can select month and day combinations to run your schedule. This feature offers a variety of options for timing a schedule including:

- a single month and a single day, such as the 31st day December
- single month and multiple days, such as the 1st and 31st day of January
- multiple months and a single day, such as the 1st day of every other month
- multiple months and multiple days, such as the 1st and 15th of every third month

To schedule a yearly run

1 In the Settings area of the Create Schedule dialog box, click **Yearly**.

2 In the Start Date field, click the drop-down arrow, and use the calendar to select the date and time.

- OR -

In the Start Date field, select the element you want to change, and use the arrows to change the value.

3 Select the months and days of the year on which you want your schedule to run.

Working with Schedules

Once you have created a schedule, you can add and remove reports, or delete the schedule entirely. When a schedule runs, the reports are generated using the parameter values provided, and are deposited in the designated share. Each time a report is generated, a new file name is created. The file name is composed of the name of the report, an ID to help you identify the report and parameter combination, and the time the report was run. You can optionally specify an alternate filename or allow new reports to overwrite old ones (by removing the unique ID and timestamp information). You can run all reports in a schedule any time, without waiting for the next scheduled time.

Reporting administrators have some control over other users' schedules and can transfer ownership of a schedule should the need arise. Reporting administrators can view and sort all schedules for all users, remove reports, and delete schedules entirely. If you are a reporting administrator, this allows you to troubleshoot scheduling issues, and control the volume of reports being generated. Administrators should work with their users to define good scheduling practices if the volume of reports is high.

See also:

- Adding Reports to a Schedule
- Editing Report Output Options on a Schedule
- Removing Reports from a Schedule
- Deleting a Schedule
- Running a Schedule

- Disabling or Enabling a Schedule
- Viewing Schedule History
- Transferring Ownership of Schedules

Adding Reports to a Schedule

From the My Reports container, you can add many reports to a schedule, and you can add a report to as many schedules as you like. Reporting Administrators may also schedule reports from the Published Reports container. If a report you want to schedule is in another container, you may copy reports from one container to another to facilitate scheduling. For more information, see Copying Reports on page 105. Once you add a report, you can enter parameter values or load favorite parameter values that will be used to generate the report. If you do not enter parameter values, the report contains all available data.

TIP: You can add the same report to a single schedule more than once, or to different schedules. This allows you to schedule different versions of the report by providing different parameter values. It is recommended that you use a parameter value description to differentiate between versions of the same report. This description appears on the scheduled report card, and can save you from having to examine the parameter values themselves to identify the contents of the scheduled report.

NOTE: When the report is run, an ID and timestamp is added to the report name, to help you identify the output. Once you have scheduled a report, you can edit the output options to enter a custom report name to be used for the filename or choose for new reports to overwrite the existing report (by removing the unique ID and timestamp information). For more information, see Editing Report Output Options on a Schedule on page 96.

NOTE: Once you have scheduled a report, you can run it with the current parameter values by displaying the scheduled report card and clicking **Run Now**.

To add reports to your schedule

1. If necessary, create the schedule. For more information, see Creating a Schedule on page 88.
2. On the Schedule tab, on the schedule card, click **Add a report to this schedule**.
3. Select the reports.
4. Click **OK**.

   A scheduled report card appears for each selected report.
5. Select a scheduled report card and click **Modify report parameters**.
6. Enter the parameter values for all required parameters, and for optional parameters as desired.

   If there is a search icon, click and search for the value. For more information, see Searching for Parameter Values on page 80.

   If favorite parameters have been configured, you can optionally click **Load Favorites** to load them now. For more information, see Entering Parameter Values on page 79.
7. Type a description in the **Parameter Set Name** box.

   Use a description that identifies the data that will be included in the report.
8. Click **Save**.

   If you do not click Save, and navigate away from the scheduled report card, no parameter values will be saved. In this case, your report returns all data, and may take longer to generate.
9. Repeat steps 5 through 7 for each report you scheduled.

Editing Report Output Options on a Schedule

You can edit the output options for a report on a schedule. Reports are generated with filenames in a standard format of *report name_id_timestamp* (for example, *Report Name_ID_yyyymmdd-hhmmss.pdf*). You may enter a custom report name to be used for the filename or choose to exclude the ID and timestamp from the filename.

To edit the output options for a report on a schedule

1. On the Schedule tab, locate the desired schedule card.
2. Navigate to the report to be changed.
3. Click **Customize report output name**.
4. Optionally, select **Use custom report name** and enter the name to be used for the filename.

   NOTE: The custom report name will be reflected on the card for the report.

5. Optionally, select **Overwrite** to exclude the ID and timestamp from the filename.

   NOTE: Disabling the ID and timestamp will mean that each subsequent run of this report will overwrite the previous report.

6. Click **OK**.

Removing Reports from a Schedule

You can remove a report from a schedule. This does not delete the report, however you now have to run the report manually, or add it to another schedule.

If you are a reporting administrator, you can remove a report from any user's schedule. This allows you to stop reports that are causing issues, such as taking up too much space in a network share, from running on schedule.

To remove a report from a schedule

1. On the Schedule tab, locate the desired schedule report card.
2. Click **Delete this report**.
3. Click **Yes** to confirm.

Deleting a Schedule

If you no longer need a schedule, you can delete it. All scheduled reports are removed, and need to be run manually or added to another schedule.

If you are a reporting administrator, you can delete any schedule. For example, if an employee leaves, you can remove all of their schedules.

To delete a schedule

1. On the Schedule tab, locate the desired schedule card.
2. Click **Delete this schedule**.
3. Click **Yes** to confirm.

Running a Schedule

When you run a schedule, all reports on the schedule are immediately run with their current parameter values. Reports are delivered as defined in the schedule. You can also run a single report with the current parameter values.

To run all reports on a schedule

1. On the Schedule tab, locate the schedule card.
2. Click **Run all reports belonging to this schedule**.

To run a single report on a schedule

1. On the Schedule tab, locate the schedule card.
2. Locate the report.
3. Click **Run this report**.

   The report is delivered as outlined in the schedule.

Disabling or Enabling a Schedule

When the need arises, you can disable a schedule to keep the reports on that schedule from running at their normal times. The Next Run will indicate that the schedule is Disabled. When you are ready to resume running the schedule, using the same icon, you can enable the schedule.

To disable a schedule

1. On the Schedule tab, locate the schedule card for a schedule that is enabled.
2. Click the **Disable this schedule** icon.

To enable a schedule

1. On the Schedule tab, locate the schedule card for a schedule that is disabled.
2. Click the **Enable this schedule** icon.

Viewing Schedule History

You can view the history for a schedule. The history shows the last ten times the schedule ran and any corresponding errors for each report in the schedule.

To view the history of a schedule

1. On the schedule tab, locate the schedule card.
2. Click the **View history** icon.
3. Click on any historical run with an error count greater than zero.
4. View the report names and corresponding detailed error messages in the right-hand pane.

Transferring Ownership of Schedules

Reporting administrators can transfer ownership of a schedule from one user to another. Transferring ownership of a schedule also transfers ownership of all reports belonging to that schedule. The credentials for the transferred schedules must be re-configured by the new owner.

To transfer ownership of schedules

1. As a Reporting Administrator, navigate to the Schedule tab of the Report Manager.
2. Click **Ownership** at the top of the list of schedules.
3. Select the existing owner of the schedules to be transferred.
4. Select the user to whom the schedules will be transferred.
5. Select the schedules to be transferred.

- OR -

Click **Select All** to select all available schedules.

6 Click **OK**.

7 Click **Yes** to confirm the transfer.

NOTE: A red warning symbol at the top of the transferred schedules indicates that the credentials of the those transferred schedules must be re-configured.The new report owner must click the pencil icon beside the warning symbol and select an account with the appropriate credentials.

Troubleshooting Scheduling Issues

If problems occur during the running of a schedule, an error indicator (a red dot) appears on the scheduled report card, along with an error message providing you with information to help you address the issue.

An error indicator on a schedule card indicates that one or more of the scheduled reports has an error. Resolve the issue, and then either wait until the next scheduled run, or manually run any needed reports by clicking **Run this report** on the scheduled report card, or run the schedule by clicking **Run all reports belonging to this schedule** on the schedule card.

You can also click the View History icon on the schedule card to see the last ten times the schedule ran and any corresponding errors. For more information, see Viewing Schedule History on page 97.

The report only exports as CSV

If you are running a report or have scheduled a report that will only output to CSV (no matter which format you select), this is likely a report that does not have a layout on the Layout tab of the report definition. For more information, see Creating Report Layouts on page 124.

The report generates but the email has an error

If a report schedule runs and the report file gets created correctly, but the email has the following error,

> "The report schedule has failed. To view the reason for the failure, go the Schedule Explorer in the Report Manager, or contact your Reporter administrator. I have verified that there are no illegal characters in the name",

this can indicate that the size of the report file exceeds the default maximum file size of 1MB for Enterprise Reporter email attachments. See Modifying the Maximum File Size for an Email Attachment on page 92 for instructions on how to increase the maximum file size for email attachments.

Using the Credential Manager

Credentials are used in different places in Enterprise Reporter. For example, nodes and report schedules both use credentials. The Credential Manager is a central store for accounts and passwords used throughout the system. This makes it easy to keep passwords up to date, and allows you to enter the credential details once, and access them repeatedly.

NOTE: Microsoft Entra and Microsoft 365 discoveries now support multi-factor authentication. The Microsoft Entra discovery credentials will need to be authenticated by Microsoft through the Credential Manager.

NOTE: Credentials added in the Report Manager are only available to the user who added them, while accounts added in the Configuration Manager are available to all Configuration Manager users on the same Enterprise Reporter server.

Accounts are not verified when you add them, and they must already exist in order to be used by Enterprise Reporter. For each account, you can add a description. This is particularly useful for differentiating between similar

accounts, such as similarly named service credentials, or your SQL Server® default "sa" accounts. The combination of the account name and the description must be unique.

Accounts with multi-factor authentication enabled need to be authenticated by Microsoft through the Credential Manager.

Credential passwords are encrypted with FIPS 140-2 compliant algorithms and an encryption key that has a user-supplied password. The encryption key is secured in the Windows Credential Manager (not to be confused with the Enterprise Reporter Credential Manager). The encryption key is used to encrypt all passwords that are used in Enterprise Reporter for collections and reporting. Additionally, Enterprise Reporter security groups and roles are used to validate who has access to the encryption key and the key cannot be retrieved without proper authorizations.

The Credential Manager will display a red key icon next to each account that requires a password.

See also:

- Changing passwords using the Credential Manager
- Changing account names using the Credential Manager

To open the Credential Manager

- On the System Configuration page, go to Credential Manager and click **Manage credentials**.

  - OR -

  Click the ellipsis anywhere credentials are required.

To use a credential from the Credential Manager

1. Select the account from the list.
2. Click **OK**.

To add a credential for use in the system

1. Open the Credential Manager.
2. Click **Add.**
3. Type the account name.

   You can enter any account that you want to use in Enterprise Reporter, including Windows accounts, SQL Server accounts, and Microsoft Entra accounts.

   NOTE: If you are entering credentials in the Configuration Manager, remember that other users may have entered the same credential, so if necessary, verify that you are adding a unique account.

   If this is a Microsoft Entra-enabled account, select the **Microsoft Entra Credential** option. Once selected, click **Authenticate** to login and authenticate the account through Microsoft.
4. Type the password for the account.
5. Optionally, type a description.

   The combination of the account name and the description must be unique.
6. Click **OK**.

To add a multi-factor authenticated credential

1. Open the Credential Manager.
2. Click **Add**.
3. Enter the account user name and password.

   NOTE: The combination of the account name and the description must be unique.

4 Optionally, enter a description.

5 Click **Authenticate**.

6 On the Microsoft Entra authentication screen, enter the account name.

7 Click **Next**.

> **NOTE:** When entering credentials in the Configuration Manager, verify that no other users have used the same credential and that the account you are adding is unique.

8 Enter the password for the account.

9 Click **Sign In**.

10 Enter the verification code sent to the account.

11 Click **Verify**.

The Credential Manager authenticates the account for discovery usage and changes the account information on any applicable discoveries.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

12 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To edit a credential

1 Open the Credential Manager.

2 Select an account.

3 Click **Edit**.

4 Optionally, modify the password by selecting **Edit Password**.

5 Make all changes.

6 Click **OK**.

7 If changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To edit a multi-factor authenticated credential

1 Open the Credential Manager.

2 Select an account.

3 Click **Edit**.

4 Modify the account.

5 Click **Authenticate**.

6 On the Microsoft Entra authentication screen, enter the account name.

7 Click **Next**.

> **NOTE:** When entering credentials in the Configuration Manager, verify that no other users have used the same credential and that the account you are adding is unique.

8 Enter the password for the account.

9 Click **Sign In**.

10 Enter the verification code sent to the account.

11 Click **Verify**.

The Credential Manager authenticates the account for discovery usage and changes the account information on any applicable discoveries.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

12 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To alter an account to be multi-factor authentication enabled

1 Open the Credential Manager.

2 Select the account to authenticate.

3 Click **Authenticate**.

4 On the Microsoft Entra authentication screen, enter the account name.

5 Click **Next**.

> **NOTE:** When entering credentials in the Configuration Manager, verify that no other users have used the same credential and that the account you are adding is unique.

6 Enter the password for the account.

7 Click **Sign In**.

8 Enter the verification code sent to the account.

9 Click **Verify**.

The Credential Manager authenticates the account for discovery usage and changes the account information on any applicable discoveries.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

10 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To delete a credential

1 Open the Credential Manager.

2 Select an account from the list.

You can only delete accounts that are not currently in use.

3 Click **Delete**.

4 Click **OK**.

Changing passwords using the Credential Manager

When passwords are changed in Active Directory and Microsoft Entra ID, they must be updated everywhere they are in use in Enterprise Reporter. It is possible that the account might be locked if you do not make this change. The Credential Manager makes this easy by providing a central store for accounts. You can change the password and it is updated in all nodes, schedules, discoveries, and so on.

NOTE: You can modify credentials from anywhere you can access the Credential Manager. Be aware when you make a change to a credential, it is applied throughout your deployment, not just in your current context.

If you modify credentials that are used by a discovery node, the node service must be restarted before the changes take effect. Enterprise Reporter will attempt to restart the node. However, if the restart fails, you may need to manually start the service on the computer that hosts the node. If there are jobs currently running on the node, they will be cancelled. To prevent this, either change the credentials during a down time, or cancel the discoveries yourself and restart them once the change takes effect.

Credential passwords are encrypted with FIPS 140-2 compliant algorithms and an encryption key that has a user-supplied password.

The Credential Manager will display a red key icon next to each account that requires a password.

To change the password on an account

1 On the System Configuration page, click **Manage credentials**.

It is recommended that you make these changes while no discoveries are running (or waiting to be run) before changing the password.

2 Select the account, and click **Edit**.

3 Select **Edit Password**.

4 Modify the password and click **OK**.

A progress dialog box appears.

NOTE: The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

5 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To change the password on a multi-factor authenticated account

1 On the System Configuration page, click **Manage credentials**.

It is recommended that you make these changes while no discoveries are running or waiting to be run before changing the password.

2 Select the account and click **Edit**.

3 Select **Edit Password**.

4 Modify the password.

5 Click **Authenticate**.

6 On the Microsoft Entra authentication screen, enter the account name.

7 Click **Next**.

> **NOTE:** When entering credentials in the Configuration Manager, verify that no other users have used the same credential and that the account you are adding is unique.

