

Dell™ Enterprise Reporter 2.5

Configuration Manager User Guide



© 2014 Dell 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 Dell Inc.

The information in this document is provided in connection with Dell 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 Dell products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL 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 DELL 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 DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell 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. Dell 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:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Refer to our web site (www.software.dell.com) for regional and international office information.

Patents

This product is protected by U.S. Patent #8,601,539 and #8,838,654. Additional Patents Pending.

Trademarks

Dell and the Dell logo are trademarks of Dell Inc. and/or its affiliates. AMD is a trademark of Advanced Micro Devices, Inc. EMC, EMC Celerra, and Isilon OneFS are registered trademarks or trademarks of EMC Corporation in the United States and other countries. Intel is a trademark of Intel Corporation in the U.S. and/or other countries. Microsoft, Active Directory, SQL Server, Visual C++, Excel, Windows, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. NetApp, the NetApp logo, and Data ONTAP are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Perl and the Perl logo are trademarks of the Perl Foundation. Android is a trademark of Google, Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims any proprietary interest in the marks and names of others.

Legend

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

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

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

Contents

Product Overview	8
Key Features of Enterprise Reporter	8
Components of Enterprise Reporter 2.5	9
The Configuration Manager	9
The Report Manager	11
The Database Wizard	12
Dell Enterprise Reporter Mobile IT Pack	12
Knowledge Portal	12
Enterprise Reporter Architecture	13
Summarizing the Workflow	13
Configuring the Configuration Manager	15
Starting the Configuration Manager	15
An Overview of the Configuration Manager Security	16
Node Credential Details	17
Logged In User Details	19
Server Service Credential Details	19
Discovery Credential (Alternate Credential) Details	20
Access Explorer Agent Credential Details	21
Managed Domain Credential Details	22
Access Explorer Database Credential Details	22
Setting Up Your First Collection Computers	22
Configuring Clusters and Nodes for Effective Data Collection	23
Things to Consider Before Creating a Cluster	23
Creating Your First Cluster and Node	24
Modifying your Deployment	25
When Do You Add a Cluster?	25
Modifying a Cluster	26
Deleting a Cluster	26
Disabling a Cluster	26
What To Do if a Cluster is Disabled	27
Enabling a Cluster	27
Managing Nodes	27
Improving the Performance of Your Discoveries (Load Balancing)	30
Adding a Node	30
Improving the Performance of a Node	31
What does the status of a node or cluster indicate?	31
Using the Credential Manager	32
Changing Passwords Using the Credential Manager	34
Changing Account Names Using the Credential Manager	34

Changing the Credentials used by the Enterprise Reporter Server	35
Configuring Global Settings	35
Discovery Management Configuration	35
System Configuration	35
Access Explorer Management Configuration	36
Tips for Customizing the Configuration Manager Views	36
Creating and Managing Discoveries	37
Defining the Data Collection (Discoveries)	37
Step 1. Create the Discovery	38
Step 2. Choose what to include in your discovery (Scopes)	38
Choosing your Active Directory® Scopes	39
Choosing your Computer Scope	41
Choosing Your File Storage Analysis Scopes	43
Choosing Your Microsoft® SQL Scopes	44
Choosing Your NTFS Scope	46
Choosing Your Registry Scope	50
Using the Browser to Include and Exclude Scopes	52
Using Queries to Define Your Scopes	55
Step 3. Schedule your Discovery	56
Run your discovery once	56
Run your discovery on a daily interval	56
Run your discovery on specified days of the week	57
Run your discovery on a specified day of the month	57
Best Practices for Creating Discoveries	58
How is a Discovery Processed?	58
Types of Tasks	59
Manually Running a Discovery	59
Viewing your Discoveries	59
Navigating the Manage Discoveries Pane	60
Viewing the History of a Discovery	61
What Does the Discovery Status Indicate?	61
Viewing the Tasks for a Finished Discovery	62
Viewing the Tasks for a Processing Discovery	62
What Does the Task Status Indicate?	63
Why is My View Empty?	63
Viewing Errors	64
Viewing Statistics	64
Viewing a Cluster's Queue	65
Working with Discoveries and Tasks	65
Modifying a Discovery	65
Canceling a Task or Discovery	66
Deleting a Discovery	66
Global Discovery Settings	67
Configuring Change History	67

Managing the Collection of Additional Attributes	67
Dell Access Explorer	69
Access Explorer Overview	69
Access Explorer Components	69
Managed Domain	70
Registered Forest	70
Managed Computer	70
Access Explorer Agent	70
Scopes	71
Database	72
Service Accounts	72
Configuring Access Explorer	74
Setting Up Access Explorer	74
Setting Up the Access Explorer Database	74
Setting Up the First Managed Domain (includes the Service Account)	75
Updating Access Explorer Configuration	75
Adding Managed Domains	75
Adding Forests	75
Editing Managed Domains or Forests	76
Adding Service Accounts	76
Editing Service Accounts	77
Deleting Service Accounts	77
Collecting Access Explorer Data	77
Setting up a Managed Computer	78
Managing Managed Computers	81
Modifying Managed Computer Properties	83
Managing Agents	84
Troubleshooting Issues with Enterprise Reporter	88
Problems Opening the Consoles	88
Troubleshooting Connectivity Issues	88
Restoring a Connection to the Enterprise Reporter Server	89
Restoring a Connection to the Enterprise Reporter Database	89
Troubleshooting Connection Timeouts	89
Troubleshooting Credential Change Failures	90
Resolving Issues in the Configuration Manager	91
Node Issues	91
Scope Enumeration Issues	93
Data Collection Issues	94
Troubleshooting Features in Enterprise Reporter	95
Exporting Logs from the Configuration Manager	95
Viewing Information About Your Enterprise Reporter Configuration	96
Viewing Errors and Statistics for Tasks	96
Disaster Recovery	96
Back Up of Enterprise Reporter	96

How to Deploy Enterprise Reporter to Another Computer After a Disaster	97
Import the Enterprise Reporter Registry Key	98
Checking the Enterprise Reporter Configuration After a Recovery	98
Troubleshooting Access Explorer	99
Agent Events	99
Where are the Logs?	99
Access Explorer Service Logs	99
Agent Logs	100
Exporting Logs	100
Why is an Agent not Connecting to the Access Explorer Service?	100
Probable Cause	100
Resolution	101
Why are Agent Leases Expiring?	101
Probable Cause	101
Resolution	101
Appendix: PowerShell cmdlets	102
What is Microsoft Windows PowerShell?	102
What are cmdlets?	102
Registering Enterprise Reporter cmdlets	103
Adding the snap-ins automatically to new sessions	103
Enterprise Reporter cmdlets	104
Enabling Enterprise Reporter cmdlets	105
Loading the Enterprise Reporter cmdlets	106
Extracting help for Access Explorer cmdlets	106
Using cmdlets to manage clusters and nodes	107
Creating a cluster	107
Creating a node	108
Disabling a node	108
Enabling a node	109
Finding a node by name	109
Piping cmdlets	109
Finding a cluster by name	110
Disabling a cluster	110
Enabling a cluster	111
Using cmdlets to manage jobs (discoveries)	112
Getting job information	112
Creating a job	113
Running a job	115
Scheduling a job	116
Deleting a job	117
Using cmdlets to run reports	117
Connecting to the server	118
Getting report information	118
Exporting a report definition	119
Generating a report with data	119

Using cmdlets to set up Access Explorer	120
Creating the Access Explorer database	120
Adding a service account	120
Adding a domain to manage	121
Adding managed computers	121
Using cmdlets to get information about Access Explorer objects	122
Getting service account information	122
Getting managed domain information	123
Getting managed computer information	123
Getting security information for a resource	124
Getting resource access information	125
Using cmdlets to manage Access Explorer agents	127
Identifying agents on a managed computer	127
Changing the agent configuration on a managed computer	129
Restarting the agent	129
Updating an agent	130
Changing the service account password	130
Changing the SQL account password	131
Using cmdlets to remove Access Explorer objects	131
Removing a managed computer	131
Removing a managed domain	131
Removing a service account	132
Index	133
About Dell	137
Contacting Dell	137
Technical Support Resources	137

Product Overview

- [Key Features of Enterprise Reporter](#)
- [Components of Enterprise Reporter 2.5](#)
- [Enterprise Reporter Architecture](#)
- [Summarizing the Workflow](#)

Key Features of Enterprise Reporter

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

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

Using the Configuration Manager, you can:

- Configure your collection environment to minimize network traffic and optimize performance.
- Create discoveries to collect data that will be made available to the Report Manager:
 - information about your Active Directory® environment.
 - information about files and folders from domains, OUs, computers, NetApp® and EMC® filers, shares, and DFS shares and clusters.
 - information about the computers in your environment.
 - data from specified SQL Servers®, instances, and databases.
 - general and registry information from selected computers.
 - high-level summary information on file storage.
- Schedule discoveries to run automatically.
- Use the Enterprise Reporter MobileIT Pack on your mobile device to keep tabs on your deployment and discoveries, and perform basic management tasks.
- Track the progress of discoveries, and pinpoint any errors in the collection.
- Configure Access Explorer to scan and index security access information on files, folders, and shares to provide up-to-date insights into the account permissions on these resources by exploring and reporting.

Using the Report Manager, you can:

- Run reports on the data you have collected.
- Make predefined reports available to reporting users by publishing them.

- Create your own customized reports.
- Customize the appearance of your reports.
- Schedule reports to run when you need them.
- Publish reports to Knowledge Portal.
- Use the Enterprise Reporter MobileIT Pack on your mobile device to keep tabs on your scheduled reports.
- Use the Explore view to easily and quickly view permissions associated with shares, folders, and files for specified accounts and to run permission and summary reports on the access the account has.
- Use the File Storage Analysis summary reports, with meaningful charts and graphs and the ability to drill down for more detailed information, to answer challenging administrative questions about file storage.

Components of Enterprise Reporter 2.5

Enterprise Reporter has three components that work together to collect and report on your corporate IT data. Additionally, you can install the Database Wizard to help manage your Enterprise Reporter database, use a mobile application to manage your consoles, and use the Knowledge Portal to make reports available online.

The Configuration Manager

In order to create reports, you must first gather the data. The Configuration Manager manages the process of creating and managing the discoveries that collect data, and the computers that perform the actual collecting. The Configuration Manager is intended for use by administrators who are responsible for managing data collection.

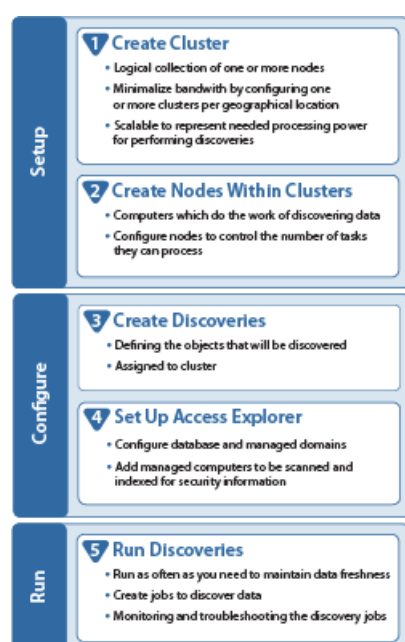
There are several tasks that you perform using the Configuration Manager:

- Configure clusters and nodes
- Create and run discoveries
- View errors and statistics for each discovery
- Configure Access Explorer and add managed computers

An Overview of the Configuration Manager

Figure 1 outlines the process of using the console to configure and perform data collections.