8 Enter the password for the account.

9 Click **Sign In**.

10 Enter the verification code sent to the account.

11 Click **Verify**.

The Credential Manager authenticates the account for discovery usage and changes the account information on any applicable discoveries.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

12 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

Changing account names using the Credential Manager

In general, if you want to change an account name, it is recommended that you create a new credential, and delete the old one. However, in the case where you want to replace the credentials in use in a number of places in Enterprise Reporter, the Credential Manager enables you to make a single change and have it be applied across your deployment. For example, if you are provided a new service credential to replace a credential used for a dozen nodes in your environment, you can change the account name on the credential.

If you modify credentials that are used by a discovery node, the node service must be restarted before the changes take effect. Enterprise Reporter will attempt to restart the node. However, if the restart fails, you may need to manually start the service on the computer that hosts the node. If there are jobs currently running on the node, they will be cancelled. To prevent this, either change the credentials during a down time, or cancel the discoveries yourself and restart them once the change takes effect.

To change the account

1 On the System Configuration page, click **Manage credentials**.

It is recommended that you make these changes while no discoveries are running or waiting to be run before changing the account

2 Select the account, and click **Edit**.

3 Modify the account and click **OK**.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

4 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

To change the multi-factor authenticated account

1 On the System Configuration page, click **Manage credentials**.

It is recommended that you make these changes while no discoveries are running or waiting to be run before changing the account.

2 Select the account and click **Edit**.

3 Modify the account.

4 Click **Authenticate**.

5 On the Microsoft Entra authentication screen, if the account has multi-factor authentication enabled, type the account name and password.

> **NOTE:** When entering credentials in the Configuration Manager, verify that no other users have used the same credential and that the account you are adding is unique.

6 Click **Sign In**.

7 Enter the verification code sent to the account.

8 Click **Verify**.

The Credential Manager authenticates the account for discovery usage and changes the account information on any applicable discoveries.

A progress dialog box appears.

> **NOTE:** The Credential Manager displays a Last Authenticated On date, which indicates when the credential was authenticated through the Microsoft authentication process as a multi-factor authenticated credential. If there is no date, then the credential was not authenticated.

9 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

When changing the password on an Microsoft Entra account, any Enterprise Reporter tenant applications using that account must also be reconfigured.

Organizing Reports

My Reports can be organized by creating report categories, and if you are a reporting administrator, you can organize Published Reports. You can then copy reports between containers and categories, or move reports within containers.

See also:

- Working with Report Categories
- Moving Reports
- Copying Reports
- Deleting Reports

Working with Report Categories

You can use categories to group reports together. You can also move and copy categories the same way you do reports.

To create a new category

1 Select the **My Reports** container.

You can also create subcategories by clicking on a category within My Reports.

2 Click **Create** and select **Category**.

3 Type a name and click **OK**.

NOTE: To rename a category, right-click the category and select Rename Category.

To delete a category

1 Select the category to be deleted.

2 Click **Delete**.

3 If a warning is displayed indicating that the category contains sub-categories or reports, click **OK** to accept the warning.

For more information on deleting reports, see Deleting Reports on page 106.

Moving Reports

You can move reports from one category to another within a container.

NOTE: You cannot move reports between containers; you must copy them. For example, if you would like a report from the Published Reports to appear in My Reports, you have to copy it. Dragging between containers automatically copies a report. For more information, see Copying Reports on page 105.

To move a report

1 If necessary, expand the container treeview so the destination category is visible.

2 In the treeview, select the report to move.

3 Drag the report into another category.

- OR -

Right-click the report and click **Cut**, then right-click the desired destination, and click **Paste**.

NOTE: You can also move categories within a container by selecting a category in step 2. When you move a category, all reports in the category are also moved.

NOTE: You cannot move reports to the Report Library from other containers.

Copying Reports

You can copy reports between containers or between categories. You can also copy a report if you want to create variations of the same report: copy the report, and then edit the settings as needed. For more information, see Editing Reports on page 107.

To copy a report

1 Expand the treeview and locate the report you want to copy.

2 Right-click the report and click **Copy**, then right-click the desired destination, and click **Paste**.

- OR -

Drag the report into another container.

NOTE: Any parameter values that have been filled into a report will be included when it is copied.

NOTE: You can also copy categories from one container to another, by selecting a category in step 1. When you copy a category, all reports in the category are also copied.

Deleting Reports

If you no longer need a report, you can delete it. Reports are permanently deleted, so make sure you no longer need the report before deleting it. When you delete a report, you also remove any scheduled instances of the report.

To delete a report

1 In the treeview, select the report and click **Delete**.

- OR -

On the Report card for the report, click **Delete**.

2 In the confirmation dialog box, click **Yes**.

3

Creating and Editing Reports

- Editing Reports
- Creating New Reports
- Report Designer Tips and Tricks
- Publishing Reports
- Integrating with SSRS

Editing Reports

You can modify reports by changing the fields that are included in the report, adding or modifying the report parameters, or changing the layout and appearance of the report. For more information, see Help Finding and Creating Custom Reports on page 8.

You can only edit reports in the My Reports container. If you are a reporting administrator, you may also edit reports in the Published Reports container; however, it is recommended that you copy reports to My Reports for editing.

You may be editing reports for different reasons, for example:

- You have created a new report and need to modify it.
- You are a reporting administrator getting ready to publish reports that are based on reports from the library, and they need tweaking to meet your needs.
- You have a published report to which someone has requested a change.

You can show a preview of the changes you have made to your report to review your edits.

See also:

- Using My Reports
- Changing the report icon
- Modifying the Fields to be Included
- Working with Report Parameters
- Changing the Layout
- Report Modification Example

Using My Reports

My Reports is a container in which you can edit, create, schedule, or publish reports. You choose what reports to include in My Reports. You can:

- Add existing reports for easier access by copying or importing.
- Copy reports to My Reports to edit them for publishing.
  For more information, see Copying Reports on page 105.

- Create a new version of an existing report.
  For more information, see Editing Reports on page 107.
- Create a new report from scratch.
  For more information, see Creating New Reports on page 122.
- Change the report header to use the global icon.
  For more information, see Changing the report icon on page 108.

For more information, see Help Finding and Creating Custom Reports on page 8.

Each installation of the Report Manager has its own unique My Reports container. You can create categories to organize your reports, and move and copy reports between categories.

TIP: Give your reports unique names. When you click My Reports, you see a list of all reports from all categories. Reports with the same name will appear to be listed twice in the card view, and the only way you will be able to differentiate between them is to examine the properties of each report.

NOTE: If you are a reporting administrator and want to make a customized report available to all users, you need to publish it. For more information, see Publishing Reports on page 132.

Changing the report icon

You can change the icon displayed in the header of reports. We recommend using an image that is 300 x 300 pixels. First, configure a global icon, then change the header icon on your reports.

NOTE: Reports that have custom layouts may need to have their layout adjusted to accommodate the custom icon. For more information, see Changing the Layout on page 120.

To set the global report header icon

1. Click the **System Configuration** tab in the Enterprise Reporter Report Manager.
2. Click **Manage report icon**.
3. Click the ellipses to open the file browser.
4. Locate and select the image to be used in report headers and click **Open**.
5. Optionally, select **Use this icon for new reports** to make the icon available on new and copied reports.
6. Click **OK** to save the configuration.

To change a report header icon on selected reports

1. Follow the steps To set the global report header icon.
2. Click the Report tab in the Enterprise Reporter Report Manager.
3. Expand My Reports or Published Reports and select the categories or reports to be updated.
4. Right click anywhere on the selected reports and click **Change Report Icon**.
5. Click **OK** to close the icon change confirmation box.

To change the report header icon on copied reports

1. Follow the steps To set the global report header icon and select **Use this icon for new reports**.
2. Click the Report tab in the Enterprise Reporter Report Manager.
3. Expand the Report Library and select the categories or reports to be copied.
4. Right-click anywhere on the selected reports and click **Copy**.
5. Right-click on My Reports and click **Paste**.
6. Click **Yes** to use the global report header icon for all copied reports.
7. Click **OK** to close the icon change confirmation box.

Modifying the Fields to be Included

You can add and remove fields from a report. Fields are organized by report type; a report can only contain fields from one report type. You cannot change the report type of a report. Each report type includes information from various related tables in the Reporter database. Some report types can be extended. By extending a report type, more fields are available to be added to your report. Typically, only a subset of the available fields are included in each report. You can add or remove fields to suit your needs.

NOTE: Each report may have a layout that defines how the fields are displayed, including the positioning, grouping and sorting. When you modify the included fields, the layout is not automatically updated. For information on modifying the layout, see Changing the Layout on page 120 and Report Designer Tips and Tricks on page 126.

You can implement some functions when choosing the fields, or when designing the report layout. For example, you can set sort ordering when you include the field in a report, or you can set it using the report layout. The difference between the two methods is where the action occurs. If you configure the fields, the action is carried out on the database before the report is generated. If you configure the report layout, the action is carried out as the report is generated. You might notice a performance increase if you configure the fields instead of the report layout.

By default, Enterprise Reporter collects a base set of attributes for each type of object. Your discovery administrator has the ability to extend some attributes in the Configuration Manager, and these are noted as (extended) after the field name in the Report Manager. They can be added to a report as usual, and you will find them in the report type associated with the object on which you are reporting. If you have requested that an attribute be collected, you need to restart your Report Manager in order to see the new fields in the report type.

You may also extend some report types to include additional fields for account objects. For example, in an NTFS report, you may want to see additional domain user fields that are collected by an Active Directory® discovery. You can accomplish this by adding account objects to the report type. The available types of account objects you can add are:

- Domain User
- Domain Group
- Local User
- Local Group

You may also extend some report types to include additional fields for identity objects. For example, in a OneDrive report, you may want to see additional Azure user fields that are collected by an Microsoft Entra discovery. You can accomplish this by adding identity objects to the report type. The available types of identity objects you can add are:

- Entra Contact
- Entra Group
- Entra User

When editing a report, in the Available Fields area, the option to extend the report type is indicated by a special folder icon next to object names underlined in blue. You can right click the object names to see the available type of account or identity objects that can be added. For detailed steps on extending the report type, see To extend a report type on page 110.

You can set the sort order for each field on this page as well. This sorts the fields in the database before reporting them. Sort order is important in determining what the report output looks like. The first sorted field is the primary sort, the second field is the secondary sort and so on. For example, if you sort ascending on Server Name, Instance Name, and Database Name then arrange the fields in that order, your results are returned like this:

Server A

Instance A

Database A

Database B

Database C

Instance B

Database A

Database B

Database C

Server B

Instance A

and so on.

See also:

- Performing Calculations Within a Report
- Indicating Data Age on a Report

To add and remove report fields

1. In My Reports, select the report, then click **Edit report**.
2. If necessary, rename the report to reflect your changes.
3. Click **Fields**.
4. In the Available Fields area, select any fields you want to add, and click **Add**.

   You can multiselect fields using the Ctrl key.

   The first time you modify fields in any editing session (add, remove, or right-click operations), a warning appears, explaining that the report layout is not automatically updated. For information on updating the layout to reflect your changes, see Changing the Layout on page 120 and Report Designer Tips and Tricks on page 126.
5. Click **OK** to continue.

   You cannot change the report type.
6. In the Selected Fields area, select any fields that you want to remove and click **Remove**.

To set the sort order of fields

1. In Selected Fields, drag the fields as required.

   You cannot move unsorted fields above sorted fields.
2. Right-click the field and select Sort Ascending or Sort Descending.

   To remove sorting, choose No Sorting.

To extend a report type

1. In the Available Fields area, right-click any object underlined in blue.
2. To add fields to the report type, select the objects you want and click **OK**.

   The new objects will appear in the Available Fields list.
3. Scroll down to see the new objects and expand them to see the additional fields.
4. Update the selected fields by clicking the **Add** and **Remove** options as usual. For more information, see To add and remove report fields on page 110.

Performing Calculations Within a Report

You can also apply an aggregate to certain fields. Aggregates provide summaries of the available rows and columns of collected data in the Reporter database. Depending on the type of field you are working with, the available aggregates are:

Table 35. Available Aggregates

Aggregate	Description
Average	Available for numeric fields, and averages all values in that field
Count	Counts each incidence of the selected field. For example, counting the version number would tell you the number of times each version number appeared.
Distinct Count	Counts each unique incidence of the selected field. For example, applying a distinct count to version number would tell you how many different versions you found.
Distinct Maximum	Returns the unique largest value for the selected field.
Min	Returns the smallest value for the selected field
Max	Returns the largest value for the selected field
Sum	Adds up the values in the selected field

To add an aggregate to a numeric field

- Right-click the field and select the aggregate

Indicating Data Age on a Report

Data in your reports may be drawn from different discoveries (for more information, see Editing Reports on page 107). This means that the freshness of your data may vary within a report. If it is important to understand when the data was collected, you can add this information to each top level object collected. The following table outlines where you can add this time stamp:

NOTE: If you want to know the last time a value changed, you can add the Timestamp field.

Table 36. Where to add the Last Collected Time for each Report Type

Report Type	Last collected time available for...
Active Directory	Domain
Microsoft Entra ID	Tenant
Azure Resource	Tenant
Computer	Computer
Exchange	Organization
Exchange Online	Tenant
Microsoft SQL Server	SQL Server
Microsoft Teams	Tenant
NTFS	Computer on which the folder, share, or file is located Shares on each computer
OneDrive	Tenant
Registry	Computer on which the registry is located
SharePoint Online	Tenant

To add the last collected time to a report

1. Ensure you are working in the My Reports container.
2. Select the report, and click **Edit report**.
3. Click **Fields**.
4. If necessary, expand the appropriate container.

5 Add **Last Collected Time**.

Remember that you must add the field to the Layout if you want it to appear in your report. For more information, see Changing the Layout on page 120 and Report Designer Tips and Tricks on page 126.

Working with Report Parameters

When you collect data in Enterprise Reporter, all data from the target is collected. To create meaningful reports, this data must be filtered, sorted and organized for specific needs. Parameters are used to filter the data.

When you add multiple parameters to a report definition, you can also group parameters to further filter the information included in a report. Each group supports a single AND or OR operator.

- An example of an inclusive grouping (joined with AND)
  - (Type of Account equals User) **AND** (Account Name starts with P)
- An example of an exclusive grouping (joined with OR)
  - (Account Name starts with P) **OR** (Account Name starts with S)

You can further connect groups with AND or OR operators to create even more complex filtering.

- For example,
  - [Domain Name includes CA]

    AND

    [(Domain User Expiration Date is in the past 29 days) **OR**
    (Domain User Expiration Date is in the next 15 days)]

  would include information that matches the criteria from the first group OR the second group.

Only one child level of grouping is supported.

- For example,
  - [(Type of Account equals User) **AND**
    ((Account Name starts with P) **OR** (Account Name starts with S))]

    OR

    [(Type of Account equals Group)]

  has nested groups and is unsupported.

See also:

- What is a Parameter?
- Types of Parameters
- Parameter Operators
- Custom Query Data Types
- Working with Parameters

What is a Parameter?

A parameter consists of the following:

Table 37. Parameter Elements

Element	Description
Prompt	• Appears as the title of the parameter when running the report. You configure this prompt to explain to the report user what the intention of the parameter is. It should clearly convey the values the user needs to enter. • A prompt is required for Optional and Required parameters. For more information on parameter usage, see Types of Parameters on page 113. • The maximum size for a prompt is 128 characters. • Sample prompts: Choose the start and end date for the data in your report. Enter the names of all domains you want to include.
Field	• The field that will be queried by the parameter. • Within a report, you can set as many parameters as you need to get the information you are looking for. You can create multiple parameters for the same field. • For more information on choosing the fields to include in your report, see Modifying the Fields to be Included on page 109.
Condition Operator	• Sets the basis for the conditions that will be set to filter the available data. • The operators available vary depending on the field. For a list of operators, see Parameter Operators on page 114. • Examples of operators: Includes, Equals, Between.
Default Value	• These values are presented when the report is run, and the user can choose to run the report using the default values, or to change the values to anything they want. • For Optional and Required parameter types, you can choose to create a default value, or list of values, depending on the operator. • Default values are required for Hidden parameters. • The form of these values is determined by the field and operator. For example, a date takes the form dd/mm/yyyy. Some operators allow you to create lists or ranges. You must enter values in the correct form before you can finish creating the parameter.