Figure 1. Using the Configuration Manager



Clusters

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

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

For more information, see [Configuring Clusters and Nodes for Effective Data Collection](#) on page 23, and [When Do You Add a Cluster?](#) on page 25.

Shared Data Locations

Each discovery cluster can have an optional shared data location that is used by each of the cluster's nodes. Data collected from discoveries is stored in this shared data location, and then added to the SQL database maintained by the Enterprise Reporter server for report generation. When new data is discovered, it is compared to the data currently held in the Enterprise Reporter database. The difference between the existing data in the database and the new data from the discovery is added.

A shared data location may only be used by nodes within its assigned cluster. Since the Enterprise Reporter server receives only the difference between previously collected data and new data, the shared data locations cannot be shared among clusters.

Nodes

A node is a computer assigned to a cluster and is responsible for processing discoveries. A node may only be assigned to a single cluster. Each node can be configured for a maximum number of concurrent tasks, allowing you to take advantage of your hardware to process discoveries more quickly. A discovery consists of one or more tasks, each of which collects information from a target. A discovery node may collect data from more than one

target and may process more than one discovery simultaneously if you allow multiple concurrent tasks. The default is five tasks running simultaneously.

Discoveries

Discoveries are created to collect data. A discovery contains a number of targets, and is assigned to a cluster. The Enterprise Reporter server distributes the work among the nodes in that cluster. For more information, see [Defining the Data Collection \(Discoveries\)](#) on page 37.

Role of the Server

The Enterprise Reporter server is the central component of the Enterprise Reporter application. It directs the collection of data, maintains the report data in a SQL database (the central data store), organizes the computers running discoveries (nodes) into logical collections called clusters, assigns discoveries to the nodes using load-balancing, and executes report schedules.

A Simple Example of Enterprise Reporter Configuration

A global corporation has decided to use Enterprise Reporter to keep track of the various SQL databases throughout their enterprise. They have offices located in New York City, London, and Tokyo, and each of these offices has a unique domain hosting several SQL databases.

Each office will host 3 discovery nodes on various computers in their respective domains. These nodes are collected into clusters. A total of 3 clusters are created; one cluster for each office. Additionally, each cluster has its own shared data location located within its domain. When a discovery is created, it is assigned to the cluster in the office.

In each office, when a discovery process is executed, the server assigns the discovery to the nodes within the assigned cluster. All of the required data is written to the local shared data location and then uploaded to the central data store controlled by the Enterprise Reporter server.

Access Explorer

Access Explorer collects data about user security on selected computers in your network. You must add one managed domain, create an Access Explorer database, and install an agent service on a server to scan a managed computer. A managed computer is one that you select for the agent service to scan and collect security information, which is stored in the Access Explorer database. You can explore and run reports on the stored information to manage security access. For more information on Access Explorer, see [Dell Access Explorer](#) on page 69.

The Report Manager

Once you have collected data, you use the Report Manager to generate reports. The Report Manager is a robust, flexible console that lets you create, modify and run reports. The Report Manager is intended for use by users who need to produce reports.

Reports in the Report Manager can be read-only, so that the settings cannot be changed, or they can be modifiable. For a modifiable report, you have control over what data is in the report, and how it is organized and laid out. Report definitions can be exported from one console, and imported into another. You can report on data collected from all clusters in your deployment.

The Database Wizard

The Database Wizard is a stand-alone utility you can use to create and manage your Enterprise Reporter database. For more information, see Managing Your Database Using the Database Wizard chapter in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

Dell Enterprise Reporter Mobile IT Pack

You can manage your clusters, nodes, discoveries and report schedules from your mobile device. If your organization has implemented a Mobile IT server, the Enterprise Reporter pack can be installed and accessed on devices running iOS or Android operating systems.

 **MOBILE:** Watch for this symbol indicating you can perform tasks on your mobile device using the Enterprise Reporter Mobile IT Pack.

Knowledge Portal

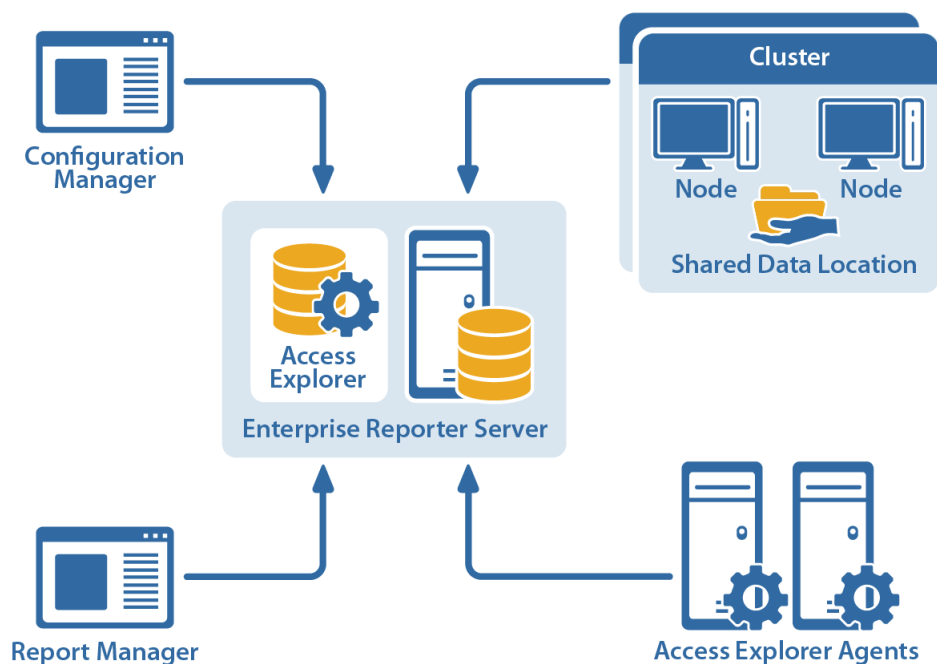
Knowledge Portal is a cross product online reporting platform. Once Knowledge Portal is deployed, you can configure Enterprise Reporter for publishing. Reports can then be published, allowing users to generate reports using a web browser instead of the Report Manager.

For more information, see the [Dell Enterprise Reporter Report Manager User Guide](#).

Enterprise Reporter Architecture

Figure 2 shows how the components of Enterprise Reporter are related.

Figure 2. Enterprise Reporter Architecture



Summarizing the Workflow

The Enterprise Reporter workflow has three distinct phases:

Table 1. Phases of Enterprise Reporter Workflow

Phase	console	description	Frequency
Configuration	Configuration Manager	Set up clusters and nodes	Set up initially Occasional modifications as your environment changes
		Execute discoveries	As often as you need to maintain the desired data freshness
Data collection	Configuration Manager	Configure Access Explorer	Set up initially
		Add managed computers	Once for every set of targets
Reporting	Report Manager	Generate reports based on collected data	As needed

These phases are not linear — you may run useful reports for a period of time, and then decide that you need to add another node, create a new discovery, or add another managed computer. You can move around between them as needed.

Configuring the Configuration Manager

- [Starting the Configuration Manager](#)
- [An Overview of the Configuration Manager Security](#)
- [Setting Up Your First Collection Computers](#)
- [Modifying your Deployment](#)
- [Improving the Performance of Your Discoveries \(Load Balancing\)](#)
- [What does the status of a node or cluster indicate?](#)
- [Using the Credential Manager](#)
- [Changing the Credentials used by the Enterprise Reporter Server](#)
- [Configuring Global Settings](#)
- [Tips for Customizing the Configuration Manager Views](#)

Starting the Configuration Manager

When you open the Configuration Manager, your first step is to connect to a server. Connecting to a server gives you access to its associated clusters, nodes, and discoveries. You need to know the name of the server, and the port number. The server name is the name of the computer where the server is installed. The port number was configured during the server installation. For more information, see [Viewing Information About Your Enterprise Reporter Configuration](#) and [Installing Enterprise Reporter](#) in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

NOTE: If UAC is enabled, you must have elevated permissions to open the Configuration Manager.

NOTE:

To start the Configuration Manager, you must be a discovery administrator.

For more information, see [Installing and Configuring the Configuration Manager and Role Based Security in Enterprise Reporter](#) in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

If this is your first time opening the Configuration Manager, you need to provide a license. For more information, see [Licencing Enterprise Reporter](#) in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

To connect to a server

- 1 Click the **Start** menu and select **All Programs | Dell | Enterprise Reporter | Configuration Manager**.
- 2 Type the name of the server.
- OR -
Click **Browse**, and locate the computer where the server is installed.
Once you have connected to a server, the server name is stored in the list for future use.
- 3 If necessary, type in the port number.

4 Click Connect.

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

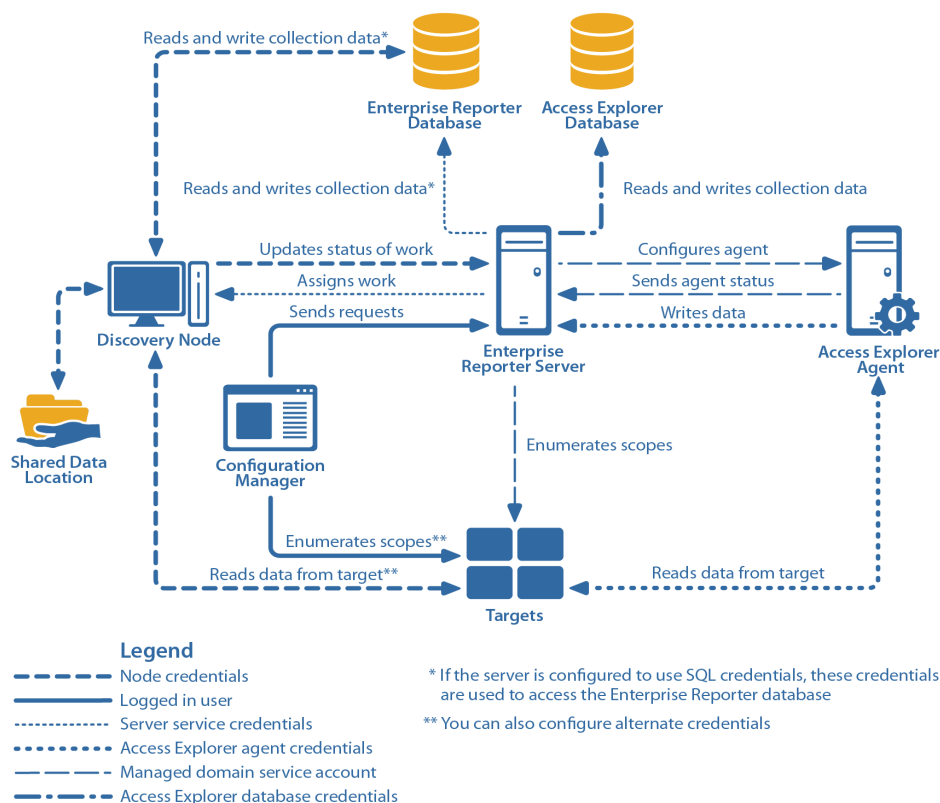
- MOBILE:** If you want to use the Enterprise Reporter Mobile IT Pack to monitor your deployment, download the application from the app store for your device (Android or iOS) and connect to the server provided by your Mobile IT administrator.

An Overview of the Configuration Manager Security

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

Figure 3 outlines where and for what each of the credentials are used, and the following tables explain the necessary permissions. For information on managing the credentials used in the Configuration Manager, see [Using the Credential Manager](#) on page 32.

Figure 3. Credentials used to communicate in the Configuration Manager



Access Explorer credentials are not stored in the Credential Manager. For more information on Access Explorer service accounts, see [Service Accounts](#) on page 72.

Node Credential Details

Node credentials are provided when a discovery node is created, and you can modify them as needed. The following table outlines the use of the node credentials, and how to properly configure your environment to ensure successful data collection:

Table 2. Node Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Server	Provide server with job status, errors, statistics and logs.	Configured during node creation, or when you edit the node properties to change the credentials. The node credentials must have local administrator access to the host computer.
Discovery Node	Shared Data Location (if the cluster is configured to use one)	Read and write to the shared data location during data collection.	The shared data location is configured during the creation of a cluster. Ensure the node has read and write access to this file share. For more information, see Things to Consider Before Creating a Cluster on page 23.

Table 2. Node Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery Node	Enterprise Reporter Database	There are two options for communicating with the database: - You can use the same service credentials that the node service uses. - You can specify SQL credentials only for use when the database is accessed. The credentials you choose must be able to read and write to the database.	The account must be in the Reporter_Discovery_Admins security group. (Note that if you use the same account as the Enterprise Reporter server it is already permissioned appropriately). For more information, see Role Based Security in Enterprise Reporter and Configuring the Database in the Dell Enterprise Reporter Installation and Deployment Guide. If you use SQL authentication to connect with the database, you must manually permission the SQL user, either by adding them to the database role Reporter_Discovery_Admin_Role (recommended) or by permissioning specific tables in the database.
Discovery Node	Targets	Read access on all targets. If required, you can configure alternate credentials for specific discoveries, instead of using the default node credentials. For more information, see Discovery Credential (Alternate Credential) Details on page 20.	On the target, ensure the node credentials have read access. The node credentials must have local administrator access to the target computer. The targets are defined as part of a discovery. The targets are assigned to a particular node based on availability, so all nodes in a cluster should have access to all targets defined in all discoveries assigned to the node's cluster.

Logged In User Details

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

Table 3. Logged In User Credentials in Configuration Manager

From	To	Permission Details	Configuration
Configuration Manager	Enterprise Reporter Server	Must be a member of the Reporter_Discovery_Admins group in order to log in to the console. Configuration Manager will send configuration and set up requests to the server.	Configuration is dependent on your deployment's security group setup. See the System Information page to determine the type of security in place. For more information, see Configuring the Database and Security Groups in the Dell Enterprise Reporter Installation and Deployment Guide .
Configuration Manager	Targets	Must be able to enumerate the targets during scope selection, unless alternate credentials are provided for the discovery. All domains with which the credentials have a forest or domain level trust will be enumerated.	On each target, grant the user read access.

Server Service Credential Details

Server service credentials are provided during the installation of the server. The following table outlines the use of the service account credentials, and how to properly configure your environment to ensure successful data collection:

Table 4. Server Service Credentials in Configuration Manager

From	To	Permission Details	Configuration
Enterprise Reporter Server	Enterprise Reporter Database	Must be able to read and write to the database. If the server is configured to use SQL authentication, the SQL credentials will be used to access the database, not the service account.	Configured automatically during installation. If you change the service credentials for the Dell Enterprise Reporter Server service, you need to ensure that a SQL login exists for that account, and create one if none exists. The login must be added to the database roles. For more information, see Configuring the Database and Security Groups in the Dell Enterprise Reporter Installation and Deployment Guide.
Enterprise Reporter Server	Discovery Node	Must be able to write to the Admin\$ share to deploy the node. Controls the actions of the node.	On the node host, grant the service account local administrator rights.

Discovery Credential (Alternate Credential) Details

By default, the node's credentials are used to enumerate scopes and access targets. If you want to use different credentials for a particular discovery, you can configure them in the Discovery Wizard.

By using alternate credentials you can target anything for which you have credentials, in any domain. You can minimize the permissions given to node credentials, and use alternate credentials for scoping and collecting your discoveries.

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

Table 5. Alternate Credentials in Configuration Manager

From	To	Permission Details	Configuration
Discovery	Node	The credentials provided are used to run the discovery. Depending on the discovery type, a variety of actions may occur, such as creating temporary files or writing to a log file. The default node credentials continue to be used to communicate with the Enterprise Reporter server and database.	Configured during the creation or editing of a discovery. Overrides the default of using the node credentials to process the discovery. Any credential used in a discovery must have local administrator access and the local logon right to all node host computers in the cluster.
Discovery	Target	Read access to all targets of the discovery. All domains with which the credentials have a forest or domain level trust will be enumerated.	On the target, ensure the alternate credentials have read access to all scopes in the discovery.

Access Explorer Agent Credential Details

The following table outlines the use of Access Explorer Agent credentials, and how to properly configure your environment to ensure successful data collection.

Table 6. Access Explorer Agent Credentials in Configuration Manager

From	To	Permission Details	Configuration
Access Explorer Agent	Enterprise Reporter Server	Writes security data acquired during a scan to the Enterprise Reporter Server.	On the managed computer, ensure the service account is configured to access an existing Active Directory® account with sufficient rights to log onto the Enterprise Reporter Server. For more information, see Adding Service Accounts on page 76.
Access Explorer Agent	Targets	Reads security data during a scan.	To install the Access Explorer agent, the service account for the agent must be a member of the Administrator group on the selected target. For more information, see Setting up a Managed Computer on page 78.

Managed Domain Credential Details

The following table outlines the use of managed domain credentials, and how to properly configure your environment to ensure successful data collection.

Table 7. Managed Domain Credentials in Configuration Manager

From	To	Permission Details	Configuration
Access Explorer Agent	Enterprise Reporter Server	Sends agent status.	The service account must have administrative access to the specified domain. For more information, see Setting Up the First Managed Domain (includes the Service Account) on page 75.
Enterprise Reporter Server	Access Explorer Agent	Configures Agent.	
Enterprise Reporter Server	Targets	Enumerates scopes.	

Access Explorer Database Credential Details

The following table outlines the use of managed domain credentials, and how to properly configure your environment to ensure successful data collection.

Table 8. Access Explorer Database Credentials in Configuration Manager

From	To	Permission Details	Configuration
Access Explorer Agent	Targets	Reads data from target.	These credentials must have the right to create databases on the target SQL Server® instance. They are subsequently used to access the database to store permission information collected from managed computers. For more information, see Setting Up the Access Explorer Database on page 74.
Enterprise Reporter Server	Access Explorer Database	Reads and writes collection data.	

Setting Up Your First Collection Computers

Before you can collect and report on data, you must set up the computers that will perform the collections. The minimum deployment is a single cluster with a single node, with the node residing on the same computer as the Enterprise Reporter server.

Configuring Clusters and Nodes for Effective Data Collection

A cluster is a logical grouping of the physical computers (nodes) that will be collecting the data. Each physical computer in a cluster is a node, and each node may belong to only one cluster. You will be assigning collection jobs to a cluster, and the collection tasks are then spread across the nodes. To help make collections more scalable, all of the computers in the cluster share a data store, where the results of a data collection are

stored. Clusters provide scalability and performance benefits—you can have as few or as many clusters as your network demands.

Figure 4 outlines a three cluster implementation of Enterprise Reporter. The server and database are located in New York, with clusters in three other cities. Each cluster contains 3 nodes.

Figure 4. A typical enterprise deployment of Enterprise Reporter



- TIP:** To maximize performance, and minimize network traffic, clusters should be physically close to the computers hosting the data you are collecting.
- NOTE:** In order to collect data, you need to create a cluster — even if you are only planning to use a single computer to perform the collections.

Things to Consider Before Creating a Cluster

Make sure you are clear on the following before creating the cluster:

Do you want to use a shared data location?

As data is collected, it is compared to previously collected data on either the SQL Server® or the shared data location, depending on how you configure your cluster. If you have a lightly loaded SQL Server® that is physically close to your nodes, you may find that performance is improved by choosing not to use a shared data location. On the other hand, if network traffic is high and your SQL Server® is under a heavy load or physically distant from the nodes in the cluster, a shared data location will produce faster results.

If you are using one, where is the shared data location?

Create the shared folder, and give read and write access to the credentials you will be using for the nodes. As long as it is accessible, the shared data location can be located on any computer in your environment. For maximum benefit, locate the data source physically close to the nodes in the cluster.

- What are the first nodes that you want to add?

A cluster is not functional until you add a node and enable it. The node computer is the computer that will resolve the targets of the collection, and perform the actual collection. You can add as many nodes as you want during the initial creation of a cluster.

- How many tasks do you want to run at the same time on each node?

Discoveries are executed as tasks on the nodes of the assigned cluster. To maximize the performance of a node, you can configure the number of tasks that can run concurrently. The default setting of five concurrent tasks is a good place to start; you can later experiment with changing this number to improve performance.

- What credentials are you going to use?

Discoveries are performed by a service that runs on the node computer. The credentials used by the node must have read and write access to the Enterprise Reporter database, and have the read permissions to access the targets, and collect the necessary data, and permission to write to the shared data location. You can optionally choose to use SQL credentials for the database connection. For more information, see [Node Credential Details](#) on page 17.

- i **NOTE:** If you use credentials that are different than the Enterprise Reporter server credentials, they need to be granted access to the database. For more information, see [Configuring the Database and Security Groups in the Dell Enterprise Reporter Installation and Deployment Guide](#).
- i **NOTE:** These credentials are also used to access the target computers during a discovery, unless alternate credentials are specified for a discovery. For more information, see [Step 1. Create the Discovery](#) on page 38.

- Access to Admin\$ on the node host

To ensure the success of node deployment, the node installation files are copied into Admin\$ (\\computername\admin\$). The service account must have read and write access to this share. Once the node has been successfully installed, you can remove this access if required.

Creating Your First Cluster and Node

The Create Cluster wizard walks you through this process. You can create a cluster without a node, and add the nodes later, but you will not be able to run a discovery without an enabled node.

To create your first cluster and node

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

A default name, First Cluster, is provided, but you should change this to something meaningful, such as the location of your cluster.

- 3 Browse to your shared data location, and click **OK**.

- OR -

Select No network share specified.

For more information, see [Things to Consider Before Creating a Cluster](#) on page 23.

- 4 Optionally, provide a description.
- 5 Optionally, modify the connection timeouts.

When you first create a cluster, it is recommended that you leave the default settings. Change the timeout settings only if you are getting timeout error messages. For more information, see [Troubleshooting Connection Timeouts](#) on page 89.

- 6 Click **Next**.

If you do not want to add any nodes at this time, skip to step 12.

- 7 Browse to the computer where the node is to be created and click **OK**.

If you do not change the default entry, the first node is created on the current computer.

- 8 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 32.

- i **NOTE:** These credentials are also used to access the target computers during a discovery, unless alternate credentials are specified for a discovery. For more information, see [Step 1. Create the Discovery](#) on page 38.

- 9 To use SQL credentials to connect to the database, select **Database Credential**, then choose SQL Authentication and select the SQL account from the Credential Manager.

- 10 Configure the number of concurrent tasks the node can process. For more information, see [Nodes](#) on page 47.

- 11 Click **Add**.

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

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

- 12 Click **Finish**.

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

The new node appears on the Discovery Nodes tab. Your node will be enabled, unless you cleared the Enable the nodes check box. For a listing of possible node statuses, see [What does the status of a node or cluster indicate?](#) on page 31.

① **NOTE:** When a node is deployed and enabled, the cluster is also enabled. If you deployed the node without enabling it, you have to manually enable the cluster. For more information, see [Enabling a Cluster](#) on page 26.