Types of Parameters

There are three types of parameters that you can create. By paying careful attention to choosing the proper parameter type, you can ensure that you get the right balance of user interaction and preset information, and that your report serves its intended purpose. Each type of parameter has to have specific elements in order to be accepted.

NOTE: If you do not enter everything required for a particular type of parameter button, the OK button will be unavailable.

Table 38. Parameter Usage Requirements

Parameter usage	When creating the parameter	When using the parameter to run the report
Required	You must provide a prompt explaining the user input required when running the report. You can choose to supply a default value to the user, who can use that value or change it.	You cannot run the report unless this parameter is given a value.
Optional	You must provide a prompt explaining the user input required when running the report. You can choose to supply a default value to the user, who can use that value or change it.	You can run the report with or without a value.
Hidden	You must provide a default value. This value will be used when the report is run. You do not need to provide a prompt.	The user running the report does not see this parameter in the parameter card list.

Parameter Operators

The operators that are available for use depend on the data type of the field you are working with. The following table outlines the operators available.

Table 39. Parameter Operators

Operator	Description	Data types
Between	Returns all data between the two values you provide. For example, if you choose a field that contains text, and search between A and C, it will return all values that start with the letters A, B and C.	String Number Date
Contains	Returns all data containing the value you provide. The value can be found anywhere within the field. For example, if you enter AN, as long as that sequence of letters is found anywhere in the field, the data is returned. This is a very flexible operator. Many of the operations you can do with Contains can also be done using other operators. It is primarily intended for use with wildcard characters. Supported characters (for strings only): • *, which replaces any number of characters • ?, which replaces a single character. Returns all data that matches the combination of text and wildcard characters that you provide. For example: • Fin* returns all data that starts with Fin, and has any number of characters after it. (For this case, you could also use the Starts with operator) • Fin? returns anything that starts with Fin and has a single additional character. • *Finance returns any data that ends with Finance. (For this case, you could also use the Ends with operator) • *Finance* returns any data that has Finance anywhere in the field. (For this case, you could also use the Contains operator.) • F*e excludes any value that starts with F and ends with e.	String

Table 39. Parameter Operators

Operator	Description	Data types
Does not Contain	Returns all data except those containing the value you provide. For example, if you enter AN, if that sequence of letters is found anywhere in the field, the data is not returned. You can use wildcard characters in the same manner as Contains.	String
Does not end with	Returns all data except that ending with the value that you provide.	String
Does not start with	Returns all data except that starting with the value that you provide.	String
Ends with	Returns all data that end with the value you provide.	String
Equals	Returns only the data that exactly matches the value you provide. Equals is not case sensitive.	String Number GUID Boolean Date
Equals with group expansion	Enter an Account Name. Results include the data for the selected account as well as the data for any group of which it is a direct or indirect member. For example, if an account is a member of Group A and Group A is a member of Group B, the results will include values/data for the account as well as Group A and Group B.	Account Name attribute Identity unique display name attribute
Excludes	You provide a list of values. Returns all values except those matching your list. This acts as an OR when joining the list you provide—it returns data that does not match any one of the values. For example, if your Excludes list is Austin, Dallas and Houston, if a field includes any of the values, the data will not be returned. The Excludes operator also acts like an OR with numbers (integers). For example, use it to exclude NTFS folder level 1 OR folder level 4 OR folder level 5. However, to exclude NTFS folders up to folder level 5, use the operator **Less than or equal to**. Supported wildcard characters (for strings only): • [*], which replaces any number of characters • [?], which replaces a single character. Wildcard characters must be surrounded by square brackets. For a full explanation of the use of these wildcard characters, see Contains on page 114.	String Number Date
Greater or equal to	Returns all data larger than and including the value you provide.	String Number Date
Greater than	Returns all data larger than the value you provide.	String Number Date

Table 39. Parameter Operators

Operator	Description	Data types
Has a value	Has two possible values: True or False. If you choose True, returns all data where the field is populated. If you choose False, returns all data where the field is empty.	String Number Boolean Date
In the next	Enter a number of days. Returns data with a date range from the date and time you run the report to the number of days in the future that you enter. For example, if you run the report at 16:30 on December 12, and you enter six days, you will get data with the dates from December 12 at 16:30 to December 18 at 16:30.	Date
In the past	Enter a number of days. Returns data with a date range from the date and time you run the report to the number of days in the past that you enter. For example, if run the report at 16:30 on December 12, and you enter six days, you will only get data with a date from December 6 at 16:30 to December 12 at 16:30.	Date
Includes	You provide a list of values. Returns all values that match any item on your list. This acts as an OR when joining the list you provide—it returns data that does not match any one of the values. For example, if your Includes list is Austin, Dallas and Houston, if a field includes any of the values, the data is returned. The Includes operator also acts like an OR with numbers (integers). For example, use it to include NTFS folder level 1 OR folder level 4 OR folder level 5. However, to include NTFS folders up to folder level 5, use the operator **Less than or equal to**. Supported wildcard characters (for strings only): • [*], which replaces any number of characters • [?], which replaces a single character. Wildcard characters must be surrounded by square brackets. For a full explanation of the use of these wildcard characters, see Contains on page 114.	String Number Date
Less than	Returns all data smaller than the value you provide.	String Number Date
Less than or equal to	Returns all data smaller than and including the value you provide.	String Number Date
Matches	You select two fields. Returns only the data where the contents of one field is identical to the other field. Matches is not case sensitive.	String GUID
Not between	Returns all data that is not between the two values you provide. For example, if you choose a date field, and set the values to not between December 10, 2011 and January 15, 2012, you will get all corresponding data from December 10 and before, and January 15 and after. You must enter the lower value first, followed by the higher value.	String Number Date

Table 39. Parameter Operators

Operator	Description	Data types
Not equals	Returns all data except for the value you provide.	String Number Date Boolean GUID
Not in the next	Enter a number of days. Returns all data except for the time period from the date and time you run the report to the number of days in the future that you enter. For example, if you run the report on December 12 at 16:30, and you enter six days, you will get all data except that with a date from December 12 at 16:30 to December 18 at 16:30.	Date
Not in the past	Enter a number of days. Returns data with any date except for the time period from the date and time you run the report to the number of days in the past that you enter. For example, if you run the report at 16:30 on December 12, and you enter six days, you will get all data except that with a date of December 6 at 16:30 to December 12 at 16:30.	Date
Starts with	Returns all data that starts with the value you provide.	String

Custom Query Data Types

The Enterprise Reporter Report Library contains many reports generated by custom queries. This table outlines the data types used in the Report Library custom queries and the operators supported for each of them. The equals operator returns only data that exactly matches a provided value, so wildcard parameters are not supported for custom query reports in the Report Library. When creating your own custom query reports, the query you write defines whether or not parameters with wildcard characters will be handled.

Table 40. Custom Query Data Types

Data Type	Description	Supported Operators
int	Holds signed 32-bit (4-byte) integers that range in value from -2,147,483,648 through 2,147,483,647. Use int to select the top ‘n’ records to limit the results of a report.	Equals
datetime	Defines a date that is combined with a time of day with fractional seconds that is based on a 24-hour clock. Use datetime to select records modified between two dates.	Equals
nvarchar [(n | max)]	The NVARCHAR data type is variable-length Unicode string data. n defines the string length and can be a value from 1 through 4,000. max indicates that the maximum storage size is 2^31-1 bytes (2 GB). The storage size, in bytes, is two times the actual length of data entered + 2 bytes.	Equals
table	A special data type that can be used to store a list of nvarchars. Use table to supply multiple values (such as a list of computer names) for a single parameter.	Includes
varchar [(n | max)]	The VARCHAR data type is variable-length string data. n defines the string length and can be a value from 1 through 4,000. max indicates that the maximum storage size is 2^31-1 bytes (2 GB).	Equals

Working with Parameters

To create a parameter

1 Select the report, then click **Edit report**.

2 Click **Parameters**.

3 Click **Add**.

4 In the Usage section, choose the parameter type.

5 If your parameter is a Hidden parameter, skip this step. In the Field section, in the Prompt text box, type a prompt.

Make sure your prompt provides the report user with enough information to properly run the report.

6 In the Field section, select the field for the parameter.

You can choose from any field included in the reporter. You can create more than one parameter per field.

7 In the Parameter Properties section, choose an operator.

8 If desired, select **Supply a default value**, and enter the value.

This step is necessary if you created a Hidden parameter in step 4.

9 Click **OK** to close the Edit Report Parameter dialog box.

10 Click **OK** to close the Edit Report Definition dialog box.

To edit a parameter

1 Select the report, then click **Edit report**.

2 Click **Parameters,** and select the parameter.

3 Click **Edit**.

4 Make changes as needed, and click **OK** to close the Edit Report Parameter dialog box.

5 Click **OK** to close the Edit Report Definition dialog box.

To delete a parameter

1 Select the report, then click **Edit report**.

2 Click **Parameters,** and select the parameter.

3 Click **Delete**.

4 Click **Yes** to confirm the deletion.

5 Click **OK** to close the Edit Report Definition dialog box.

To group parameters

1 Select the report, then click **Edit report**.

2 Click **Parameters.**

3 Press CTRL and select the parameters to be grouped.

> **NOTE:** To include a parameter in an existing group, you must first ungroup the existing group, and then select all of the parameters to be included in the group.

4 Click the Group button.

5 Click **OK** to close the Edit Report Definition dialog box.

To ungroup parameters

1 Select the report, then click **Edit report**.

2 Click **Parameters.**

3 Press **CTRL** and select the parameters within a group that are to be ungrouped.

4 Click the **Ungroup** button.

5 Click **OK** to close the Edit Report Definition dialog box.

To change the operator between parameters

1 Select the report, then click **Edit report**.

2 Click **Parameters**.

3 Click a parameter outside of a group to change all of the operators outside of groups (including the operators between groups).

- OR -

Click a parameter within a group to change all of the operators for that group.

For more information, see Working with Report Parameters on page 112.

4 Click the **AND/OR** button to change the operator from AND to OR or vice versa.

5 Click **OK** to close the Edit Report Definition dialog box.

Creating or Editing an Expand Nested Groups Parameter

Some reports support adding a parameter that allows you to expand nested group members and specify how they are displayed in the report. Some reports already contain this parameter which can be edited.

To create an Expand Nested Groups parameter

1 Select the report, then click **Edit report**.

2 Click **Fields**.

3 In the Available Fields area, select the Expand Nested Groups field, and click **Add**.

4 Click **Parameters**.

5 Click **Add**.

6 In the Usage section, choose the parameter type.

7 If your parameter is a Hidden parameter, skip this step. In the Field section, in the Prompt text box, type a prompt.

Make sure your prompt provides the report user with enough information to properly run the report.

8 In the Field section, select the field Expand Nested Groups.

9 In the Parameter Properties section, select the Equals operator.

10 If more fields for the nested group members are desired, select Supply a default value.

11 Optionally, select a default value from the pull down menu.

12 Optionally, click **Add Fields** to add more fields for nested group members. For more information on adding fields, see To add more nested group member fields when running a report on page 82.

13 Click **OK** to close the Edit Report Parameter dialog box.

14 Click **OK** to close the Edit Report Definition dialog box.

To edit an Expand Nested Groups parameter

1 Select the report, then click **Edit report**.

2 Click the **Parameters** tab.

3 Select the Expand Nested Groups parameter.

4 Click **Edit**.

5 In the Usage section, choose the parameter type.

6 If your parameter is a Hidden parameter, skip this step. In the Field section, in the Prompt text box, type a prompt.

Make sure your prompt provides the report user with enough information to properly run the report.

7 In the Field section, select the field Expand Nested Groups. For more information on selecting available fields, see Modifying the Fields to be Included on page 109

8 In the Parameter Properties section, select the Equals operator.

9 If more fields for the nested group members are desired, select Supply a default value.

10 Optionally select a default value from the pull down menu.

11 Optionally click **Add Fields** to add more fields for nested group members. For more information on adding fields, see To add more nested group member fields when running a report on page 82.

12 Click **OK** to close the Edit Report Parameter dialog box.

13 Click **OK** to close the Edit Report Definition dialog box.

Changing the Layout

If you add or remove fields to or from your report and the report has a layout, you will need to verify that the layout is still appropriate. You may also want to modify the layout to suit your own preferences.

TIP: You should always back up your report by making a copy before modifying the layout. You cannot undo changes to a layout once you have clicked OK in the Edit Report dialog box.

If you have date and time fields in the report, you might want to add your local time zone to the report layout. When date and time data is collected, it is stored in local time. When a report is run, the time is expressed in the time zone of the console running the report. For example, if a user in New York City logged on at 4:15 pm, but the report was run in Los Angeles, which is three hours behind, the report will show that user logging in at 1:15 pm.

The Layout is modified using the Report Designer from DevExpress. You may change the layout manually, import a layout from an existing report, or auto-generate a layout. For more information, see Report Designer Tips and Tricks on page 126 or the Report Designer User Guide (Developer Express), located in the folder where you installed the Quest Enterprise Reporter Report Manager.

To modify the layout of a report

1 Click **My Reports**.

- OR -

Expand **My Reports** and select the category containing the report.

If you are a reporting administrator, you can also edit reports in Published Reports; however, it is recommended that you copy the report to My Reports for editing.

2 In the treeview, select the report you want to edit.

3 From the menu options, under Manage Report, click **Edit report**.

4 Select the **Layout** tab.

5 Click **Edit** to open the Report Designer.

If you would rather start from a blank layout, and create a new layout, click **Design New**.

6 To add any parameter (such as the time zone) to your report, in the Report Designer, click **Field List**, expand the parameters container, and drag the parameter (for example, TimeZone) to the appropriate location on the report.

7 Make any additional changes to the layout.

For details on using the features of the Report Designer, see Report Designer Tips and Tricks on page 126 or the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

8 Optionally, click **Show preview** to generate a sample of the report to review the edits.

9 Click **OK** to close the Report Definition dialog box.

To import the layout of an existing report

1 Click **My Reports**.

- OR -

Expand **My Reports** and select the category containing the report.

If you are a reporting administrator, you can also edit reports in Published Reports; however, it is recommended that you copy the report to My Reports for editing.

2 In the treeview, select the report you want to edit.

3 From the menu options, under Manage Report, click **Edit report**.

4 Select the **Layout** tab.

5 Click **Import layout**.

6 Select the report containing the layout to be imported and click **OK**.

7 Using the report editor, ensure that the fields imported in the layout match the data to be displayed in the report and make any additional changes to the layout and click **OK**.

For details on using the features of the Report Designer, see Report Designer Tips and Tricks on page 126 or the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

8 Optionally, click **Show preview** to generate a sample of the report to review the edits.

9 Click **OK** to close the Report Definition dialog box.

To use the Report Wizard to generate a new layout for the report

1 Click **My Reports**.

- OR -

Expand **My Reports** and select the category containing the report. In the treeview, select the report you want to edit.

If you are a reporting administrator, you can also edit reports in Published Reports; however, it is recommended that you copy the report to My Reports for editing.