① **NOTE:** If a node fails to deploy, you must delete the node and recreate it. For information, see [Node Issues](#) on page 91.

Modifying your Deployment

For some situations, a single cluster with one node may be adequate. Other deployments may range from two or more nodes in a cluster to many clusters with many nodes in each.

When Do You Add a Cluster?

Typically, clusters are geographically based. Set up a cluster for each geographical location. You could also set up clusters to match your security structure, and group nodes into clusters based on the credentials you want to use for collections. For details on adding a cluster, see [To create your first cluster and node](#) on page 24.

Modifying a Cluster

You can change the name of a cluster, its description, and its associated shared data location. You may also want to change the timeout settings for the cluster if you are getting timeout error messages as you work in the Configuration Manager. For more information, see [Troubleshooting Connection Timeouts](#) on page 89. Another troubleshooting tool available to you is to change the level of logging for the nodes in the cluster. For more information, see [Changing the Node Logging Level](#) on page 93.

① **NOTE:** Before you change the shared data location, make sure no jobs are running. See [Viewing a Cluster's Queue](#) on page 65 and [Canceling a Task or Discovery](#) on page 66 for more information.

To modify a cluster

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 On the Cluster Details tab in the bottom pane, change the name, description, database timeout settings, node logging level, or shared data location.
- 3 Click **Apply**.

Deleting a Cluster

Before you can delete a cluster, all nodes in the cluster must first be removed. Nodes cannot be removed until all jobs have either finished processing or been canceled. For more information, see [Removing a Node](#) on page 27 and [What does the status of a node or cluster indicate?](#) on page 31.

- ① **NOTE:** A discovery is assigned to a cluster. If you delete a cluster, the discovery cannot run. Re-create the discovery and assign it to another cluster.

To delete a cluster

- 1 In the Manage Discovery Clusters pane, select the cluster.
Since the cluster has no nodes, it is in the Disabled state. If it is not disabled, you still have nodes deployed and must remove them.
- 2 Click **Delete Cluster**.
- 3 In the confirmation dialog box, click **Yes**.

Disabling a Cluster

Disable a cluster whenever you want to take all of the nodes in that cluster offline, but you know you will be using the cluster again. For example, if you need to perform maintenance tasks, you can disable a cluster. No work will be assigned to the cluster, but you can quickly bring it back online by enabling it.

To disable a cluster

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 Click **Disable Cluster**.
 - ① **MOBILE:** You can disable a cluster on your mobile device using the Enterprise Reporter Mobile IT Pack.

What To Do if a Cluster is Disabled

A cluster that is not online is indicated in red. A disabled cluster cannot accept any jobs, so you should either troubleshoot the problem and enable the cluster, or re-create the discovery and assign it to another cluster. Care should be used when re-assigning discoveries, as you may affect the network load by increasing the distance between the data and the nodes.

- ① **MOBILE:** You can view the status of your cluster on your mobile device using the Enterprise Reporter Mobile IT Pack.

Enabling a Cluster

If you have disabled a cluster, you need to enable it before it can do any work. When you enable a cluster, it enables all nodes in the cluster. This makes the cluster available for collections.

To enable a cluster

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 Click **Enable Cluster**.
 - ① **MOBILE:** You can enable a cluster on your mobile device using the Enterprise Reporter Mobile IT Pack.

Managing Nodes

You may want to change the credentials your node is using. Occasionally, nodes may need to be disabled or stopped in order to perform regular system maintenance, or as part of troubleshooting issues with your Enterprise Reporter deployment.

Modifying Node Credentials

You can modify the node credentials using the Configuration Manager. To ensure that your change goes smoothly, the new credentials should be permissioned as outlined in [Node Credential Details](#) on page 17. 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 hosting the node. If there are jobs currently running on the node, they will be canceled. To prevent this, either change the credentials during a down time, or cancel the discoveries yourself and restart them once the change takes effect.

Occasionally a credential change will fail, for example because the node host computer is not available on the network or has a firewall configured, or because you have provided invalid credentials. In this case, the node will indicate that it failed to start in the bottom pane of the Manage Discovery Clusters view. You can manually restart the service using the Services console on the remote computer. For more information, see [Troubleshooting Credential Change Failures](#) on page 90.

❗ **NOTE:** If you are performing a password update on credentials, see [Changing Passwords Using the Credential Manager](#) on page 33 for more information.

❗ **NOTE:** Nodes can potentially lock an Active Directory® password, so remember to change the password on the node whenever you update the password on the node's account.

To modify the credentials a node uses

- 1 Select **Manage Discovery Clusters**, and click the cluster containing the node.
It is recommended that you cancel any running discoveries before changing your password.
- 2 In the bottom pane, select the **Discovery Nodes** tab.
- 3 Select the node, and click **Node Properties**.
- 4 To modify the service credential, select a user account from the Credential Manager.
- 5 To modify the credential that is used to connect to the Enterprise Reporter database:
 - Click Database Credential
 - Select the type of authentication
 - If using SQL Server® Authentication, select a SQL account from the Credential Manager.

If you are using Windows® authentication to connect to the database, you must use the same account as the service credential.
- 6 Click **OK**.
A progress dialog box appears.
- 7 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.
- 8 Click **Close**.

Removing a Node

A node may need to be removed for a number of reasons, including:

- You may be replacing the computer or hard drive hosting the node service.

- Your node deployment failed. In this case, you must delete the node, and then recreate it. For more information, see [Node Issues](#) on page 91.
- You want to delete a cluster.
- You may no longer need the node.

 **NOTE:** You must disable a node before you can delete it.

 **NOTE:** When you remove a node, it uninstalls the node from the host computer. If the removal fails for any reason, you can use the Control Panel on the host computer to uninstall the Dell Enterprise Reporter Node.

To delete a node:

- 1 On the Manage Discovery Clusters pane, select the cluster.
- 2 In the bottom pane, select **Discovery Nodes** tab and select the node.
- 3 Click **Disable Node**.
- 4 Click **Remove Node**.
- 5 In the confirmation dialog box, click **Yes**.

The node's state changes to Undeploying until it is removed.

Why Disable a Node?

Disable a node whenever you want to take the node offline, but you know you will be using the node again. For example, if you need to perform maintenance tasks on the node computer, you can disable a node. No work will be assigned to the node, but you can quickly bring it back online by enabling it. You also need to disable a node before you can stop it (see [Stopping a Node](#) on page 28).

To disable a node

- 1 On the Manage Discovery Clusters pane, select the cluster.
- 2 In the bottom pane, select the **Discovery Nodes** tab and select the node.

You can multi-select nodes to disable all nodes in the cluster.

- 3 Click **Disable Node**.

If a node is actively processing a task, you will be prompted to either allow the task to finish processing, or cancel the task before disabling.

Once the action is complete, the status of the node will change to Disabled. For a listing of possible node statuses, see [What does the status of a node or cluster indicate?](#) on page 31.

 **MOBILE:** You can disable a node on your mobile device using the Enterprise Reporter Mobile IT Pack.

Stopping a Node

If you want to stop the service on the node host computer, you can use the Stop Node button. For example, this is useful when you need to change the password for your node credentials.

 **NOTE:** You must disable a node before stopping it. For more information, see [Why Disable a Node?](#) on page 28.

To stop a node

- 1 On the Manage Discovery Clusters pane, select the cluster.
- 2 In the bottom pane, select the **Discovery Nodes** tab and select the disabled node.
- 3 Click **Stop Node**.

Occasionally the server will be unable to stop a node. In this case, you can use the Services console on the node host computer to stop the node.

 **MOBILE:** You can stop a node on your mobile device using the Enterprise Reporter Mobile IT Pack.

Enabling a Node

Occasionally, a node may go offline and need to be enabled. Or, you may have chosen to create the node without enabling it. In order to be used for discoveries, a node must be enabled.

To enable a node

- 1 On the Manage Discovery Clusters pane, select the cluster.
- 2 In the bottom pane, select the **Discovery Nodes** tab and select the node.
You can multi-select nodes to enable all nodes in the cluster.
- 3 Click **Enable Node**.

 **MOBILE:** You can enable a node on your mobile device using the Enterprise Reporter Mobile IT Pack.

Starting a Node

When you start a node, it is immediately enabled, and available for processing discoveries.

To start a node

- 1 On the Manage Discovery Clusters pane, select the cluster.
- 2 In the bottom pane, select the **Discovery Nodes** tab and select the stopped node.
- 3 Click **Start Node**.

 **MOBILE:** You can start a node on your mobile device using the Enterprise Reporter Mobile IT Pack.

Improving the Performance of Your Discoveries (Load Balancing)

When a discovery is run on a cluster, the Enterprise Reporter server assigns work to its nodes. You can add nodes to a cluster at any time. Each node can only belong to one cluster. You can increase the performance of your discoveries by adding new nodes, or increasing the number of concurrent tasks existing nodes can process.

Each target is assigned to a node, balancing the distribution across the nodes until all the nodes are processing as many tasks as they are able. If no nodes are available to process the task, they must wait until a node becomes available. Node performance is based on a combination of memory, processor speed and network bandwidth. If your network, computer memory, or processor speed are less than you would like, lean towards adding nodes, not increasing the load they can handle. If your node is under used, lean towards increasing the number of concurrent tasks, not adding nodes. For more information, see [Nodes](#) on page 47.

 **NOTE:** Depending on your hardware, you may find that a node can handle several concurrent tasks at a time. When your node starts to slow down, adding more tasks will not increase performance—only adding a node will increase performance. Experiment until you find the balance of nodes and concurrent tasks for your configuration.

Adding a Node

Since a node must belong to a cluster, you must first create a cluster. For more information on creating clusters, see [To create your first cluster and node](#) on page 24.

- NOTE:** The credentials you provide are the credentials used to access the targets of your discovery. Ideally, this should be a service account that has elevated privileges, not a user account. If you use credentials that are different than the Enterprise Reporter server credentials, they need to be granted access to the database.

To create a node

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

If the account you want is not on the list, click Add and enter the credential, then select it from the list. For more information, see [Using the Credential Manager](#) on page 32.

- NOTE:** These credentials are also used to access the target computers during a discovery, unless alternate credentials are specified for a discovery. For more information, see [Step 1. Create the Discovery](#) on page 38.

- 5 To use SQL credentials to connect to the database, select **Database Credential**, then choose SQL Authentication and select the SQL account from the Credential Manager.
- 6 Configure the number of maximum concurrent tasks the node can process. For more information, see [Nodes](#) on page 47.
- 7 Click **Add**.
- 8 Repeat steps 3 through 7 to add additional nodes.
- 9 Click **OK**.

The new node appears on the Discovery Nodes tab. By default, nodes on this pane are sorted by status. Your node will be enabled, unless you cleared the Enable nodes check box. For a listing of possible node statuses, see [What does the status of a node or cluster indicate?](#) on page 31.

- NOTE:** If a node fails to deploy, you must delete the node and recreate it. For more information, see [Node Issues](#) on page 91.

Improving the Performance of a Node

You can configure a node to process fewer or more tasks simultaneously. Changing this number can help improve performance. A node processing too few tasks concurrently is not being fully utilized, while one processing too many may experience performance issues as the computer gets overloaded. It may take some experimentation to determine the optimal setting for each node.

Modifying the maximum number of concurrent tasks on a node

- 1 On the Manage Discovery Clusters pane, select the cluster to which the node to modify belongs.
- 2 On the Discovery Nodes tab in the bottom pane, select the desired node.
- 3 Click **Node Properties**.
- 4 Change the maximum number of concurrent tasks, and click **OK**.
A progress dialog box appears.
- 5 Once the change is successfully made, click **Close** in the progress dialog box.