2 From the menu options, under Manage Report, click **Edit report**.

3 Select the **Layout**.

4 Click **Auto-generate** to start the layout wizard.

5 Step through the wizard.

For more information, refer to the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

6 Once you have completed the wizard, click **OK** to close the Report Definition dialog box.

7 Optionally, click **Show preview** to generate a sample of the report to review the edits.

Report Modification Example

The following example walks you through all of the steps necessary to modify a report.

Example: You want to modify the SQL Database report to only display databases from SQL Servers® running SQL Server® 2008. The report in the library does not include the version in it, so you will need to add that field to the report. You are going to change the title to reflect this, so you do not need to include the version for each database. This means you will use a hidden parameter for the version, and filter the data to show only the version you choose.

To modify your SQL Database report

1. Copy the SQL Databases report from the Report Library to My Reports.
2. In the My Reports treeview, select the report.
3. Click **Edit Report**.
4. Change the title of the report to **SQL Server 2008 Databases**.
5. Click the **Fields** tab, and add the Version field to the report.

   Click **OK** in the warning dialog box. Because we do not want this field to show on the report, no layout modification is necessary. If you want to display the new field, you must add the field to the layout. For more information, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.
6. Click the **Parameters** tab and click **Add**.
7. Set the Usage to **Hidden**.
8. In the Select the field to associated with this parameter list, click **Version**.
9. In the Parameter Properties area, set the condition operator to **Contains**.
10. Select the SQL Server version you want (for example, SQL Server 2008 is version 10.0).
11. Click **OK**.
12. Optionally, click the **Layout** tab and click **Show preview** to generate a sample of the report to review the edits.
13. Click **OK** in the Edit Report Definition dialog box.

Creating New Reports

If you are unable to get the information you want by modifying an existing report, you can create a new report from scratch. In cases when you cannot get the information you want by creating reports from existing fields and operators, or when you need to transform the data, you can use a custom query report.

> **CAUTION: Custom query reports allow you to run code that is compiled and run when the report is generated. To avoid any security breaches, ensure you have properly secured your SQL Server® and database.**

For additional information, see Help Finding and Creating Custom Reports on page 8.

See also:

- Creating Report Layouts
- Setting CSV File Export Options
- Exporting and Importing Report Definitions

To create a new report

1. Select **My Reports** or a container within My Reports.

   If you intend to publish this report, you should still create it in My Reports, and ensure it works as anticipated before publishing the report. For more information, see Editing Reports on page 107.

2 Click **Create** | **Report**.

3 On the General page, enter a report name, author and description.

These are searchable fields, so provide consistent information in your reports to make them easy to find.

4 Click the **Fields** tab.

5 Click the **Report Type** text box and navigate through the categories to select the Report Type that contains the fields you want in your new report.

You can only select fields from one report type.
For an overview of report types, see Report Types Included in Enterprise Reporter on page 59.

6 Select the fields to display in your report, and click **Add**.

7 To sort on a field or apply an aggregate, right-click the field and choose the option from the menu. For more information, see Modifying the Fields to be Included on page 109.

8 Click the **Parameters** tab.

9 Click **Add** to create the required parameters. For more information, see Working with Report Parameters on page 112.

10 Click the **Layout** tab.

11 Optionally, click **Auto-generate**, **Design new**, or **Import layout** to create a report layout.

For more information, see Creating Report Layouts on page 124, Changing the Layout on page 120 and Report Designer Tips and Tricks on page 126. For a full explanation of report layouts, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

The Query page shows you the query that will be used to generate your report.

12 Optionally, click **CSV Options** tab and set the CSV export options for this report.

For more information, see Setting CSV File Export Options on page 125.

13 Click **OK** to close the Report Definition dialog box.

The report is listed in the location you selected in step 1.

To create a custom query report

1 Select **My Reports** or a container within My Reports.

If you intend to publish this report, you should still create it in My Reports, and ensure it works as anticipated before publishing the report. For more information, see Editing Reports on page 107.

2 Click **Create** | **Custom Query Report**.

3 On the General page, enter a report name, author and description.

These are searchable fields, so provide consistent information in your reports to make them easy to find.

4 Click the **Query** tab.

5 In the Report Query text box, type or paste your query.

You can use any query writing tool to generate the query, then copy it and paste it here.

> **NOTE:** The query you write defines whether or not parameters with wildcard characters will be handled.

6 Click **Validate Query**, then click **OK**.

If necessary, resolve any issues and validate your query again.

7 Optionally, on the Parameters page, create the required parameters. For more information, see Working with Report Parameters on page 112.

If your custom query contains at least one declare parameter (such as Declare @p nvarchar(128)), the Parameters page will be available.

NOTE: Wildcard character support will only be available if the query was written to handle it.

8 Optionally, on the Layout page, create your report layout.

For more information, see Creating Report Layouts on page 124 and Changing the Layout on page 120 and Report Designer Tips and Tricks on page 126. For a full explanation of report layouts, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

9 Optionally, on the CSV Options page, set the CSV export options for this report.

For more information, see Setting CSV File Export Options on page 125.

10 Click **OK**.

The report appears in the location you selected in step 1.

Creating Report Layouts

The report layout determines the how information is grouped, sorted, and displayed in a report. Report layouts are optional; however, reports without a layout may only be exported in CSV format.

There are three ways to create a new layout for a report. 1) You can start from scratch, and manually place fields and text labels, set sorting and grouping and so on. 2) You can import a layout from an existing report. 3) Layouts can be auto-generated using the Report Wizard. By stepping through the six steps in the wizard, you can easily generate a layout that includes the relevant fields in a useful manner:

- Step 1 - Choose Columns to Display in Your Report
- Step 2 - Add Grouping Levels
- Step 3 - Summary Options
- Step 4 - Choose Report Layout
- Step 5 - Choose Report Style
- Step 6 - Enter a Report Title

For a full explanation of the creating new layouts, refer to Report Designer Tips and Tricks on page 126 and the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

To create a new report layout using the Wizard

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

For more information, see Editing Reports on page 107.

2 Click **Auto-generate**.

3 Step through the wizard.

For more information, see Report Designer Tips and Tricks on page 126 and the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

4 Once you have completed the wizard, click **OK** to close the Report Definition dialog box.

To import a layout from an existing report

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

For more information, see Editing Reports on page 107.

2 Click **Import layout.**

3 Select the report containing the layout to import.

4 Using the report editor, ensure that the fields imported in the layout match the data to be displayed in the report.

   For details on using the features of the Report designer, see Report Designer Tips and Tricks on page 126 and the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

5 Click **OK**

To create a new report layout from scratch

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

   For more information, see Editing Reports on page 107.

2 Click **Design a new.**

   For details on using the features of the Report designer, see Report Designer Tips and Tricks on page 126 and the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

3 Click **OK**.

Setting CSV File Export Options

The definition for each report contains options that are applied when exporting the report to a CSV file. You may edit the following options to tailor the CSV file output to meet your needs:

- select fields to export
- edit display names of fields
- sort fields in the export
- control column headers

For more information on how to export reports to raw, unformatted CSV files, see Running Reports or Exporting Reports to CSV and Other Formats from Different Containers on page 78.

To set CSV file export options

1 Click **My Reports**.

   - OR -

   Expand **My Reports** and select the category containing the report. In the treeview, select the report you want to edit.

   If you are a reporting administrator, you can also edit reports in Published Reports; however, it is recommended that you copy the report to My Reports for editing.

2 From the menu, under Manage Report, click **Edit report**.

3 Click the **CSV Options** tab.

4 Optionally, select the fields to export using the **Include** column.

5 Optionally, click any **Display Name** to edit it.

6 Optionally, sort the order of the fields output to the CSV file by selecting any cell in the table and using the up and down arrows to arrange the fields.

7 Optionally, clear the **Include column headers in exported file** option to suppress column headers.

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

Exporting and Importing Report Definitions

There are a two ways to move reports between consoles: you can publish a report, which makes it available to all users of the server, or you can export a report definition, and then import it to a specific console. You can export a single report or an entire category of reports with all of its child categories and their reports. You will have the option to include the related parent report categories so that you can retain your report groupings for future imports. Choosing this option will include the parent category hierarchy without any of the parent category reports. When you export a report, all report settings are stored, including the report name, fields, parameter settings, filters, report layout and any queries. The report definition is saved in your chosen folder, with the extension .xrd. If you save the related report categories in your export, an archive file is saved with the extension .xrp. To import the reports, either to another category in your console, or to another console, make the .xrd file or the .xrp file available.

NOTE: Report names can contain characters, such as \ or %, that cannot be used in filenames. In this case, when the exported file is saved, Reporter replaces those characters with underscores.

To export report definitions

1. Select the reports or categories to export.
2. Click **Export**.
3. In the Browse for Folder dialog box, navigate to a destination folder and click **OK**.
4. Click **Yes** to include the related report categories in the export.

   Choosing this option will include the parent category hierarchy without any of the parent category reports.
5. If an archive file with the same name already exists in the selected destination, a confirmation dialog box appears. Click **Yes** to overwrite the archive file.
6. If a report with the same name already exists in the selected destination, a confirmation dialog box appears. Click **Yes** or **Yes to All** to replace duplicates.
7. Click **OK**.

To import report definitions

1. Select the destination container or category.
2. Click **Import**.
3. In the Open dialog box, navigate to the folder containing the report definition files (.xrd or .xrp).
4. Select the reports, and click **Open**.

   If a report with the same name already exists in the selected container or category, a confirmation dialog box appears. Choose Replace or Replace All to replace the report, or choose Create a new copy and the imported report will be renamed by adding an incremental number in brackets after the report name.

Report Designer Tips and Tricks

The Report Manager provides access to the Report Designer, which allows you to modify an existing report layout or to create a new report layout. The following section provides some simple tips and tricks for using the Report Designer Tool.

For detailed information on accessing the layout designer tool, see Changing the Layout on page 120 and the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

The Report Designer Tool contains the following elements, which will be referred to in the following sections:

- Designer window
- Preview window
- Script window

- Toolbox
- Report Explorer tab
- Fields List tab
- Property Grid panel

See also:

- Report Bands
- Binding a Data Field to a Control
- Adding a Parameter Field to a Report Layout
- Adding a New Grouping to a Report Layout
- Adding a New Column to a Table
- Formatting Rules: Hiding or Showing a Field Based on Data Values
- Creating a Calculated Field
- Creating a Script to Run with a Report

Report Bands

When the layout designer is first opened, you are provided with a standard report layout template. A report layout contains report bands. Bands are report sections that can be printed once in a report (report header and footer), on each report page (page header and footer), for each data entry (detail band), for each data group (group header and footer).

The Detail Band is the central part of a report. Unlike other report bands, you cannot delete this band. The contents of the Detail band are repeated for every data entry produced by the report query.

The template provided in the Report Manager contains the following bands:

- Report Header (one band per report)
- Page Header (one band per page)
- Main Group Header
- Group Header 2
- Group Header 1
- Detail Header
- Detail Band
- Group Footer 1
- Page Footer (one band per page)

Controls can be added to each band. Some of the standard types of controls available are as follows:

- Label
- Check box
- Rich Text
- Picture Box
- Panel
- Table
- Line
- Shape

- Chart

Each control has multiple properties that can be updated using the Property Grid. Properties related to appearance, behavior, layout, and data can be set and edited. For full information on each property, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

Binding a Data Field to a Control

When modifying or creating a report, you may need to display the contents of a database field at a specific location within the report. To control how, where and when the database field is displayed, you must use the Report Designer Tool to select an appropriate type of control then bind the data field to that control.

For this example, we will edit an existing report and bind a field to a rich text control. The same process can be used for most controls – labels, rich text, table cells, and so on.

For more information on data binding, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

To bind a data field to a control

1 In My Reports, select the report, then click **Edit report**.

2 To edit the existing layout, click the **Layout** button, then click the **Edit** button.

For more information, see Changing the Layout on page 120.

3 From the Toolbox, drag the Rich Text control to the location where the database field is to be displayed on the report.

Rulers and grid lines are available to help you align the control with other controls on the report.

4 Click the control in the report and use the options in the Property Grid to adjust properties such as font, size and color.

5 With the control still selected on the report, click the **Fields List** tab and expand the Table folder under dataSet1.

Every database field that has been added to your report on the Fields tab will be displayed. For more information on adding fields to your report see Modifying the Fields to be Included on page 109.

Click the database field to be bound to the rich text control and drag it on top of the rich text control on the report.

- OR -

With the control still selected on the report, navigate to the Data section of the Property Grid. Expand **Data Bindings | Rtf** and click the **Binding** drop-down arrow and select the field to be bound to this control.

Adding a Parameter Field to a Report Layout

Each parameter of a report is included in the Field List and can be added to the layout of that report.

To add a parameter field to your report

1 In the Report Designer, click the **Field List.**

2 Expand the **Parameters** node.

3 Drag the parameter (for example, TimeZone) to the appropriate location on the report.

Adding a New Grouping to a Report Layout

Groupings are set in a report layout using group bands. Each group band needs to be configured with applicable settings to group the information in your report in a meaningful manner.

To add a new grouping to a report layout

1. In My Reports, select the report, then click **Edit report**.
2. To edit the existing layout, click the **Layout** button, then click the **Edit** button.

   For more information, see Changing the Layout on page 120.
3. In the Designer pane, right-click the location on the report where you want to insert a grouping header.
4. Click **Insert Band** and click **Group Header** to create a group header band.
5. Click the group header band and click on the **>** icon to open the Group Header Tasks dialog box.
6. Click ▪▪▪ next to Group Fields to display the Group Field Collection Editor.
7. Click **Add** to add a new group field to the collection.
   In the Group Field properties panel, click the **Field Name** drop-down arrow and select the data field for grouping.

   Repeat this step for each level of grouping required.
8. Click **OK** to save the grouping collection.
9. Optionally configure group header settings such as **Keep Together** and **Repeat Every Page** to control how the groupings are displayed in the report.

Adding a New Column to a Table

When creating or modifying a report, there are many instances where you will want to edit a table. The default report template has tables created in each band.

To add new cells to a table

1. In My Reports, select the report, then click **Edit report**.
2. To edit the existing layout, click the **Layout** button, then click the **Edit** button.

   For more information, see Changing the Layout on page 120.
3. Click the band that contains the table control to be edited.
4. Click the table.
5. Right click and select **Insert | Column To Right**.

   - OR -

   Right click and select **Insert | Column to Left**.
6. Click the new column.
7. In the Property Grid, set the applicable properties.
8. To bind the new column to a data field, select the data field from the Fields List tab and drag it on top of the column.

   For more information, see Binding a Data Field to a Control on page 128.

Formatting Rules: Hiding or Showing a Field Based on Data Values

This advanced option is used when you want to control the display of data based on the value of the data. For example, if the value of the data to be displayed in a field is null, you may wish to suppress it. There are many other formatting rules that can be applied based on the value contained in the data. For more information, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

In this section, we are going to illustrate formatting rules using an example of hiding/showing a table cell control based on a data value.

To hide or show a field based on data values

1. In My Reports, select the report, then click **Edit report**.
2. To edit the existing layout, click the **Layout** button, then click the **Edit** button.

   For more information, see Changing the Layout on page 120.
3. Click the table cell in the report that is to be shown or hidden based on the value of the data it contains.
4. On the Property Grid, scroll to the Appearance section and click the **Formatting Rules** property.
5. Click ▪▪▪ to open the Formatting Rules Editor.
6. Click **Edit Rule Sheet** to create a new rule.
7. Click ✚ to add a new formatting rule.
8. In the Behavior section, click the **Condition** field.
9. Click ▪▪▪ next to the Condition field and set a conditional expression for the rule.

   There are multiple expressions that can be created. For setting a condition on a data value, select the data field from the list, select operator and value to be compared.

   Example: [Domain Name (Domain)] == ‘ABC’
10. Click **OK** to save the condition.
11. To show the table cell based on the condition, set the **Formatting | Visible** behavior to **Yes.**

    - OR -

    To hide the table cell based on the condition, set the **Formatting | Visible** behavior to **No.**
12. Click **Close**.
13. To apply this formatting rule to the table cell, click the rule and click the **>** icon to add the rule to the list for “Rules Applied to This Control”.
14. Click **OK**.

Creating a Calculated Field

Calculated fields are data fields that can be created to perform calculations over different data fields in your report.

To create a calculated field

1. In My Reports, select the report, then click **Edit report**.
2. To edit the existing layout, click the **Layout** button, then click the **Edit** button.

For more information, see Changing the Layout on page 120.

3 Click the **Fields List** tab.

4 To add a new calculated field to the field list, in DataSet1, right-click the **Table** folder and click **Add Calculated Field**.

The new calculated field is created under the Table folder.

5 To open the Collection Editor, right-click the new calculated field, and click **Edit Calculated Field**.

6 Enter a name in the (Name) property.

7 In the calculated field properties, select the appropriate field type.

Possible field types include String, DateTime, TimeSpan, Byte, Int16, Int32, Float, Double, Decimal and Boolean.

8 To open the Expression Editor, click **Expression property** and click ▪▪▪.

9 Set the applicable expression and click **OK**.

The calculated field value is based on the results of the expression. The expression can be created using functions, operators, data fields, constants and parameters. For example, to create a full name field from two fields (First and Last Name) use “”.

For more information, see the Report Designer User Guide (Developer Express), located in the folder where you installed the Report Manager.

10 Click **OK** to save the calculated field.

11 Drag and bind the calculated field to any control for display in report layout.

For more information, see Binding a Data Field to a Control on page 128.

Creating a Script to Run with a Report

Scripting allows you to insert scripts into a report and run them when the report is previewed, printed, or exported. Script commands should be placed within the event handlers of the report objects. When the corresponding event occurs (for example, a mouse click), the script code runs.

Script languages supported include C#, Visual Basic® and J#.

To add a script to an event

1 In My Reports, select the report, then click **Edit report**.

2 To edit the existing layout, click the **Layout** button, then click the **Edit** button.

For more information, see Changing the Layout on page 120.

3 Select the report control or object to execute the script on an event.

4 On the Property Grid in the Behavior section, expand the **Scripts** property and click the event on which to run the script.

5 To create a script for the selected event, click the drop-down arrow and select **New**.

6 In the Script Editor, enter the text for the new script.

Use the Validate option to validate and view script errors in the bottom panel.

7 Click **OK** to save changes and exit the script editor.

- OR -

Click the **Designer** tab to return to the Report Designer to continue editing the report.

You can edit and view the script by selecting the Scripts tab on the main Report Designer page.

Publishing Reports

Reporting administrators can publish reports that will be useful to their users. When a report is added to the Published Reports container, it is visible to all reporting users the next time they open their console. These reports are generally customized to suit your environment. You can base a published report on a report from the library, or you can create a new report and publish it. If you are a reporting administrator, you can edit reports directly in Published Reports; however, it is recommended that you copy reports to My Reports for editing.

If you have many published reports, you can create categories to group your reports for easier access. For information on copying reports, see Copying Reports on page 105. For information on categories, see Working with Report Categories on page 105.

To publish a report

- Copy a report from My Reports or the Report Library into Published Reports.

To update a published report

1. Copy the report from Published Reports into My Reports.
2. Modify the report as needed.
3. When you are ready to publish, delete the old version from Published Reports.

   If you skip this step, when you copy the revision back to Published Reports, it will be renamed to Report Name (1).
4. Copy the report from My Reports to Published Reports.

Integrating with SSRS

You can configure Enterprise Reporter for publishing reports to SQL Server Reporting Services (SSRS). Reports can then be published allowing users to generate reports using a web browser instead of the Report Manager.

See also:

- Configuring SSRS
- Publishing Reports to SSRS

Configuring SSRS

In order to configure the Report Manager so that you can publish reports, you must provide:

- The reporting services URL that hosts SSRS as configured in SSRS.
  This must be entered in the form http://<servername>/<instancename>.
- A user account for accessing the reporting services URL.
  The account must have access to the URL.
- A shared data source, to be used by all reporting administrators.
  If the data source doesn't exist, it is created. You can use an existing data source by entering its name. The data source is automatically linked to your Enterprise Reporter database. You need to provide an account that is able to access the Enterprise Reporter database and has been given appropriate rights to read collected data from the database. The account needs to be in the Reporter_Reporting_Admins or Reporter_Reporting_Operator groups.

  NOTE: Only reporting administrators can configure and publish to SSRS.

NOTE: For information on configuring SSRS, see the product documentation included on your CD or download package.

To configure SSRS for publishing reports

1. On the System Configuration page, click **Configure SSRS used by Enterprise Reporter**.
2. Enter the reporting services URL.
3. Open the Credential Manager and select or add an account.

   For more information, see Using the Credential Manager on page 98.
4. Test your connection.
5. Enter a name for your shared data source.

   If you have previously created a shared data source that you want to use, enter the same name. If you are setting up a new data source, it will be created using the provided name the first time a report is published.
6. Choose the type of authentication (either Windows or SQL Server depending on how SSRS was configured).
7. Open the Credential Manager and select or add an account that can access the Enterprise Reporter database.
8. Click **OK**.

Publishing Reports to SSRS

Reporting administrators can publish any report to SSRS. Once published, users with access can generate these reports from a web browser.

You can publish an entire container at once. All reports in the container will appear in a flat list, even if they were originally in a subcontainer in Enterprise Reporter.

CAUTION: The ability to publish reports to Quest Knowledge Portal and the integration with Quest Knowledge Portal has been removed from the product. After upgrade to Enterprise Reporter 3.5, all reports will have to be published to SSRS, as previously published reports to Quest Knowledge Portal will no longer be available and cannot be updated.

If you intend to publish reports to a custom path in SQL Server Reporting Services (SSRS), additional permissions must be configured.

- For any path outside of the **SSRS | Enterprise Reporter** path and its subdirectories, the Reporter_Reporting_Admins and Reporter_Reporting_Operators groups must be given to the SSRS **Browser** role on the **SSRS | Enterprise Reporter | Shared Resources** location.

TIP: Before publishing a report, verify that a report with the same name has not already been published. Reports with the same name will be overwritten automatically.

CAUTION: Verify any reports that have been published with errors. Use the Open Log option to examine details in the log and determine what issues to resolve. Some features, such as scripts, which are possible in Enterprise Reporter, are not supported by SSRS. When you run a report in SSRS with filters, data types, fields or controls that are not supported, the field appears as undefined. You can modify the report to resolve the errors in Enterprise Reporter (see Editing Reports on page 107) and then republish it. For example, you could change an operator.

To publish reports to SSRS

1. On the Report tab, right click any report or container.

   You can select multiple reports.

   You cannot publish the default containers: My Reports, Published Reports or Report Library.
2. Click **Publish to SSRS**.

3 If you are only publishing a single report, you can modify the name.

4 If you want to create or publish to a folder, type the path structure.

The full URL to the published report is shown.

5 Click **OK**.

6 A dialog box displays each step of progress during publishing.

Any errors encountered during publishing are also displayed.

7 If your report published successfully, click **Close**.

You can now run this report from SSRS. For details, see your SSRS administrator or see the SSRS User Guide in the Technical Documentation.

- OR -

If your report had errors, click **Open Log** and examine the details in the log to determine what issues to resolve, then click **Close**.

4

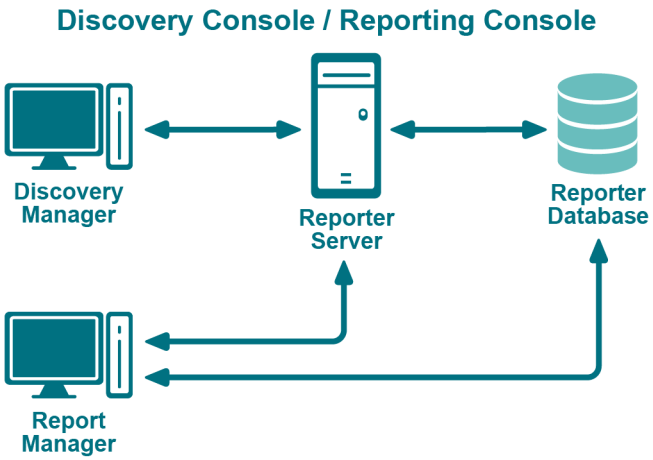
Troubleshooting Issues with Enterprise Reporter

- Troubleshooting connectivity issues
- Troubleshooting Connection Timeouts
- Troubleshooting credential change failures
- Auditing Report Manager Activity
- Exporting Logs from the Report Manager
- Resolving Issues in the Report Manager
- Troubleshooting Issues with SSRS

Troubleshooting connectivity issues

Each console maintains connections to the Enterprise Reporter server and to the SQL Server database that stores Enterprise Reporter data. A loss of either connection causes problems. Figure 4 outlines the connections between the components and the server and database.

Figure 4. Connections between components and the server and database.



Topics

- Restoring a connection to the Enterprise Reporter Server
- Restoring a connection to the Enterprise Reporter database

Restoring a connection to the Enterprise Reporter Server

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

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

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

Restoring a connection to the Enterprise Reporter database

If your server has lost its connection to the database, you can still open a console and connect to the server, but functionality will be limited. You will be unable to create discoveries, run reports or modify your configuration. Ensure that the SQL Server hosting the Enterprise Reporter database is running, and that the server can access it.

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

Troubleshooting Connection Timeouts

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

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

There are the following settings for each timeout configuration:

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

NOTE: Local administrative privileges are required to change timeout settings.

To change the database timeout settings for the Enterprise Reporter Server

1. Click **System Configuration**.
2. Under Time-Outs, click **Manage database settings used by Enterprise Reporter**.
3. To change the time allowed to establish a connection, modify the Connection Timeout.
4. To change the time allowed to process a database command, modify the Command Timeout.
5. To change the time allowed to generate a report, modify the Report Command Timeout.

Troubleshooting credential change failures

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

If a report schedule fails after changing a credential, it could mean that:

- Your credentials do not have access to the delivery share. Ensure the credentials are valid, and that they have write access to the share.
- Your credentials are not valid for your SMTP server. You can test the credentials in the SMTP configuration dialog box. For more information, see Delivering Scheduled Reports by Email on page 89.

Auditing Report Manager Activity

User activity from the Reporter Manager console is stored in the Quest Enterprise Reporter Windows Event Log on the machine for the Enterprise Reporter Server. Using this information, you can audit the following user activity for compliance purposes:

Table 41. Report Manager Activity in the event log

Event	Event ID	Event Format
Create Report	2015	User <USERNAME> on machine <MACHINENAME> created report '<REPORTNAME>' (<REPORTID>)
Run Report (manual)	2016	User <USERNAME> on machine <MACHINENAME> created report '<REPORTNAME>' (<REPORTID>)
Modify Report	2017	User <USERNAME> on machine <MACHINENAME> modified report '<REPORTNAME>' (<REPORTID>)
Delete Report	2018	User <USERNAME> on machine <MACHINENAME> deleted report '<REPORTNAME>' (<REPORTID>)

You can interrogate the event log directly for object user activity information. As shown in Table 41, each event is logged with the fully qualified user name of the Enterprise Reporter user who performed the event and the machine name where the event occurred.

Exporting Logs from the Report Manager

This section gives an overview of how to export logs from the Report Manager.

See also:

- Exporting the Report Manager Logs
- Viewing the Report Manager Logs

Exporting the Report Manager Logs

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

To export Report Manager logs

1. Click **System Information**.
2. Under Client Logging Information, click **Export Report Manager logs**.
3. Click **Export**.
4. Click the link to locate your zip file.

   You can now email your log files to your Quest Support representative.
5. Click **Close**.

Viewing the Report Manager Logs

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

To view the Report Manager logs

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

Resolving Issues in the Report Manager

The Report Manager is used to generate reports using the data collected by the Configuration Manager. There are some issues that may occur while using this console.

See also:

- What To Do if the Data in Your Report is Not What You Expect
- Other Issues
- Viewing information about your Enterprise Reporter configuration

What To Do if the Data in Your Report is Not What You Expect

There are a number reasons why there may be no data or data that is unexpected. The following table outlines some of the possible problems and solutions.

Table 42. Possible Causes for Unexpected Report Results

Problem	Solution
Your report has different data than the last time you ran it, and you do not think it should.	Check your parameter values, and ensure that you are running the correct report. If you are running a scheduled report, ensure that no changes were made to the underlying report. For more information, see Scheduling Reports on page 87. If this does not address the issue, it is possible there is a data collection issue, such as scopes or tombstoning. Inform your Enterprise Reporter administrator. For more information, see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.
You supply values for the supplied parameters, but your report has no data.	The parameters are joined together with AND logic. This means that if you supply values for parameters, all the values have to be true for all data in the report. Remove the values and rerun the report to determine if this is the issue.
Your report does not return the data you were expecting, even with no values provided for the parameters.	Examine the report definition to ensure that fields you need are included in the report, and that there are no parameters that would prevent the expected data from appearing, including hidden parameters. If you need to customize the report, see Editing Reports on page 107 and Viewing Report Properties on page 83.
Your groups appear to have incomplete members.	Group membership is an option in NTFS and SQL Server® discoveries. For more information, see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation.
Your report does not have any data.	If no other solution works, it is possible that no data has been collected. Collections are performed using the Configuration Manager. Contact your Enterprise Reporter administrator to ensure a proper discovery is created to cover the scope of your report.
After upgrading, editing older reports can result in missing data for a field.	Check with your Enterprise Reporter administrator to see if the field is an extended field—extended attributes have (extended) after them. It is likely that is now collected by default, and you can replace the extended attribute with the default in the report.
Data does not seem to be updated for a specific field	Check with your Enterprise Reporter administrator to see if the field is still being collected. Administrators can manage which attributes are collected.
You have used the * wildcard as a parameter value, but no data is returned.	A number of parameters included in the Library reports have been specially developed to be easier to use. You must select values from the list of options in order to see results in your report.
You are scheduling a report, and you are denied access to a share.	Ensure that the credentials have write access to the target share. If the share is located on the Reporter server, the server credentials are used. If the share is not located on the Reporter server, the credentials specified when creating the schedule are used.
You need to change the format of the data in your report. For example, your report is showing a computer using the fully qualified domain name, and you would like it to show the common name.	Use a custom query report. To make things easier, you can copy the query from an existing report into a query editor, make the necessary changes, and then paste the new query into the custom query report.

Other Issues

The following table outlines other issues that you may encounter using the Report Manager.

Table 43. Troubleshooting Report Manager Issues

Problem	Solution
Dragging and dropping does not work.	Drag and drop works as follows: • Moves reports between categories in a container. • Copies reports between containers. • Prevents moving or copying reports where you are not permitted—for example, into the Report Library.
You cannot create a report.	Depending on your access level, you may not be able to create reports in Published Reports. You cannot add reports to the Library. If you want to add reports to Published Reports so that all users connected to the Reporter server can use the report, you can either copy the report and paste it into Published Reports, or you can import a report definition. For more information, see Copying Reports on page 105.
Drop-down lists in parameter cards are empty.	The drop-down lists are populated by data collected by discoveries. One reason for an empty list may be that there is no relevant data. For more information, contact your Enterprise Reporter administrator or see the Quest Enterprise Reporter Configuration Manager User Guide in the Technical Documentation. If this is not the case, large data sets may take a while to appear on the drop-down list. In this case, you will see a progress indicator. Wait for the data to load, and proceed with your report.
Your reports timeout while generating.	You can increase the amount of time allowed to connect to the database using the **System Configuration | Time-Outs**.
You get a warning about a linked report that is missing: "The <ExchangeReportName> report cannot be found. Ensure that this report exists in your Enterprise Reporter library: My Reports\<PathToReport>	This warning indicates that you are trying to drill down to a report that is missing. This may occur in the following situations: • The missing report was not copied from Published Reports to My Reports. • The report administrator did not make the missing report available in the Published Reports making it unavailable to copy to My Reports. • The missing report was copied from Published Reports to My Reports but was subsequently deleted. The report administrator must ensure that the report listed in the warning has been published. For more information, see Publishing Reports on page 132. Then, you must copy the missing report from published reports to the location listed in the warning. For more information, see Copying Reports on page 105.