What does the status of a node or cluster indicate?

As you deploy, enable and disable nodes and clusters, the Configuration Manager gives you feedback. This feedback is visible in the Status column of the Manage Discovery Clusters pane. By default, clusters and nodes are grouped and sorted by Status.

 **NOTE:** You can change the sort order and grouping of your nodes and clusters.

 **MOBILE:** You can view the status of your nodes and clusters on your mobile device using the Enterprise Reporter Mobile IT Pack.

The following table outlines each status of a cluster:

Table 9. Statuses of a Cluster in Configuration Manager

Status	Meaning
Disabled	The cluster is disabled and no new jobs will be processed. Any jobs currently running when the node was disabled will continue to process until they either complete or are canceled by the user.
Enabled	The cluster has at least one enabled node and is available to process jobs.

The following table outlines each status of a node:

Table 10. Statuses of a Node in Configuration Manager

Status	Meaning
Deploying	The node is currently being installed on the node computer.
Deployment Failed	The node could not be successfully deployed. For information on troubleshooting, see Node Issues on page 91.
Enabled	The node is online and available to process jobs.
Disabled	The node is disabled and no new jobs will be processed. If you attempt to disable a node while it is actively processing a task, you will be prompted to either cancel it or wait to disable the node until the task has completed.
Failed to Start	The node is still stopped, as the server was unable to start it.
Failed to Stop	The node is still running, as the server was unable to stop it. It will not accept new tasks from the server.
Faulted	The nodes regularly communicate with the server to confirm their health. A faulted node has not had contact within an acceptable time frame.
Incompatible Version	The node is not the same version of the software as the Enterprise Reporter server to which it is connecting.
Initializing	The node service is currently being configured, and required components are being downloaded to the node.
Removal Failed	The node service could not be deployed (or undeployed) successfully from the node computer.
Starting	The node service is in the process of starting up.
Stopped	The node service has been stopped. It is unavailable to process jobs until it is restarted.
Stopping	The node service is in the process of stopping.

Table 10. Statuses of a Node in Configuration Manager

Status	Meaning
Undeploying	The node service is currently being uninstalled from the node computer.
Upgrading	The node is currently being upgraded on the node computer.

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: 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.

NOTE: Credentials for Access Explorer are not stored in the Credential Manager. For more information on Access Explorer service accounts, see [Server Service Credential Details](#) on page 19.

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.

To open the Credential Manager

- On the System | Configuration page, click **Manage credentials used by Enterprise Reporter**.
- OR -
- Click the ellipsis anywhere credentials are required.

To use a credential from the Credential Manager

- Select the account from the list.
- Click **OK**.

To add a credential for use in the system

- Open the Credential Manager.
- Click **+ Add**.
- Type the account name.

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

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.

- Type the password for the account.
- Optionally, type a description.
The combination of the account name and the description must be unique.
- Click **OK**.

To edit a credential

- 1 Open the Credential Manager.
- 2 Select an account.
- 3 Click  **Edit**.
- 4 Make any changes.
- 5 Click **OK**.

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®, they need to be updated everywhere they are in use in Enterprise Reporter. It is possible that the account could 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, 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 hosting the node. If there are jobs currently running on the node, they will be canceled. 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 password on an account used by Enterprise Reporter

- 1 On the System | Configuration page, click **Manage credentials used by Enterprise Reporter**.
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 Modify the password and click **OK**.
A progress dialog box appears.
- 4 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

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 hosting the node. If there are jobs currently running on the node, they will be canceled. 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 used by Enterprise Reporter

- 1 On the System | Configuration page, click **Manage credentials used by Enterprise Reporter**.
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.
- 4 Verify that your changes were processed. If any errors occur, you will need to troubleshoot the issue and manually make any changes.

Changing the Credentials used by the Enterprise Reporter Server

The credentials you use to run the Dell Enterprise Reporter server service on the host computer are not stored in the Credential Manager. If you want to change these credentials—either to a different account, or to update the password, you need to take the following steps:

- Stop any currently running discoveries. It is important to wait until all discoveries have finished canceling to ensure the integrity of your data.
For more information, see [Canceling a Task or Discovery](#) on page 66.
- Disable all nodes in each cluster.
For more information, see [Why Disable a Node?](#) on page 28.
 **CAUTION:** At this point, you may want to inform your reporting users that they will lose connection to the Enterprise Reporter server, and they may lose work if they have not saved their latest changes.
- On the computer hosting the server, use the Services console to stop the service, then modify the properties of the Dell Enterprise Reporter Server service to use the new credentials.
See your Microsoft® documentation for details.
- Restart the service.
- In the Configuration Manager, enable the nodes.
For more information, see [Enabling a Node](#) on page 29.
- Restart any discoveries you canceled.
For more information, see [Manually Running a Discovery](#) on page 59.

Configuring Global Settings

There are several global settings on the Configuration pages that you can manage for Enterprise Reporter.

Discovery Management | Configuration

- **Change History**
You can enable or disable change history for each discovery type. For more information, see [Best Practices for Creating Discoveries](#) on page 58.
- **Extend Reporter Attributes**
You can collect more than the default attributes for Active Directory® objects. For more information, see [Managing the Collection of Additional Attributes](#) on page 67.

System | Configuration

- **Credential Manager**
You can manage credentials for use throughout the system. For more information, see [Using the Credential Manager](#) on page 32.
- **Software Improvement**
This optional program is designed so that Dell can receive anonymous feedback about the features you use, in order to continually improve Enterprise Reporter. No personal information is collected. The performance of the software is not affected.
 **NOTE:** You can opt out of the software improvement program for any component by clearing the appropriate check box in the dialog box.
- **Database Settings**
You can increase the timeout for the Enterprise Reporter server. Connection timeouts control how long the server has to establish a connection to the database, while the command timeout controls the amount of time available for processing a command on the database.
For more information, see [Troubleshooting Connection Timeouts](#) on page 89.

Access Explorer Management | Configuration

- **Configure Managed Domains**
A managed domain is an association of service accounts (user credentials) to Active Directory® domains to install agents for scanning of security information. You must install at least one managed domain to deploy Access Explorer. See [Setting Up the First Managed Domain \(includes the Service Account\)](#) on page 75.
- **Configure service accounts**
Service accounts must have administrative access to the server on which you install the Access Explorer agent service. For more information, see [Adding Service Accounts](#) on page 76.

Export logs

You can choose to export all the Access Explorer logs to two files that you can send to your Dell Support Representative. The two files (AE_Agents.zip and AE_Server.zip) can be found in a subdirectory identified by the generation date in the Exported Logs folder on the Enterprise Reporter server. The path to the two files is presented when you initiate the export. Click the link to access the two files.

For more information, see [Exporting Logs](#) on page 100.

Tips for Customizing the Configuration Manager Views

To help you view information in the Configuration Manager, you can sort columns and resize panels.

To sort a column

- Click the column header.

To change the size of a panel

- Click and drag a pane divider.

Creating and Managing Discoveries

- [Defining the Data Collection \(Discoveries\)](#)
- [Step 1. Create the Discovery](#)
- [Step 2. Choose what to include in your discovery \(Scopes\)](#)
- [Step 3. Schedule your Discovery](#)
- [Best Practices for Creating Discoveries](#)
- [How is a Discovery Processed?](#)
- [Viewing your Discoveries](#)
- [Working with Discoveries and Tasks](#)
- [Global Discovery Settings](#)

Defining the Data Collection (Discoveries)

Once you have configured a cluster, you can begin setting up discoveries. Discoveries define the targets from which you will be collecting data. Enterprise Reporter uses a "collect all" model. After you run a discovery, you can run reports that include the data you have collected. For more information on reporting, see the [Dell Enterprise Reporter Report Manager User Guide](#). Enterprise Reporter includes the following types of discoveries:

Table 11. Types of Discoveries included in Enterprise Reporter

Type	Description
Active Directory®	Collects information about your domains and AD objects within the domains, such as users, groups, sites and trusts.
Computer	Collects information specific to a computer, such as printers, shares and security policies.
File Storage Analysis	Collects information about your network's file storage capacity and usage.
Microsoft® SQL	Collects information about your Microsoft® SQL Servers®.
NTFS	Collects information about your NTFS structure—files, folders and permissions.
Registry	Collects registry keys and values from available registry hives.

 **NOTE:** The remote registry service needs to be enabled for the collection of some attributes.

There are several steps for creating a discovery. A wizard guides you through the process, which varies slightly depending on the type of discovery.

Step 1. Create the Discovery

When you are creating a discovery, it is important to consider what cluster will be running the discovery. A discovery can only belong to one cluster. When you run the discovery, the collection is performed by the nodes in the cluster.

By default, the credentials used to access the targets and read the data are those provided when creating the node. If required, you can specify alternate credentials during the creation of your discovery. For more information, see [Node Credential Details](#) on page 17.

 | **VIDEO:** Watch the video: [Introduction to Discoveries](#)

 | **TIP:** It is recommended that you assign the discovery to the cluster closest to the data.

 | **NOTE:**
You cannot change the assigned cluster once the discovery has been created.

To create a discovery

- 1 On the Manage Discoveries pane, click **New Discovery**.
- 2 Select the type of discovery. On the first page of the Create Discovery wizard, type a unique name for your discovery.
- 3 Provide an optional description that outlines the data you collect with this discovery.
- 4 Select the assigned cluster.

Your change history status is indicated. For more information, see [Best Practices for Creating Discoveries](#) on page 57.

 | **NOTE:** A cluster with a red icon is currently disabled. Your discovery cannot be run until you resolve the issue with your cluster.

- 5 To specify credentials for this discovery, select Use alternate credentials and choose an account from the Credential Manager.

For more information, see [Using the Credential Manager](#) on page 32.

- 6 Choose whether to ping computers in the discovery, and how long to allow for a response. (NTFS, computer and registry discoveries do not ping by default.)

This sets the amount of time given to confirm a computer's existence prior to attempting to collect data. Leave this option disabled if it is not possible to ping the computers in the discovery.

- 7 Click **Next** to continue to the Scope page.

Step 2. Choose what to include in your discovery (Scopes)

Scopes define the targets of the discovery. Scope options vary depending on the type of discovery you are creating. When you are choosing scopes, the credentials you use determine the available targets. If you are using default node credentials, only targets that the logged in user has access to are shown. If you provided alternate credentials when you created the discovery, those credentials are used to enumerate your scopes. For more information, see [Discovery Credential \(Alternate Credential\) Details](#) on page 20.

 | **TIP:** It is recommended that you only include a target (computer) in a single discovery for each type.

-  **NOTE:** Use care when changing credentials. Credentials must have read access to all targets of the discovery, or tasks will fail. If this is not possible for all targets, break the discovery into smaller discoveries.

Some discovery types have additional optional collections, which collect related data that add value to your reports. For example, if an NTFS discovery encounters AD groups in the security settings on an object, you can collect and report on the nested members of the groups. The data is collected for all scopes in the discovery and will add time to your discovery, so take this into consideration when selecting this option.

You may be able to enable this in a subset of your discoveries. For example, if you have six different discoveries with varying schedules that could potentially collect the same group members, you could enable it in only the discovery that is scheduled once a week, assuming that is sufficient to meet your reporting needs. In this way, performance is maximized, and reports have the data they need. It does not matter what discovery type is used to collect the data, as long as you are sure the data will be complete. Results are available for any report that includes the field.

Choosing your Active Directory® Scopes

Active Directory® scopes determine what information will be collected when you run the discovery. There are several steps you should take to properly design your discovery.