Viewing information about your Enterprise Reporter configuration

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

To view system information in the Report Manager

- Click the **System Information** tab.

Troubleshooting Issues with SSRS

The following table outlines other issues that you may encounter using SSRS.

Table 44. Troubleshooting SSRS Issues

Problem	Solution
When attempting to load the SSRS website, the main pane just displays "Loading..."	This may be the result of the SSRS web site not being in a trusted zone, or Internet Explorer Compatibility mode being disabled. Please try the following: 1 Open **Internet Explorer | Internet Options | Security** tab. 2 Select **Local Intranet** at the top. 3 Click the **Sites** button. 4 Add an entry for the server hosting SSRS. For example, http://server_name. 5 Add an entry for the SQL server that has reporting services. For example, http://SQL_server_name. 6 Ensure that Compatibility mode is enabled for SSRS site: ▪ Visit SSRS URL. ▪ Click on T**ools | Compatibility View Settings** and add the web page. 7 Ensure that you can browse to the default SQL reporting site, and that there are no errors. By default, this is http://sql_server_name/reports.

A

Appendix: PowerShell cmdlets

- What is Microsoft Windows PowerShell?
- What are cmdlets?
- Registering Enterprise Reporter cmdlets
- Adding the snap-ins automatically to new sessions
- Enterprise Reporter cmdlets
- Enabling Enterprise Reporter cmdlets
- Loading the Enterprise Reporter cmdlets
- Using cmdlets to manage clusters and nodes
- Using cmdlets to manage discoveries
- Using cmdlets to run reports

What is Microsoft Windows PowerShell?

Microsoft Windows PowerShell is a Windows command-line shell and scripting language designed specifically for system administrators and built on top of the Microsoft .NET Framework. Windows PowerShell is included with Windows Server 2016, Windows Server 2019, and Windows Server 2020.

PowerShell 5.1 is the version of Windows PowerShell that ships with Windows Server 2022, Windows Server 2019, and Windows Server 2016.

What are cmdlets?

Windows PowerShell has the concept of cmdlets. A cmdlet is a simple, single-function command that manipulates objects and is designed to be used in combination with other cmdlets.

If you already had Windows PowerShell installed on your computer before you installed Quest Enterprise Reporter, the Enterprise Reporter cmdlets were automatically installed and registered with Windows PowerShell.

The examples in this section show you leverage the cmdlets available in Enterprise Reporter. These cmdlets allow you to perform many of the functions of Enterprise Reporter in an automation environment. Thee are also useful in environments where a repetitive process involving Enterprise Reporter is needed.

Registering Enterprise Reporter cmdlets

If you installed Windows PowerShell on your computer after you installed Quest Enterprise Reporter, you must register the cmdlets before you can start using them in Windows PowerShell.

To register the Enterprise Reporter cmdlets

1 Open Windows PowerShell and type the following at the command prompt:

```
Add-PSSnapin Quest.Reporter.Configuration
```

```
Add-PSSnapin Quest.Reporter.Reporting
```

2 Type the following at the command prompt to verify that the snap-in was added:

```
Get-PSSnapin
```

All registered snap-ins are listed.

To register the Enterprise Reporter cmdlets used for the Database Content Wizard

1 Open Windows PowerShell as Administrator and type the following at the command prompt:

```
Import-Module "C:\Program Files\Quest\Enterprise
Reporter\ConfigurationManager\DatabaseContentWizardCmdlets.Dll" -verbose
```

2 Type the following at the command prompt to verify that the module was added:

```
Get-command -Module Database*
```

All registered database modules are listed.

Adding the snap-ins automatically to new sessions

If you do not want to add the Enterprise Reporter snap-ins manually each time you start a new Windows PowerShell session, you can modify the Windows PowerShell profile file so that the snapins are added automatically.

To add Enterprise Reporter snap-ins automatically when you start a new Windows PowerShell session

- Add the following lines to the Windows PowerShell profile file (profile.ps1) file:

```
Add-PSSnapin Quest.Reporter.Configuration
```

```
Add-PSSnapin Quest.Reporter.Reporting
```

The location of the Windows PowerShell profile file is as follows:

WINDOWS\system32\windowspowershell\v1.0

NOTE: If you see the error message "...profile.ps1 cannot be loaded because the execution of scripts is disabled" the next time you start a new Windows PowerShell session, type the following at the Windows PowerShell command prompt:

- Set-ExecutionPolicy RemoteSigned

Then, type the following at the Windows PowerShell command prompt to confirm that the execution policy has been changed:

- Get-ExecutionPolicy RemoteSigned

Enterprise Reporter cmdlets

This table lists the cmdlets included with Quest™ Enterprise Reporter.

Table 45. Enterprise Reporter cmdlets for use with Windows PowerShell

Cmdlet	Module
Add-ERADDiscoveryAttribute	Quest.Reporter.Configuration
Add-ERComputerDiscoveryWMIClass	Quest.Reporter.Configuration
Add-ERNode	Quest.Reporter.Configuration
Add-ERSystemCredential	Quest.Reporter.Configuration
Connect-ERConfigurationServer	Quest.Reporter.Configuration
Connect-ERReportingServer	Quest.Reporter.Reporting
Disable-ERCluster	Quest.Reporter.Configuration
Disable-ERNode	Quest.Reporter.Configuration
Enable-ERCluster	Quest.Reporter.Configuration
Enable-ERNode	Quest.Reporter.Configuration
Export-ERReportDefinition	Quest.Reporter.Reporting
Get-ERCluster	Quest.Reporter.Configuration
Get-ERDirectoryConfiguration	Quest.Reporter.Configuration
Get-ERItSearchConfiguration	Quest.Reporter.Configuration
Get-ERJobDefinition	Quest.Reporter.Configuration
Get-ERJobRun	Quest.Reporter.Configuration
Get-ERLastJobRun	Quest.Reporter.Configuration
Get-ERLogs	Quest.Reporter.Configuration
Get-ERNasConfiguration	Quest.Reporter.Configuration
Get-ERNode	Quest.Reporter.Configuration
Get-ERReport	Quest.Reporter.Reporting
Get-ERReportSQL	Quest.Reporter.Reporting
Get-ERSystemCredential	Quest.Reporter.Configuration
Get-ERUnassociatedNode	Quest.Reporter.Configuration
Import-ERReport	Quest.Reporter.Reporting
Initialize-Services	Quest.Reporter.Reporting
Invoke-ERReport	Quest.Reporter.Reporting
New-ERCluster	Quest.Reporter.Configuration
New-ERCredentialMapping	Quest.Reporter.Configuration
New-ERJobDefinition	Quest.Reporter.Configuration
Publish-ERReport	Quest.Reporter.Configuration
Register-ERDirectoryDiscoveryType	Quest.Reporter.Configuration
Register-ERLicense	Quest.Reporter.Configuration
Remove-ERCluster	Quest.Reporter.Configuration
Remove-ERDirectoryConfiguration	Quest.Reporter.Configuration
Remove-ERJobDefinition	Quest.Reporter.Configuration
Remove-ERNasConfiguration	Quest.Reporter.Configuration
Remove-ERNode	Quest.Reporter.Configuration
Send-ERItSearchData	Quest.Reporter.Configuration

Table 45. Enterprise Reporter cmdlets for use with Windows PowerShell

Cmdlet	Module
Set-ERADChangeHistory	Quest.Reporter.Configuration
Set-ERCommonChangeHistory	Quest.Reporter.Configuration
Set-ERComputerChangeHistory	Quest.Reporter.Configuration
Set-ERConfigurationManagerOptIn	Quest.Reporter.Configuration
Set-ERConfigurationServer	Quest.Reporter.Configuration
Set-ERDirectoryConfiguration	Quest.Reporter.Configuration
Set-ERDirectoryDiscoveryTypeConsent	Quest.Reporter.Configuration
Set-ERItSearchConfiguration	Quest.Reporter.Configuration
Set-ERJobDefinition	Quest.Reporter.Configuration
Set-ERJobDefinitionSchedule	Quest.Reporter.Configuration
Set-ERNasConfiguration	Quest.Rerporter.Configuration
Set-ERNodeCluster	Quest.Reporter.Configuration
SetERNTFSChangeHistory	Quest.Reporter.Configuration
Set-ERRegistryChangeHistory	Quest.Reporter.Configuration
Set-ERSettingsSSRS	Quest.Reporter.Reporting
Set-ERSQLChangeHistory	Quest.Reporter.Configuration
Set-ERSystemCredential	Quest.Reporter.Configuration
Start-ERBackup	DatabaseContentWizardCmdlets
Start-ERClean	DatabaseContentWizardCmdlets
Start-ERMerge	DatabaseContentWizardCmdlets
Start-ERRestore	DatabaseContentWizardCmdlets
Start-ERTransfer	DatabaseContentWizardCmdlets
Submit-ERJobDefinition	DatabaseContentWizardCmdlets
Update-ERNode	Quest.Reporter.Configuration

Enabling Enterprise Reporter cmdlets

Before you can use any of the Enterprise Reporter cmdlets, you might need to configure the older systems (before Windows 2012 R2) on which you will be running the cmdlets.

To enable the Enterprise Reporter cmdlets

- Within the folder C:\Windows\System32\WindowsPowerShell\v1.0, create a new file called powershell.exe.config that contains the following lines:

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0" />
    <supportedRuntime version="v2.0.50727"/>
  </startup>
</configuration>
```

Loading the Enterprise Reporter cmdlets

You can create a profile file that displays the list of Quest™ Enterprise Reporter cmdlets each time you open Windows Powershell.

To create a profile to display the list of Enterprise Reporter cmdlets

1. On the system where Enterprise Reporter is installed, open Windows PowerShell.
2. Enter this command to set the registry value so you can run scripts:

   ```
   Set-Executionpolicy RemoteSigned
   ```
3. Enter this command to create a Windows PowerShell profile file:

   ```
   New-Item -path $profile -type file –force
   ```
4. Enter this command to open the profile file in Notepad:

   ```
   notepad $profile
   ```
5. Add the following commands to load the Enterprise Reporter snapins, connect to the server, and display the list of cmdlets:

   ```
   add-pssnapin Quest.Reporter.Configuration

   add-pssnapin Quest.Reporter.Reporting

   Connect-ERConfigurationServer localhost

   Connect-ERReportingServer localhost

   get-command -Module quest*
   ```
6. Save the profile and exit Notepad.
7. Exit Windows PowerShell, and then open it.

   The snapins load and a list of commands display.

Using cmdlets to manage clusters and nodes

The examples in this section deal with the basics of Enterprise Reporter, which are clusters and nodes for the clusters. Without nodes, clusters cannot direct any work to be done and without clusters, nodes cannot do any work.

This section contains the following examples:

- Creating a cluster
- Creating a node
- Disabling a node
- Enabling a node
- Finding a node by name
- Piping cmdlets
- Finding a cluster by name
- Disabling a cluster

- Enabling a cluster

Creating a cluster

The New-ERCluster cmdlet creates a new cluster in Enterprise Reporter Configuration Manager on which discoveries can be run. Nodes are associated with this cluster, which can be installed on systems in remote locations to allow jobs to run closer to the physical location.

Syntax

```
New-ERCluster [-Name] <String> [[-Description] <String>] [[-SharedDataLocation]
<String>] [[-ConnectionTimeout] <String>] [[-CommandTimeout] <String>]
```

NOTE: The only parameter that is required is Name. All other variables can be added at a different time. Any parameter that contains a space must be enclosed in quotation marks.

Example

In this example, the new cluster named Second Cluster is created.

```
New-ERCluster -Name "Second Cluster" -Description "This is a test description" -
SharedDataLocation  C:\Shared -ConnectionTimeout 100 -CommandTimeout 500
```

Creating a node

The Add-ERNode cmdlet creates a new node that is associated with a cluster in Enterprise Reporter Configuration Manager. Nodes run the jobs assigned to them by the cluster. A cluster can have numerous nodes installed on different systems, which allows for more efficient processing of jobs and returns quicker results.

Syntax

```
Add-ERNode [-Cluster] <String> [-ComputerName] <String> [-Credential] <PSCredential>
[[-MaxJobSlots] <Int32>]
```

NOTE: Only the -MaxJobSlots parameter is optional; all other parameters must be supplied.

Example

This example involves a three step process. The first step encrypts the password used by the service account before sending it across the network. The second step combines the encrypted password with the service account into a new system object containing the credentials for the service account. The third step indicates the cluster, identifies the server where the node is to be installed, supplies the credentials, and defines how many jobs slots the node is to use.

```
secpasswd = ConvertTo-SecureString 'pA$$w0d' -AsPlainText -Force
credentials = New-Object System.Management.Automation.PSCredential
('AMER\Administrator', $secpasswd)
Add-ERNode "Second Cluster" "AMERGEN02" $credentials 5
```

Now the cluster named Second Cluster, which was created in the previous example (see Creating a cluster), has a node associated with it and is ready to run a job.

Disabling a node

There are times when a system may require maintenance or be taken down for some specific reason. During these times you will want to disable the node installed on that system. Disabling the node allows the cluster to manage the jobs based on the remaining nodes that are available for work.

NOTE: Even though you may have disabled a node, any jobs running on the node continue to be processed until completed. Only new jobs are not assigned to the node. Therefore, if maintenance is planned for the system, consider disabling the node in plenty of time for any job to finish.

Syntax

```
Disable-ERNode [-Node] <Node> [-CancelTasks [<SwitchParameter>]] [-PassThru
[<SwitchParameter>]]

Disable-ERNode [-Cluster] <String> [-ComputerName] <String> [-CancelTasks
[<SwitchParameter>]] [-PassThru [<SwitchParameter>]]
```

Example 1

In this example, the node associated with the cluster named First Cluster that is installed on the computer named AMERGEN01 is disabled.

```
Disable-ERNode -Cluster "First Cluster" -ComputerName AMERGEN01
```

Example 2

In this example, the node information is stored in the variable $node. The information contained in $node is then used as input to the Disable-ERNode cmdlet.

```
$node = Get-ERNode -Node AMERGEN01.amer.sitraka.com
Disable-ERNode -Node $node
```

Enabling a node

Once any work has been done on the system and you want to bring the node back into use, you need to enable the node so that the cluster knows the node is available and ready for work. Once the node is enabled, the cluster will assign the jobs waiting to be processed.

Syntax

```
Enable-ERNode [-Node] <Node> [-PassThru [<SwitchParameter>]]

Enable-ERNode [-Cluster] <String> [-ComputerName] <String> [-PassThru
[<SwitchParameter>]]
```

Example 1

In this example, the node associated with the cluster named First Cluster that is installed on the computer named AMERGEN01 is enabled.

```
Enable-ERNode -Cluster "First Cluster" -Passthru -ComputerName AMERGEN01
```

Example 2

In this example, the node information is stored in the variable $node. The information contained in $node is then used as input to the Enable-ERNode cmdlet.