AD Discovery: Include scopes

You can include domains, OUs and containers in your scope. For full information on using the browser to add scopes, see [Using the Browser to Include and Exclude Scopes](#) on page 51.

To explicitly include objects in your scope

- 1 Click  Add.

- OR -

For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.

- 2 Expand the treeview to locate the desired object.

You can press Ctrl to select multiple objects.

You may find it helpful to filter the treeview. For more information, see [Filtering in the Browser](#) on page 54.

- 3 Click **Include** to add to your selected scopes list.
- 4 Click **OK**.

-  **NOTE:** When you add a domain, its child domains are not included—each domain must be explicitly added. When you add an OU or container, all children are included.

AD Discovery: Optionally refine your scope list with exclusions

Active Directory® excluded objects are resolved after included objects. For example, if you include an object that is below an excluded object in the AD structure, it will not be collected, as the exclusion will take precedence. For more information, see [Using the Browser to Include and Exclude Scopes](#) on page 51.

To explicitly exclude objects from your selected scope

- 1 Click  Add.

- 2 Expand the treeview to locate the object you want to exclude.
You can press Ctrl to select multiple objects.
- 3 Click **Exclude**.

AD Discovery: Optionally select a domain controller

In order to enumerate your domain, Enterprise Reporter looks to a domain controller. Depending on the domain controller chosen, the time it takes to perform the collection may vary. You can either allow Enterprise Reporter to choose the first available domain controller returned by Active Directory®, or you can select one that will optimize collection time. In this case, select a domain controller that is located physically close to the cluster you assigned to the discovery, or one that you know is a fast computer.

To set the domain controller used to enumerate a domain

- 1 Add your scopes.
For more information, see [AD Discovery: Include scopes](#) on page 39 or [NTFS Discovery: Optionally refine your scope list with exclusions](#) on page 46.
- 2 In the scopes list for the included domain you want to configure, click "..."
- 3 To use the first available domain controller returned by Active Directory®, select **Automatic selection**.
- OR -
To assign a specific domain controller, choose **Select an available domain controller**, and then select a domain controller from the list.
- 4 Click **OK**.

AD Discovery: Decide what to collect from any domain

When you run an Active Directory® discovery, it is resolved to a list of domains. You can collect a variety of information from these domains. The basic domain information, including a list of all OUs in the domain are always collected. Additionally, you can choose to collect:

- Accounts
 - Collect foreign accounts
Accounts are users, contacts, groups, and direct members of the groups. Your included domains may contain accounts from other trusted domains. If you choose not to collect these, group membership collections will not contain these foreign members. If you collect foreign accounts and any happen to be groups, you can choose to recursively collect the members of those groups.
 - Query all domain controllers for last logon
The Active Directory® LastLogonTimestamp attribute is always collected for users and computers and can be used to determine if a user or computer account has recently logged onto the domain. To determine the actual time of the most recent logon for a user or computer account, enable this option to query all domain controllers for the LastLogon attribute.
 - In addition, you may choose to collect remote desktop information for the accounts collected.
 - You may also choose to collect thumbnail photographs of domain users.
- Computers
In addition to collecting the Active Directory® attributes of each computer, you can choose to collect two attributes of the physical computer: the server type, and whether it is hidden.
- Domain controllers
- Sites

- Trusts
- Permissions

In addition to collecting Active Directory® objects, you may also choose to collect Active Directory® object permissions.

Choosing your Computer Scope

Computer scopes determine what information will be collected when you run the discovery. There are several steps you should take to properly design your discovery.

 **VIDEO:** Watch the video: [Creating a Computer Discovery](#)

Computer Discovery: Include scopes

You can specifically add domains, OUs, containers or computers. Domains, OUs and containers can contain many computers, which can significantly increase the time it takes to run the discovery.

For full information on using the browser to add scopes, see [Using the Browser to Include and Exclude Scopes](#) on page 51. You can create scopes using a dynamic query, which is resolved when the discovery is run. This gives you the flexibility to describe the computers you want to target. For more information, see [Using Queries to Define Your Scopes](#) on page 54.

 **NOTE:** Use caution when creating your queries. Ensure that the resulting set of targets is not too large for a single discovery. As well, query results should not include computers included in another discovery of the same type. If a target is in more than one discovery of a particular type, rejected tasks will appear. For more information, see [Data Collection Issues](#) on page 94.

To explicitly include objects in your scope

- 1 Click  **Add**.

- OR -

For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.

- 2 Expand the treeview to locate the desired object.

You can press Ctrl to select multiple objects.

You may find it helpful to filter the treeview. For more information, see [Filtering in the Browser](#) on page 54.

- 3 Click **Include** to add to your selected scopes list.
- 4 Click **OK**.

 **NOTE:** When you add a domain, its child domains are not included—each domain must be explicitly added. When you add an OU or container, all children are included.

Computer Discovery: Optionally refine your scope list with exclusions

Exclusions refine the inclusions you have defined. You can do this optional step in conjunction with inclusions. For full details, see [Refining Your Scope with Exclusions](#) on page 53.

To explicitly exclude objects from your selected scope

- 1 Click  **Add**.
- 2 Expand the treeview to locate the object you want to exclude.
You can press Ctrl to select multiple objects.

- 3 Click **Exclude**.

Computer Discovery: Decide what to collect from any computer in the discovery

You can collect a variety of information from the computers in your discovery. The computer attributes (such as operating system details) are always collected, and you can optionally collect:

- Printers
- Shares
 - ① **NOTE:** If you want to collect printer shares, you must enable both the Printers and the Shares check box.
- Volumes
- Accounts (Users and Groups)
 - ① **NOTE:** Accounts are not collected from domain controllers, as they are domain accounts associated with the computer, not computer accounts.
- Security Policies
- Extended WMI Entities
- Services
- Event Log Configuration
 - ① **NOTE:** Permissions are automatically collected where applicable. You can collect the members of any groups found during this collection by enabling the Collect group members check box.

Choosing Your File Storage Analysis Scopes

File Storage Analysis scopes determine what information will be collected when you run the discovery. There are several steps you should take to properly design your discovery.

File Storage Analysis Discovery: Include scopes

You can include domains, OUs and containers in your scope. For full information on using the browser to add scopes, see [Using the Browser to Include and Exclude Scopes](#) on page 51. You can create scopes using a dynamic query, which is resolved when the discovery is run. This gives you the flexibility to describe the computers you want to target. For more information, see [Using Queries to Define Your Scopes](#) on page 54.

- ① **NOTE:** Use caution when creating your queries. Ensure that the resulting set of targets is not too large for a single discovery. As well, query results should not include computers included in another discovery of the same type. If a target is in more than one discovery of a particular type, rejected tasks will appear. For more information, see [Data Collection Issues](#) on page 94.

To explicitly include objects in your scope

- 1 Click **+** **Add**.
- OR -

For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.

- 2 Expand the treeview to locate the desired object.
You can press Ctrl to select multiple objects.

You may find it helpful to filter the treeview. For more information, see [Filtering in the Browser](#) on page 54.

- 3 Click **Include** to add to your selected scopes list.
- 4 Click **OK**.

 **NOTE:** When you add a domain, its child domains are not included—each domain must be explicitly added. When you add an OU or container, all children are included.

File Storage Analysis Discovery: Optionally refine your scope list with exclusions

Exclusions refine the inclusions you have defined. You can do this optional step in conjunction with inclusions. For full details, see [Refining Your Scope with Exclusions](#) on page 53.

To explicitly exclude objects from your selected scope

- 1 Click **+** Add.
- 2 Expand the treeview to locate the object you want to exclude.
You can press Ctrl to select multiple objects.
- 3 Click **Exclude**.

File Storage Analysis Discovery: Decide what to collect from any server in the discovery

You can collect a variety of information from the computers in your discovery. The storage attributes (such as server and volume details) are always collected, and you can optionally collect:

- Files
- Folders
- Shares
- Users
- Home Directories

 **NOTE:** Selecting the Home Directory option automatically collects shares, regardless of the other options selected.

Choosing Your Microsoft® SQL Scopes

The scopes of a SQL discovery can consist of database servers, instances or databases, in any combination. There are two steps for creating your scope:

- Select what to include.
- Select what to exclude. You can exclude targets explicitly for a server or instance, or globally for all servers.

 **VIDEO:** Watch the video: [Creating a SQL Discovery](#)

 **TIP:** It is strongly recommended that each SQL Server® is included in only one discovery. Including a server in differently configured discoveries can result in data loss.

MS SQL Discovery: Include scopes

To explicitly include objects in your scope

- 1 On the Scopes page of the Create Discovery wizard, click  **Add**.
- OR -
For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.
- 2 Click the drop down arrow in the Server selection field to display a list of the SQL Servers®, instances and databases known to Configuration Manager.
- 3 To add servers, select the servers and click **Add**.
If your server does not appear on the list, you can type it in the form "SQLServerName" and click Add.
Ensure this server is not included in any other discovery.
- OR -
To add instances, select the instances and click **Add**.
If your instance does not appear on the list, you can type it in the form "SQLServerName\InstanceName" and click Add.
Ensure that this is the only discovery where the contents of the host SQL Server® are included.
- OR -
To add databases, select the databases and click **Add**.
If your instance does not appear on the list, you can type it in the form "SQLServerName\InstanceName\Database Name" and click Add.
Ensure that this is the only discovery where the contents of the host SQL Server® are included.
 **NOTE:** You can remove targets in both the Add SQL Scopes dialog box and the Scopes page of the Create Discovery wizard. Select the scopes from the list, and click Remove.
- 4 Click **OK** to close the scopes selection.
- 5 If desired, select **Collect Group Members**.
If you want to report on the members of any group included in SQL permissions, select this option. Collecting group members increases the discovery time.
- 6 Click **Next** to continue to the Exclusions page.

MS SQL Discovery: Excluding Instances and Databases From Your Scope (Scope Exclusions and Global Exclusions)

There are two ways to refine the scope of your discovery. Both are accessed on the Exclusions page of the Create Discovery wizard.

- 1 SQL scope exclusions allow you to specifically exclude:
 - an instance or database within a server
 - a database within an instance. **NOTE:** If you exclude a specific database or instance, that data will not be available for reporting, as you should not add the database or instance to another discovery.

- 2 Global exclusions allow you to exclude databases from all servers or instances included in the scope based on their names. By default, all databases that ship with Microsoft® SQL Server® are excluded.

 **NOTE:** To exclude an instance on a server, the server must be included in the scopes. To exclude a database, the server and instance must be included in the scopes.

To exclude specific instances or databases from your discovery (Scope exclusions)

- 1 On the Exclusions page of the Create Discovery wizard, click the **Scope** button.
- 2 Select the scope to modify, and click the  **Modify** button.
- 3 To exclude instances, ensure the server is expanded, then select the instances and click **Add**.

The SQL instance "MSSQLServer" is the name Enterprise Reporter gives to an unnamed instance on the server.

- OR -

To exclude databases, expand the instance, select the databases and click **Add**.

 **NOTE:** You can restore removed targets to the scope by selecting them from the Excluded Scopes list, and clicking Remove.

- 4 Click **OK**.
- 5 Repeat steps 1 through 4 for any other scopes from which you want to set scope exclusions.
- 6 Click the **Global** button to set global exclusions.

- OR -

Click **Next** to continue to the Schedule page.

To exclude all databases with a specific name from your discovery (Global exclusions)

- 1 On the Exclusions page of the Create Discovery wizard, click the **Global** button.
- 2 In the text box, type the name of the database to exclude.