```
$node = Get-ERNode -Node AMERGEN01.amer.sitraka.com
Enable-ERNode -Node $node
```

Finding a node by name

As nodes are an important part of the job processing, knowing about the nodes is vital so that you can ensure they are functioning properly and that the cluster has enough nodes to process jobs. The Get-ERNode cmdlet retrieves information about a node. You In addition, a cluster can be specified to show all nodes associated with the cluster. A computer can also be queried to see if there is a node install on it.

Syntax

```
Get-ERNode [[-Node] <String>] [[-Cluster] <String>]
```

Example 1

This example returns information from all nodes in all clusters.

```
Get-ERNode
```

Example 2

This example returns all nodes on the computer named AMERGEN01.

```
Get-ERNode -Node AMERGEN01
```

Example 3

This example returns all nodes in the cluster named First Cluster.

```
Get-ERNode -Cluster "First Cluster"
```

Piping cmdlets

Cmdlets can pipe the output from one cmdlet into another cmdlet. This feature is useful and powerful when you pipe the Get-ERNode cmdlet into Enable-ERNode and Disable-ERNode cmdlets.

Example 1

This example disables all nodes associated with the cluster named First Cluster. The data for all nodes is retrieved by the Get-ERNode cmdlet, and then piped into the Disable-ERNode cmdlet.

```
Get-ERNode -Cluster "First Cluster" | Disable-ERNode
```

Example 2

This example enables all nodes associated with the cluster named First Cluster. The data for all nodes is retrieved by the Get-ERNode cmdlet, and then piped into the Enable-ERNode cmdlet.

```
Get-ERNode -Cluster "First Cluster" | Enable-ERNode
```

Finding a cluster by name

As with nodes you can retrieve information about clusters. This information includes whether the cluster is enabled or disabled, if the cluster is using a shared data location, and the path of the shared data location.

Syntax

```
Get-ERCluster [[-Cluster] <String>]
```

Example 1

This example returns information on all clusters associated with Enterprise Reporter.

```
Get-ERCluster
```

Example 2

This example returns information on the cluster named Second Cluster. Note that he cluster name is in quotes because Windows PowerShell requires that any parameter containing spaces must be enclosed with quote marks.

```
Get-ERCluster -Cluster "Second Cluster"
```

Disabling a cluster

As with nodes, there are times when a system may require maintenance or you may want to stop the processing of specific jobs for some specific reason. During these times you will want to disable the cluster. Disable a cluster, effectively stopping new jobs and tasks from starting on any nodes within that cluster.

NOTE: Even though you may have disabled a cluster, any jobs running on the cluster will continue to run until completed. Disabling the cluster will disable all the nodes associated with it.

Syntax

```
Disable-ERCluster [-Cluster] <Cluster> [-CancelJobs [<SwitchParameter>]] [-PassThru [<SwitchParameter>]]
```

```
Disable-ERCluster [-Name] <String> [-CancelJobs [<SwitchParameter>]] [-PassThru [<SwitchParameter>]]
```

Example 1

In this example, the cluster named First Cluster is disabled.

```
Disable-ERCluster -Name "First Cluster"
```

Example 2

In this example, jobs scheduled to run on the cluster named First Cluster are canceled, and then the cluster is disabled. Jobs currently running will finish even though the cluster is disabled.

```
Disable-ERCluster "First Cluster" -CancelJobs
```

Example 3

In this example, the Get-ERCluster cmdlet first retrieves information about the cluster named First Cluster, and then stores it in the $cluster variable. Next, the cluster with the name stored in the $cluster.name variable is disabled.

If the Get-ERCluster cmdlet is run without identifying a cluster, it returns the information on all clusters. This technique can be useful when there are a number of clusters since they can be looped through disabling each one.

```
$cluster = Get-ERCluster “First Cluster”
Disable-ERCluster $cluster.name
```

Example 4

In this example, the Get-ERCluster cmdlet retrieves information for the cluster named Second Cluster and pipes it into the Disable-ERCluster cmdlet.

```
Get-ERCluster "Second Cluster" | Disable-ERCluster
```

Enabling a cluster

Once a cluster is enabled, the nodes assigned to the cluster start processing jobs. As with disabling the cluster, enabling the cluster will enable all the nodes associated with it.

Syntax

```
Enable-ERCluster [-Cluster] <Cluster> [-PassThru [<SwitchParameter>]]
[<CommonParameters>]

Enable-ERCluster [-Name] <String> [-PassThru [<SwitchParameter>]]
[<CommonParameters>]
```

Example 1

This example enables the cluster named First Cluster.

```
Enable-ERCluster "First Cluster"
```

Example 2

This example first stores cluster information in the $cluster variable, and then uses it as input to the Enable-ERCluster cmdlet. Note that the cluster name does not need to be parsed out and passed to the Enable-ERCluster cmdlet.

```
$cluster = Get-ERCluster
Enable-ERCluster $cluster
```

Example 2

This example uses Get-ERCluster to retrieve information for the cluster named First Cluster and pipes it to the Enable-ERCluster cmdlet.

```
Get-ERCluster -Cluster "First Cluster" | Enable-ERCluster
```

Using cmdlets to manage discoveries

An important aspect of Enterprise Reporter, discoveries return information about the systems in your environment. Discoveries gather data about Active Directory, computers, SQL Server, and NTFS permissions for files and folders. When using Enterprise Reporter cmdlets, discoveries are referred to as jobs. The examples in this section demonstrate how to create and run jobs using cmdlets.

This section contains the following examples:

- Getting job information
- Creating a job
- Running a job
- Scheduling a job
- Enabling a cluster

Getting job information

You probably have configured and run discoveries in the Enterprise Reporter Configuration Manager. These job definitions are useful in understanding how the cmdlets work and provide good examples for you to follow when creating new jobs using cmdlets. The Get-ERJobDefinition cmdlet returns information on the jobs.

Syntax

```
Get-ERJobDefinition [-ClusterId <Nullable`1[Guid]>] [-ClusterName <String>] [-
JobDefinitionName] <String>

Get-ERJobDefinition [-Unassigned [<SwitchParameter>]]

Get-ERJobDefinition -JobDefinitionId <Guid>
```

```
Get-ERJobDefinition -JobDefinition <JobDefinition>
```

Example 1

In this example, information about a job identified with the name of Active Directory is returned.

```
Get-ERJobDefinition -JobDefinitionName "Active Directory"
```

Output

```
JobDefinitionId     : ecaae8bb-f0f8-48ee-91ff-da959a937dfa
JobTypeId           : bec47934-cadf-4b94-8ff7-68efadc88165
Name                : Active Directory
Description         :
Configuration       : <DiscoveryResolutionTask
subType="ActiveDirectory"><Scopes><Scope
                      type="ActiveDirectory"><Content><Root class="Domain"
inex="Include"><Ldap>LDAP:

//AMER.amer.sitraka.com/DC=AMER,DC=amer,DC=sitraka,DC=com</Ldap><Dns>

AMER.amer.sitraka.com</Dns><DC>AMERGENDC.AMER.amer.sitraka.com</DC>
                     </Root></Content></Scope></Scopes><Parameters><Parameter

key="GatherSharedEntities"><Value>False</Value></Parameter><Parameter
                       key="CollectDCs"><Value>True</Value></Parameter><Parameter
                     key="CollectAccounts"><Value>True</Value></Parameter><Parameter

key="CollectComputers"><Value>True</Value></Parameter><Parameter
                       key="CollectOUs"><Value>True</Value></Parameter><Parameter
                       key="CollectSites"><Value>True</Value></Parameter><Parameter
                       key="CollectTrusts"><Value>True</Value></Parameter><Parameter

key="CollectPhysicalComputerInfo"><Value>False</Value></Parameter><Parameter

key="FindForeignMember"><Value>False</Value></Parameter><Parameter
                       key="SyncLogon"><Value>False</Value></Parameter><Parameter

key="CollectPermissions"><Value>False</Value></Parameter><Parameter

key="CollectRemoteServices"><Value>False</Value></Parameter><Parameter
                       key="CollectPhotosForUsers"><Value>False</Value></Parameter>
                       </Parameters></DiscoveryResolutionTask>
AssignedClusterId   : af0e6da4-10b9-4b20-bf5a-f19f0d71b589
CredentialId        :
AssignedClusterName : First Cluster
IsTombstoned        : False
Schedule            : <Trigger Type="RunOnceTrigger" StartDateTime="2014-07-
14T13:50:00Z"
                       Expression="2014-07-14 13:50:00Z@0 50 13 14 7 ? 2014" />
NextRun             :
```

Example 2

In this example, information about all the jobs (the * wildcard is used in -JobDefinitionName) located on the cluster named Second Cluster is returned.

```
Get-ERJobDefinition -ClusterName "Second Cluster" -JobDefinitionName *
```

Output

```
JobDefinitionId     : 7a8d758b-15e8-4f84-a30e-1c8545eed4f5
JobTypeId           : bec47934-cadf-4b94-8ff7-68efadc88165
Name                : Computer
```

```
Description         :
Configuration       : <DiscoveryResolutionTask subType="Computer"><Scopes><Scope
type="Computer">
                       <Content><Rootclass="Domain"
inex="Include"><Ldap>LDAP://AMER.amer.sitraka.com

/DC=RPTCH,DC=dev,DC=hal,DC=ca,DC=qsft</Ldap><Dns>AMER.amer.sitraka.com
                     </Dns></Root></Content></Scope></Scopes><Parameters><Parameter

key="GatherSharedEntities"><Value>False</Value></Parameter><Parameter
                    key="CollectAccounts"><Value>True</Value></Parameter><Parameter

key="CollectEventLogConfig"><Value>True</Value></Parameter><Parameter
                    key="CollectPolicies"><Value>True</Value></Parameter><Parameter
                    key="CollectPrinters"><Value>True</Value></Parameter><Parameter
                    key="CollectServices"><Value>True</Value></Parameter><Parameter
                     key="CollectShares"><Value>True</Value></Parameter><Parameter
                     key="CollectVolumes"><Value>True</Value></Parameter><Parameter

key="CollectExtendedWMIEntities"><Value>True</Value></Parameter><Parameter
                      key="PingTimeout"><Value>0</Value></Parameter></Parameters>
                      </DiscoveryResolutionTask>
AssignedClusterId   : 390b0bd1-6488-4ace-b2cc-616925b55c06
CredentialId        :
AssignedClusterName : Second Cluster
IsTombstoned        : False
Schedule            : <Trigger Type="RunOnceTrigger" StartDateTime="2014-07-
15T13:58:00Z"
                      Expression="2014-07-15 13:58:00Z@0 58 13 15 7 ? 2014" />
NextRun             :
```

As you can see in these examples, there is a lot of information contained in the job definition. The largest and seemingly most complicated part is the configuration, which contains all of the information about the jobs that you created using the Discovery Wizard. For more information about the configuration, see Creating a job.

Creating a job

Using cmdlets to create a new job requires planning as there is a lot information contained in a job definition. You would use cmdlets to automate a process, such as cloning a current job or creating a new job in an environment with limited resources.

Syntax

```
New-ERJobDefinition [-Name] <String> [-JobType] <String> [-Configuration] <String>
[[-ClusterId] <Guid>] [[-CredentialId] <Guid>] [[-Description] <String>] [[-
Schedule] <String>] [[-NextRun] <Nullable`1[DateTime]>] [-PassThru
[<SwitchParameter>]]
```

- [-JobType] values are: ActiveDirectory, Computer, Exchange, MS SQL, NTFS, and Registry.
- [-Configuration] is the XML representation of the job or discovery configuration. See any of the job examples in the Getting job information section, which discussed the Get-ERJobDefinition cmdlet. This is the best way to get a configuration to use in creating a job manually.

  The configuration can be contained in an XML file, making it easier to navigate. Using Notepad, copy the configuration from an existing job and paste it into a file. It is recommended that you create default files with the extension .XML and have the format as seen below which makes it easier to go thru and make the setting you want to make.

  Do not use any special program that provides an XML format. Any additional data in the file will not be interpreted correctly and can cause errors with the job creation. Use Notepad to avoid unseen character formatting.

Example 1

As you can see in this example, each section of the XML file has an opening and a closing statement. When you are working with a copy of the configuration from the Get-ERJobDefinition cmdlet, pay attention to spaces, text, slashes, and other characters, as missing or extra characters will cause an issue with the job.

```
<DiscoveryResolutionTask subType="NTFS">
  <Scopes>
    <Scope type="NTFS">
      <Content>
        <Root class="Computer" inex="Include">

<Ldap>LDAP://AMER.amer.sitraka.com/DC=AMER,DC=amer,DC=sitraka,DC=com</Ldap>
          <Dns>\\AMERGEN02.AMER.amer.sitraka.com</Dns>
        </Root>
      </Content>
    </Scope>
  </Scopes>
  <Parameters>
    <Parameter key="CollectPublicShares">
      <Value>True</Value>
    </Parameter>
    <Parameter key="TreatSharesAsShares">
      <Value>True</Value>
    </Parameter>
    <Parameter key="CollectFolderPermissions">
      <Value>True</Value>
    </Parameter>
    <Parameter key="CollectChildACLDifferences">
      <Value>True</Value>
    </Parameter>
    <Parameter key="FolderDepth">
      <Value>-1</Value>
    </Parameter>
    <Parameter key="GatherSharedEntities">
      <Value>False</Value>
    </Parameter>
    <Parameter key="GlobalInclude"/>
    <Parameter key="GlobalExclude" />
    <Parameter key="CollectFiles">
      <Value>True</Value>
    </Parameter>
    <Parameter key="CollectFilePermissions">
      <Value>True</Value>
    </Parameter>
    <Parameter key="CollectOnlyExplicitFilePermissions">
      <Value>False</Value>
    </Parameter>
    <Parameter key="IncludeFile">
      <Value>*.*</Value>
    </Parameter>
    <Parameter key="PingTimeout">
      <Value>0</Value>
    </Parameter>
  </Parameters>
</DiscoveryResolutionTask>
```

Example 2

In this example, the contents of the XML configuration file is used with the New-ERJobDefinition cmdlet. The values for the -Configuration parameter are enclosed in a single quote mark (').

The parameters in this example are formatted to make it easier for you to read. When running the cmdlet, the parameters cannot contain any carriage returns in the command line. If you want to use this example, you must first paste it into NotePad and remove the carriage returns.

```
New-ERJobDefinition -Name "NTFS All" -JobType NTFS -Configuration
'<DiscoveryResolutionTask  subType="NTFS"><Scopes><Scope type="NTFS"><Content><Root
class="Domain"
inex="Include"><Ldap>LDAP://AMER.amer.sitraka.com/DC=AMER,DC=amer,DC=sitraka,DC=com
</Ldap><Dns>AMER.amer.sitraka.com</Dns></Root></Content></Scope></Scopes><Parameter
s>
<Parameter key="CollectPublicShares"><Value>True</Value></Parameter><Parameter
key="TreatSharesAsShares"><Value>True</Value></Parameter><
Parameter key="CollectFolderPermissions"><Value>True</Value></Parameter><Parameter
key="CollectChildACLDifferences"><Value>True</Value></Parameter><Parameter
key="FolderDepth"><Value>-1</Value></Parameter><Parameter
key="GatherSharedEntities"><Value>False</Value></Parameter><Parameter
key="GlobalInclude"/><Parameter
key="GlobalExclude" /><Parameter
key="CollectFiles"><Value>True</Value></Parameter><Parameter
key="CollectFilePermissions"><Value>True</Value></Parameter><Parameter
key="CollectOnlyExplicitFilePermissions"><Value>False</Value></Parameter><Parameter
key="IncludeFile"><Value>*.*</Value></Parameter><Parameter
key="PingTimeout"><Value>0</Value></Parameter></Parameters></DiscoveryResolutionTas
k>'
-ClusterId af0e6da4-10b9-4b20-bf5a-f19f0d71b589 -Schedule '<Trigger
Type="RunDailyTrigger"
StartDateTime="2014-07-17T04:00:00Z" Expression="2014-07-1704:00:00Z@0 0 4 1/2 * ?"
EveryNDay="2" />'
```

Example 3

In this example the configuration is in an XML file, which allows changes to be made to the configuration when using the cmdlets. The XML files are just simple files that can be edited using Notepad and do not require any special formatting. The configuration of any current job is in the XML format and can be used as a template.