 **NOTE:** You can use the * and ? wildcards when listing global exclusions.

- 3 Click  **Add**.
- 4 Click the **Scope** button to set scope exclusions.

- OR -

Click **Next** to continue to the Schedule page.

Choosing Your NTFS Scope

NTFS scopes determine what information will be collected when you run the discovery. There are a number of steps you should take to properly design your discovery.

 **VIDEO:** Watch the video: [Creating an NTFS Discovery](#)

NTFS Discovery: Include scopes

The scopes you add will determine the computers and specific folders that will be the targets of the discovery when it is run. You can explicitly add domains, OUs, containers, computers, NetApp filers, shares, DFS or NetApp file shares. Domains, OUs and containers can contain many computers, which can significantly increase the time it takes to run the discovery. For more information, see [Including Objects in Your Scope](#) on page 51.

You can create scopes using a dynamic query, which is resolved when the discovery is run. This gives you the flexibility to describe the computers you want to target. For more information, see [Using Queries to Define Your](#)

Scopes on page 54.

- ① **NOTE:** Use caution when creating your queries. Ensure that the resulting set of targets is not too large for a single discovery. As well, query results should not include computers included in another discovery of the same type. If a target is in more than one discovery of a particular type, rejected tasks will appear. For more information, see [Data Collection Issues](#) on page 94.

To explicitly include objects in your scope

- 1 Click **+** Add.

- OR -

For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.

- 2 Expand the treeview to locate the desired object.

You can press Ctrl to select multiple objects.

You may find it helpful to filter the treeview. For more information, see [Filtering in the Browser](#) on page 54.

- 3 Click **Include** to add to your selected scopes list.

- 4 Click **OK**.

- ① **NOTE:** When you add a domain, its child domains are not included—each domain must be explicitly added. When you add an OU or container, all children are included.

To explicitly include a DFS share (NTFS discoveries only)

- 1 Click **+** Add.
- 2 Click **Add DFS share**.
- 3 Type the DFS root path using the fully qualified domain name.
- 4 Click **Include** to include the DFS share.

NTFS Discovery: Optionally refine your scope list with exclusions

Exclusions refine the inclusions you have defined. You can do this optional step in conjunction with inclusions. For full details, see [Refining Your Scope with Exclusions](#) on page 53.

To explicitly exclude objects from your selected scope

- 1 Click **+** Add.
- 2 Expand the treeview to locate the object you want to exclude.
You can press Ctrl to select multiple objects.
- 3 Click **Exclude**.

To explicitly exclude a DFS share (NTFS discoveries only)

- 1 Click **+** Add.
- 2 Click **Add DFS share**.
- 3 Type the DFS root path using the fully qualified domain name.
- 4 Click **Exclude** to include the DFS share.

NTFS Discovery: Select your global scopes

Global scopes are folders that are collected from every computer in the scope. When you run the discovery, Enterprise Reporter uses the scopes you selected in the first two steps to resolve a list of computers that will be targeted. Anything you include or exclude globally is applied to these computers. Use global scopes to:

- Collect common paths on all computers. For example, if you have included computers from different Windows® Operating Systems, the path to the Windows folder may be different. Instead of having to specifically add the Windows folder, you can choose the global [WINDOWS] scope, and Enterprise Reporter can determine where that folder is located on each computer.
 - Collect specific folders or the contents of specific shares on all computers. If there is a folder that you want to collect on many of the computers, it is more efficient to include it globally. If the folder or share is not on all targets, the inclusion will be ignored for those targets.
 - Exclude common paths, specific folders or the contents of specific shares on all computers. You can make the same selections outlined above, but choose to exclude them instead of collecting them.
- ① **NOTE:** A global scope is not valid alone. You must first include a domain, OU, container, computer, NetApp filer, folder or share. See [NTFS Discovery: Include scopes](#) on page 45 for more information.
- ① **NOTE:** If you add a global exclusion that conflicts with an explicit inclusion from Step 1, the explicit inclusion will be processed, and the global exclusion will be ignored.

To add a global scope

- 1 From the Add Global list, choose the common path.
- OR -
From the Add Global list, choose the common path, then type "\" and a share or folder.
For example, select [WINDOWS] then type \Temp to include or exclude the temp folder on all computers.
- OR -
Type a share or folder.
Because these are going to be collected for all computers in the resolved discovery, you cannot include a computer name in the path. Invalid characters include "|", "[", and "]".
- 2 Click **Include** or **Exclude**.
You can press Enter to add to your list. Enter functions as the last button you clicked - for example, if you have just clicked Include, Enter includes your global scope.

NTFS Discovery: Decide what to collect from any computer in the discovery

When you run a discovery, it is resolved to a list of computers and folders. For all computers in the discovery, you need to decide what the starting point for your collection is. This combines with your global scopes and recursion level (see [NTFS Discovery: Set your recursion options](#) on page 48) to determine what folders are collected from each computer in the scope. By default, folders in public shares are collected.

If you select Folders accessible through public shares, the following data is collected:

- All folders available through public shares on any computer included in the scope, directly or indirectly
- Explicitly added folders
- Folders in explicitly added shares, DFS shares, and NetApp filers
- All globally included folders
- All folders in globally included shares

If you select Folders on all volumes, all folders on any computer resolved from the scope are collected, unless:

- they are specifically excluded from the discovery.

- specific folders or shares are the only objects included on the computer. In this case, the specified folders or the folders in the specified shares are the only data that will be collected.

NTFS Discovery: Decide how to access the folders in the discovery

There are two ways that NTFS discoveries in Enterprise Reporter can access folders, and you can choose which to use.

- Collected through the network share.

The folder will be accessed using the share path by default. This can be useful if shares are distributed, as in the case of DFS shares or Net App filers where administrative shares are disabled or not available. The NTFS object that is being shared (for example a folder) is not collected, and will not be displayed in the report. In order to collect this way, you must have read access to the share.

For example, folders and files on a share called \\NYC_SVR\TrainingMaterials that is physically located on the computer named NYC_SVR in the path c:\HR\NYC\NewHires\TrainingMaterials would be accessed and displayed as \\NYC_SVR\TrainingMaterials.

- Collect through the administrative share.

If you select Collect through the administrative share, you must access to the administrative share and have local administrator access on the target computer. The full path name from the root drive will display in the report.

In the above example, the share would be accessed as \\NYC_SVR\C\$\HR\NYC\NewHires\TrainingMaterials, and displayed in reports as C:\NYC_SVR\HR\NYC\NewHires\TrainingMaterials.

NTFS Discovery: Set your recursion options

You have three options to choose how deep into the tree the discovery will collect data:

- The default is to collect all folder levels, starting from the included scope.
- You can collect just the root level by setting the folder depth to 0.
- You can choose the number of levels to collect, starting from the included scope, by setting the folder depth as desired. The root is not counted as a recursion level. If you have an excluded scope within an included scope, no folders below the exclusion are collected. In a very complicated nested set of includes and excludes along the same branch, the recursion level is reset with each includes scope.

NTFS Discovery: Optionally collect permission data

You can collect permission information about all objects being collected. By default, permissions are not collected, as they extend the time it takes to run your discovery. If your reporting users require this data, select the Collect permissions check box.

If you collect permissions, you can choose to collect the members of any groups, by enabling Collect Group Members. The setting on the Scopes page affects both files and folder permissions.

 **NOTE:** Only the DACL and Owner permissions are collected.

NTFS Discovery: Review your scopes

The scopes are now selected and configured. It is a good idea to review your scopes before continuing. You can click Next to move on to the Files page.

NTFS Discovery: Configure your file collection

You can decide what files, if any, to collect from the folders you targeted with the scopes page. You can use both wildcards and regular expressions to include or exclude groups of files. These are applied to every scope in the discovery. Both explicit and inherited permissions are collected for all files included in the discovery.

To collect all files

- Click **Collect files**.
Include *.* appears in the list.

To use wildcards to include or exclude files

- 1 Ensure that **Using wildcards** is selected. If necessary, click to change.
- 2 Type in the desired pattern using the acceptable wildcards.
Use * to replace any number of characters, and ? to replace a single character.
- 3 Click **Include** or **Exclude**.
Your file pattern appears on the list, replacing *.*.
You can press Enter to add to your list. Enter functions as the last button you clicked—for example, if you have just clicked Include, Enter includes your file pattern.

To use regular expressions to include or exclude files

- 1 Ensure you **Using Regex** is selected. If necessary, click to change.
- 2 Type in the desired expression, using Microsoft® .NET Framework or Perl® 5 syntax.
For more information, search [Microsoft.com](https://www.microsoft.com) for Microsoft® .NET Framework regular expressions.
- 3 Click **Include** or **Exclude**.

To remove a file pattern

- 1 Select the file pattern on the list.
- 2 Click **Remove**.

To collect file permission data

- 1 Select **Collect permissions**.
- 2 To refine your collection of files, select **Only collect files with explicit permissions**.

This option may shorten the time your discovery takes to run.

 **NOTE:** If you select “Only collect files with explicit permissions”, files that only have inherited permissions are ignored when you run the discovery. These files will not be available to reporting users.

 **NOTE:** To collect the members of all groups included in the file permissions, make sure **Collect Group Members** is selected on the **Scopes** page.

To collect duplicate file information

- Select **Collect duplicate file information**.
 **NOTE:** Enabling this option locates duplicate files per computer within a single discovery by performing CRC checks to compare files that have both the same name and the same size. Collecting duplicate file information increases the discovery time.

Choosing Your Registry Scope

Registry scopes determine what information will be collected when you run the discovery. There are several steps you should take to properly design your discovery.

Registry Discovery: Include scopes

You can specifically add domains, OUs, containers, computers, hives and keys. For full information on using the browser to add scopes, see [Using the Browser to Include and Exclude Scopes](#) on page 51.

You can create scopes using a dynamic query, which is resolved when the discovery is run. This gives you the flexibility to describe the computers you want to target. For more information, see [Using Queries to Define Your Scopes](#) on page 54.

- ① **NOTE:** Use caution when creating your queries. Ensure that the resulting set of targets is not too large for a single discovery. As well, query results should not include computers included in another discovery of the same type. If a target is in more than one discovery of a particular type, rejected tasks will appear. For more information, see [Data Collection Issues](#) on page 94.

Registry Discovery: Optionally refine your scope list using exclusions

Exclusions refine the inclusions you have defined. You can do this optional step in conjunction with inclusions. For more information, see [Refining Your Scope with Exclusions](#) on page 53.

To explicitly exclude objects from your selected scope

- 1 Click **+** Add.
- 2 Expand the treeview to locate the desired domain, OU, container, computer, NetApp filer, folder or share.

You should only exclude children of the objects you have already included.

You can press Ctrl to select multiple objects.
- 3 Click **Exclude**.

Registry Discovery: Select your global scopes

Global scopes are hives or keys that are collected from every computer in the scope. When you run the discovery, Enterprise Reporter uses the scopes you selected in the first two steps to resolve a list of computers that will be targeted. Anything you include or exclude globally is applied to these computers. Use global scopes to:

- Collect a registry hive on all computers. User specific hives cannot be collected; only available hives are listed.
 - Collect specific registry keys on all computers. If there is a key that you want to collect on many of the computers, it is more efficient to include it globally. If the key is not on all targets, the inclusion will be ignored for those targets.
 - Exclude hives or keys on all computers. You make the same selections outlined above, but choose to exclude them instead of collecting them.
- ① **NOTE:** A global scope is not valid alone. You must first include a domain, OU, container, computer, hive or key. See [Registry Discovery: Include scopes](#) on page 50 for more information.
- ② **NOTE:** If you add a global exclusion that conflicts with an explicit inclusion from Step 1, the explicit inclusion will be processed, and the global exclusion will be ignored.