```
$filepath = "c:\configuration.xml"
$configuration =[string]::join([environment]::newline, (get-content -path
$filepath))
$foundCluster = Get-ERCluster 'First Cluster'
New-ERJobDefinition -Name NTFS10 -JobType NTFS -Configuration $configuration –
ClusterId $foundCluster.ClusterId
```

Example 4

In this example, you want to clone a current job. The important item to note is that the -Name parameter needs to be changed to a unique value. The first cmdlet Get-ERJobDefinition gets the data on the job you wish to clone. In the New-ERJobDefinition cmdlet you use the data in the configuration of the cloned job by using $JobDefinition.Configuration to supply the needed configuration for the new job.

```
$JobDefinition = Get-ERJobDefinition "NTFS All"
$foundCluster = Get-ERCluster 'First Cluster'
New-ERJobDefinition -Name NTFS2 -JobType NTFS -Configuration
$JobDefinition.Configuration -ClusterId $foundCluster.ClusterId
```

Running a job

Now that you have a job or two you need to run them to retrieve data from your environment by sending a job to the Enterprise Reporter server for immediate execution. Depending on what is processing within the server, the job may be queued to run at the next available time. This is different than scheduling a job which is discussed later.

Syntax

```
Submit-ERJobDefinition [-JobDefinitionId] <Guid>

Submit-ERJobDefinition [-JobDefinition] <JobDefinition>
```

Example 1

In this example, the job or discovery identified by the JobDefinitionId ecaae8bb-f0f8-48ee-91ff-da959a937dfa is submitted for immediate processing. If the job starts, True is returned.

```
Submit-ERJobDefinition -JobDefinitionId ecaae8bb-f0f8-48ee-91ff-da959a937dfa
```

Example 2

In this example, the information about the job definition retrieved by the Get-ERJobDefinition cmdlet is piped to the Submit-ERJobDefinition cmdlet, so the job starts immediately. If the job starts, True is returned.

```
Get-ERJobDefinition "Active Directory" | Submit-ERJobDefinition
```

Scheduling a job

You may want to change the start time for a scheduled job because it conflicts with another job.

NOTE: The schedule must be in CRON format. The time are UTC or GMT (time zone Z (zulu)).

Syntax

```
Set-ERJobDefinitionSchedule [-JobDefinitionId] <Guid> [[-Schedule] <String>]

Set-ERJobDefinitionSchedule [-JobDefinition] <JobDefinition> [[-Schedule] <String>]

Set-ERJobDefinitionSchedule [-JobDefinitionName] <String> [[-Schedule] <String>]
```

Example 1

This is an example of a Run Once job set to start at a specific date and time. First, the job is placed into the $discovery variable using the Get-ERJobDefinition cmdlet. Second, the Set-ERJobDefinitionSchedule cmdlet is executed with a different time and date for the job. Note the single quote that encloses the time.

```
$discovery = get-ERJobDefinition "Active Directory"
Set-ERJobDefinitionSchedule $discovery.JobDefinitionId '<Trigger
Type="RunOnceTrigger"  StartDateTime="2014-07-15T16:50:00Z" Expression="2014-07-15
16:50:00Z@0 50 16 15 7 ? 2014" />'
```

Example 2

This is an example of a Run Daily job set to start at a specific date and time, and to run every day.

```
Set-ERJobDefinitionSchedule -Schedule '<Trigger Type="RunDailyTrigger"
StartDateTime="2014-05-27T14:40:00Z" Expression="2014-05-27 14:40:00Z@0 40 14 1/1 *
?" EveryNDay="1" />'
```

Example 3

This is an example of a Run Daily job set to start at a specific date and time, and to run every 4th day.

```
Set-ERJobDefinitionSchedule -Schedule '<Trigger Type="RunDailyTrigger"
StartDateTime="2014-05-28T16:04:00Z" Expression="2014-05-28 16:04:00Z@0 4 16 1/4 *
?" EveryNDay="4" />'
```

Example 4

This is an example of a Run Weekly job set to start at a specific date and time, and to run on Monday, Wednesday, and Friday.

```
Set-ERJobDefinitionSchedule -Schedule '<Trigger Type="RunWeeklyTrigger"
StartDateTime="2014-05-30T16:01:00Z" Expression="2014-05-30 16:01:00Z@0 1 16 ? *
MON,WED,FRI" RunOnWeekDays="21" />'
```

Example 5

This is an example of a Run Monthly job set to start at a specific date and time and to run on the 1st Wednesday of the month.

```
Set-ERJobDefinitionSchedule -Schedule '<Trigger Type="RunMonthlyTrigger"
StartDateTime="2014-06-03T16:02:00Z" Expression="2014-06-03 16:02:00Z@0 2 16 3 * ?"
MonthlyScheduleType="NthDayOfTheMonth" WeekType="First" WeekDay="Wednesday"
DayOfTheMonth="3" />'
```

Example 6

This is an example of a Run Monthly job set to start at a specific date and time on the 3rd Wednesday of the month.

```
Set-ERJobDefinitionSchedule -Schedule '<Trigger Type="RunMonthlyTrigger"
StartDateTime="2014-06-18T16:02:00Z" Expression="2014-06-18 16:02:00Z@0 2 16 ? *
WED#3" MonthlyScheduleType="NthDayOfTheNthWeek" WeekType="Third"
WeekDay="Wednesday" DayOfTheMonth="28" />'
```

Deleting a job

Syntax

```
Remove-ERJobDefinition [-JobDefinitionId] <Guid>

Remove-ERJobDefinition [-JobDefinition] <JobDefinition>

Remove-ERJobDefinition [-JobDefinitionName] <String>
```

Example 1

In this example, all job definitions that start with the letter A are piped into the Remove-ERJobDefinition cmdlet for deletion.

```
Get-ERJobDefinition a* | Remove-ERjobdefinition
```

Example 2

```
$job = Get-ERJobDefinition "AD Discovery"
Remove-ERJobDefinition $job
```

First, the job data is placed into the $job variable. Second, the Remove-ERJobDefinition is run with $job as the input.

Using cmdlets to run reports

Now that you have collected data for your environment, you will want to produce reports with the data. Normally this is done using the Report Manager, but there are a number of cmdlets available to provide reports. The examples in this section demonstrate how to run reports using cmdlets.

This section contains the following examples:

- Connecting to the server
- Getting report information
- Exporting a report definition

- Importing a report definition to a category
- Generating a report with data

Connecting to the server

Before you can use the report cmdlets, you must establish a connection to the Enterprise Reporter server. If you do not have your profile set up (see Loading the Enterprise Reporter cmdlets), you will need to establish a connection.

Syntax

```
Connect-ERReportingServer [-Server] <String> [[-Port] <Int32>]
```

Example

In this example, a connection is established to the AMERGEN01 server through port 7738.

```
Connect-ERReportingServer -Server AMERGEN01 -Port 7738
```

Getting report information

Report Manager has a report library that is broken into a logical folder structure with reports in each folder. The functional cmdlets require the ID and path associated with each report and not just the report name. To get the report ID and path, use the Get-ERReport cmdlet. You can use wildcard expressions with this cmdlet. The wildcard search is performed on the full report path including folder names and report name.

Syntax

```
Get-ERReport [[-ReportName] <String>]
```

Example 1

This example returns all information on the Domain Accounts report.

```
Get-ERReport "*\Active Directory\Domain Accounts*"
```

Output

```
Id                                   CategoryPath                    ReportName
--                                   ------------                    ----------
58355095-75ee-4d21-9c11-1ccc15cbe3e3 Report Library\Active Directory Domain
Accounts
```

Example 2

This example returns all the reports that begin with Domain.

```
Get-ERReport "*\Active Directory\Domain*"
```

Output

```
Id                                   CategoryPath                    ReportName
--                                   ------------                    ----------
58355095-75ee-4d21-9c11-1ccc15cbe3e3 Report Library\Active Directory Domain
Accounts
e4067d44-b100-46e9-94da-8c3348584b50 Report Library\Active Directory Domain
Computer Information
```

```
59143e6b-cf55-4aa7-b70c-69c2b5b61659  Report Library\Active Directory  Domain
Controller Information

584229c5-dc71-4107-a0e5-38a2a6d4b8de  Report Library\Active Directory  Domain Groups
with Members

e6cf50aa-6078-4be8-aa92-3b0850264855  Report Library\Active Directory  Domain Groups
without Members

c49948e9-0337-47bd-bd48-e5cbf861391f  Report Library\Active Directory  Domain Groups

e4067d44-b100-46e9-94da-8c3348584b50  Report Library\Active Directory  Domain Hidden
Computers

237e4518-b843-4af7-911d-2b0ed62f1001  Report Library\Active Directory  Domain Sites

92e8568c-850d-416a-8b2b-3b01ad0f1b43  Report Library\Active Directory  Domain
Summary

b41d8e07-d0f4-46da-a2ae-bdd96992a12b  Report Library\Active Directory  Domain Trusts

73d3a6b2-95d7-4690-9aad-3fdf39dac04e  Report Library\Active Directory  Domain Users
with Recent Logons

73d3a6b2-95d7-4690-9aad-3fdf39dac04e  Report Library\Active Directory  Domain Users
without Recent Logons

95ccdb73-b815-47d2-af98-bc359201b6cd  Report Library\Active Directory  Domain Users
```

Exporting a report definition

Reports in Report Manager can be modified and configured. The modified report can be exported to a designated location for disaster recovery or to share with others. The complete report information obtained from the Get-ERReport cmdlet is required when performing the export. For more information, see Getting report information.

Syntax

```
Export-ERReportDefinition [-Report] <Report> [-Destination] <String>
```

Example 1

In this example, the Get-ERReport cmdlet places the report information for a report in the Report Library into the $rpt variable. Next, the report definition is exported to the c:\ drive. The exported definition contains the report name and the report Id: Domain Users_95ccdb73-b815-47d2-af98-bc359201b6cd.xrd.

```
$rpt = Get-ERReport "Report Library\Active Directory\Domain Users"
Export-ERReportDefinition $rpt -Destination c:\
```

Example 2

In this example, the Get-ERReport cmdlet places the report information for a report located in My Reports into the $rpt variable. Next, the report definition is exported to the c:\ drive. The exported definition contains the report name and the report Id: Domain Computer Information_e4067d44-b100-46e9-94da-8c3348584b50.xrd.

```
$rpt = Get-ERReport "My Reports\Domain Computer Information"
Export-ERReportDefinition $rpt -Destination c:\
```

Importing a report definition to a category

Reports in Report Manager can be modified and exported. The exported reports can later be imported into a new or existing category within the Enterprise Reporter report library.

Syntax

```
Import-ERReport [-ReportPath] <String> [[-TargetCategory] <String>]
[<CommonParameters>]
```

Example 1

In this example, the report is imported to the default category My Reports.

```
Import-ERReport -ReportPath c:\Report.xrp
```

Example 2

In this example, the report is imported to a category named My Reports\Imported.

```
Export-ERReportDefinition c:\Report.xrd -TargetCategory "My Reports\Imported"
```

Generating a report with data

You can generate reports in either PDF or CSV format, with the CSV file as a comma delimited file. Reports can be useful as recordkeeping or for disaster recovery. The complete report information obtained from the Get-ERReport cmdlet is required when performing the export. For more information, see Getting report information.

Syntax

```
Invoke-ERReport [-Report] <Report> [-Type] <String> [-Destination] <String>
```

Example 1

In this example, the report information is placed into the $rpt variable with the cmdlet Get-ERReport. Next, the report in PDF format is written to the c:\ drive.

```
$rpt = Get-ERReport "Report Library\Active Directory\Domain Users"
Invoke-ERReport -Report $rpt -Type PDF -Destination c:\
```

Example 2

In this example, the information for the report located in My Reports is placed into the $rpt variable with the cmdlet Get-ERReport. Next, the report in PDF format is written to the c:\ drive.

```
$rpt = Get-ERReport "My Reports\Domain Computer Information"
Invoke-ERReport -Report $rpt -Type PDF -Destination c:\
```

B

Appendix: Log Viewer

- Starting the Enterprise Reporter Log Viewer
- Finding and opening log files
- Viewing and searching log file entries
- Filtering log file entries

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

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

Starting the Enterprise Reporter Log Viewer

To start the Enterprise Reporter Log Viewer in the Configuration Manager

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

To start the Enterprise Reporter Log Viewer in the Report Manager

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

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

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

Finding and opening log files

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

\ProgramData\Quest\Enterprise_Reporter

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

To open log files using the Log Viewer browser

1 Double-click the log file containing entries to be viewed.

- OR -

Select the log file containing entries to be viewed and click the **Open** icon.

- OR -

Drag the log file containing entries to be viewed onto the main log entry viewing panel.

- OR -

Drag a log file from Windows File Explorer onto the main log entry viewing panel.

To unzip log files in the Log Folder panel

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

- OR -

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

To clear log files in the Imported Log Files panel

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

- OR -

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

Viewing and searching log file entries

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

To search for specific text within the log entries

1 Enter the text to locate in the **Find** text box.

2 Press **Enter** to locate the first occurrence of the text within the log entries being viewed.

The matching log entry will be highlighted.

3 Optionally, click the **Find Next** icon to find the next occurrence of the text within the log entries being viewed.

4 Optionally, click the **Find Previous** icon to find the previous occurrence of the text within the log entries being viewed.

To search for errors by error text within the log entries

1 Enter the error text to locate in the **Find** text box.

2 Optionally, click the **Next Error** icon to find the next occurrence of the text within the ERROR log entries being viewed.

3 Optionally, click the **Previous Error** icon to find the previous occurrence of the text within the ERROR log entries being viewed.

To browse for errors within the log entries

1 Click on the log entry from which you wish to browse.

2 Optionally, right-click the log entry and select **Next Error** to browse to the next error within the log entries being viewed.

3 Optionally, right-click the log entry and select **Previous Error** to browse to the next error within the log entries being viewed.

To view the details of a log entry

1 Double-click a log entry.

- OR -

Right-click a log entry and select **View Details**.

- OR -

Select a log entry and click the **View Details** icon above the main log entry viewing panel.

To clear all event log entries

1 Click the **Clear All** button above the main log entry viewing panel.

2 Accept the warning message to continue with removing all of the log entries.

Filtering log file entries

Once a listing of log file entries is displayed, the Filters option can be used to limit the entries by dates and other properties. For more information, see Viewing and searching log file entries on page 162. Setting a Start Date will display entries with a time stamp that occurs on or after that date. Setting an End Date will display entries with a time stamp that occurs on or before that date. Selecting options for each property will display entries matching those options.

To filter log file entries

1 Once you are viewing a listing of log file entries, click the **Filters** button.

2 Optionally, enter a Start Date.

3 Optionally, enter an End Date.

4 Optionally, select at least one option per property.

5 Optionally, click the reset button to clear all filters and start again.

6 Click **Apply** to display the log file entries that match the filters.

About us

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

Technical support resources

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

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

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