To add a global scope

- 1 From the Add Global list, choose a hive.

- OR -

From the Add Global list, choose the hive, then type "\" and a key.

For example, select HKEY_LOCAL_MACHINE then type \Software to include all software registry keys on all computers.

- OR -

Type a hive and key.

Because these are going to be collected for all computers in the resolved discovery, you cannot include a computer name in the path. Invalid characters include "|", "[", and "]".

- 2 Click **Include** or **Exclude**.

You can press Enter to add to your list. Enter functions as the last button you clicked—for example, if you have just clicked Include, Enter includes your global scope.

Registry Discovery: Optionally include registry values

You can choose whether or not to collect the registry values. This is disabled by default to enhance discovery performance.

Registry Discovery: Set your recursion level

You can choose how many branches deep to collect. Large registry hives can take a while to collect, so you can improve performance by restricting the number of branches.

Using the Browser to Include and Exclude Scopes

The browser is designed to allow you to drill into the acceptable objects for a given discovery type. Although the browser may vary slightly between discoveries, the basic use of it is consistent.

Your discovery should contain objects for which you want to collect similar data because:

- there are several options that are applied to every object in the discovery, such as global scopes and discovery options.
- it makes it easier to understand what you are collecting.
- you are more likely to meet the needs of your reporting users by providing consistent data.

 **NOTE:** The account you are logged in as is used to enumerate the scopes. If you are not seeing the expected objects in your browser, check your permission level.

Including Objects in Your Scope

A valid discovery requires that you include at least one object. You can explicitly include high-level objects—domains, OUs and containers. This implicitly adds all computers in the selected object. For some discovery types, you can include objects using a query for more flexibility. See [Using Queries to Define Your Scopes](#) on page 54 for more information. When you run the discovery Enterprise Reporter resolves the high level object to a list of targeted computers, or in the case of an AD discovery, to a list of domains. These can be useful because if the contents of the container change, so do the targets of the discovery. Once Enterprise Reporter resolves this list, the other options in the scope can be applied.

 **TIP:** It is strongly recommended that each computer is included in only one discovery. Including a computer in differently configured discoveries can result in data loss. If you add individual computers, ensure that they have not already been implicitly included in another discovery by way of a domain, OU, or container.

Depending on the discovery type, you may also be able to select:

- **Specific computers**—You can drill into domains, OUs and containers and select individual computers. All options in the scope are applied to each selected computer, including global scopes.
- **Folders and shares**—You can drill into a computer and select folders and shares. All relevant options in the scope are applied.
- **Registry hives and keys**—You can drill into a computer and select specific hives and keys. Because the local registry hives are not available for collection, they are not available to select. When you include a specific folder or share, Enterprise Reporter interprets this to mean that is all you want to collect from the host computer; global scopes will not be applied.
- **DFS Shares**—A published Windows® Server DFS share can be added like any other share, from the System\Dfs-Configuration container within a domain. You can use the Browse dialog box to manually add all other DFS shares.

 **NOTE:** When you include a specific folder, share, or registry entry, Enterprise Reporter interprets this to mean that is all you want to collect from the host computer; global scopes will not be applied. When you exclude a specific object, Enterprise Reporter collects everything on the computer except that object, taking in to account the global scopes.

 **NOTE:** If you select competing scopes, the parent object will be collected. For example, if you include a computer, and a specific path on a computer (which on its own would only collect that path), the entire computer will be collected.

To explicitly include objects in your scope

- 1 Click  **Add**.

- OR -

For all discovery types except Active Directory, if you have a text file containing the computers to be selected, click **Import** and follow the steps as outlined in [Importing Computers to Your Scopes](#) on page 52.

- 2 Expand the treeview to locate the desired object.

You can press Ctrl to select multiple objects.

You may find it helpful to filter the treeview. For more information, see [Filtering in the Browser](#) on page 54.

- 3 Click **Include** to add to your selected scopes list.
- 4 Click **OK**.

 **NOTE:** When you add a domain, its child domains are not included—each domain must be explicitly added. When you add an OU or container, all children are included.

To explicitly include a DFS share (NTFS discoveries only)

- 1 Click  **Add**.
- 2 Click **Add DFS share**.
- 3 Type the DFS root path using the fully qualified domain name.
- 4 Click **Include** to include the DFS share.

Importing Computers to Your Scopes

On the scopes page, instead of using the Add button to add one computer at a time, you may choose to import multiple computers from a file for the following types of discoveries:

- Computer
- Microsoft® SQL

- NTFS
- Registry

You may import from any text file containing a list of the fully qualified domain names (or IP addresses) of the computers to be targeted with one computer per line, as in the following example:

```
\\computer1.domain.com
\\192.168.10.25
computer3.domain.com
```

Only unique computer names free of invalid characters will be imported.

To import computers to your scopes

- 1 On the scopes page, click the **Import** button.
- 2 Browse to locate the file containing the computers to be added.
- 3 Select the file and click **Open** to start the import.
- 4 Review the import progress and results messages and click **OK** when complete.
 -  **NOTE:** Any computer that is not successfully imported will be indicated by a red dot next to its name with an error description in the Message column.
- 5 Successfully imported computers will be visible in the Selected Scopes pane.
- 6 Optionally, fix any errors in the text file and repeat steps 1 through 5 until all computers are imported.
 -  **NOTE:** There is no need to remove previously imported computers from the text file as only unique computer names will be loaded during subsequent imports.

Refining Your Scope with Exclusions

This step can be done in conjunction with the inclusions. Exclusions refine your scope further. Use the browser or a query to exclude scopes.

For example, you can add a computer, but exclude a specific folder; or add a domain and exclude a specific OU. The following rules are used to process your exclusions:

- If you add an exclusion without the inclusion of a parent, it has no meaning and will be ignored. As long as the exclusion can be traced up the AD tree to a parent object, the exclusion can be processed.
- If you explicitly exclude a folder or share, that data will not be available for reporting. You should not add the folder or share to another discovery, as data loss can occur if a computer is targeted by more than one discovery. You can, however, exclude an entire computer from a domain, OU or container, and include that computer in a different discovery.
- For an Active Directory® discovery, excluded objects are processed after included objects. Any OU or container that is included below an excluded one in the AD structure will not be included, as the exclude will take precedence.

To explicitly exclude objects from your selected scope

- 1 Click  **Add**.
- 2 Expand the treeview to locate the object you want to exclude.
You can press Ctrl to select multiple objects.
- 3 Click **Exclude**.

To explicitly exclude a DFS share (NTFS discoveries only)

- 1 Click  **Add**.
- 2 Click **Add DFS share**.

- 3 Type the DFS root path using the fully qualified domain name.
- 4 Click **Exclude** to include the DFS share.

Filtering in the Browser

It can be difficult to find the objects you are looking for when you are selecting your scope. To address this, you can use filtering in the browser. Filtering starts from your selected location, and is applied one level down. For example, if you filter at the domain level, the filter is applied to the first level containers. You remove filters one at a time, starting with the last filter you applied.

To apply a filter

- 1 Expand the tree, and then select your starting point.
You must expand the first level of the selected node in order for the filter to work.
- 2 In the **Apply filter to** box, type your search string.
- 3 Click **Apply Filter**.

 **NOTE:** You can also right-click any node on the tree and choose Filter.

To remove a filter

- 1 Click **Undo Filter** to remove the last filter applied.
The details of the filter you will remove are displayed in the "Last Filter applied to" box.
- 2 Repeat if needed to remove other filters.

Using Queries to Define Your Scopes

Queries can be used on their own or to complement explicit scopes for the following types of discoveries:

- Computer
- File Storage Analysis
- NTFS
- Registry

Queries allow you to define a set of criteria that will be resolved when the discovery runs. For example, you can create a query that looks for computer names that contain "Finance" across an entire domain. When the discovery runs, the query will execute and resolve a list of targets. Queries can be run against a particular domain, a container in a domain, or against all child domains of the domain you are currently logged in to. By default, queries create an included scope, but you can modify it to be excluded if you want.

 **NOTE:** Only queries based on computers, organization units and containers are relevant. Other parameters will be ignored.

To include a scope using a query

- 1 Click  **Add**.
- 2 Click **Add scope using a query**.
- 3 To choose a specific domain to target with the query, select it from the In list.
- OR -
To choose a specific container or OU to target, click **Browse**, locate the target and click **OK**.
- OR -
To target the current domain and all child domains, from the In list, select **Entire Directory**.

- 4 From the Find list, select **Computers**, **Organizational Units** or **Custom Search**, then make your selections on the tabs shown.

Each selection you add builds a query. Ensure the Custom Search only includes computers, containers and organizational units. Note that on the Advanced tab of the Custom Search option, you can use any appropriate LDAP query. To test your query, click Find Now.

- 5 Click **OK** to save your query.

The query is saved, and the domain against which it will run is shown in the scopes list. To view the query, you can hover over the domain name. If the query was run against the Entire Directory, the originating domain is shown, and all its trusted domains will be queried when the discovery is executed.

To exclude objects using a query

- 1 Follow the steps for adding a query. See [To include a scope using a query](#) on page 54.
- 2 In the Selected Scopes list, right-click the query and select **Exclude**.

Step 3. Schedule your Discovery

There are four types of schedules you can create. These are the same as the schedule types you can create to run reports in the Report Manager. You can only create one schedule per discovery. You can also run your discovery manually at any time (see [How is a Discovery Processed?](#) on page 57 for more information).

NOTE: All times are stored in UTC format. They will not be adjusted when your local time changes, such as for Daylight Savings Time.

NOTE: Once you create a schedule for the discovery, you can see the next scheduled run in the main Manage Discoveries pane. For more information, see [Viewing your Discoveries](#) on page 58.

MOBILE: You can view your discovery schedules on your mobile device using the Enterprise Reporter Mobile IT Pack.

- [Run your discovery once](#)
- [Run your discovery on a daily interval](#)
- [Run your discovery on specified days of the week](#)
- [Run your discovery on a specified day of the month](#)

Run your discovery once

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

To schedule a single run of your discovery

- 1 On the Schedule page of the Create Discovery wizard, click **Run Once**.
- 2 Select the date and time.
- 3 Click **+ Add**.

Your schedule appears in the bottom pane of the Wizard. If it is not the schedule you want, click **Remove**.

- 4 Click **Finish** to complete the creation of your discovery.

Run your discovery 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 discovery to run daily

- 1 On the Schedule page of the Create Discovery wizard, click **Daily**.
- 2 Select the date and time.
- 3 Set the interval for your daily run.

- 4 Click **+ Add**.

Your schedule appears in the bottom pane of the Wizard. If it is not the schedule you want, click **Remove**.

- 5 Click **Finish** to complete the creation of your discovery.

Run your discovery on specified days of the week

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

To schedule a discovery to run on selected days

- 1 On the Schedule page of the Create Discovery wizard, click **Weekly**.
- 2 Select the date and time.
- 3 Select the days on which you want your discovery to run.

- 4 Click **+ Add**.

Your schedule appears in the bottom pane of the Wizard. If it is not the schedule you want, click **Remove**.

- 5 Click **Finish** to complete the creation of your discovery.

Run your discovery on a specified day of the month

You can select a certain day of the month to run your discovery. 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 discovery to run on a specified day of the month

- 1 On the Schedule page of the Create Discovery wizard, click **Monthly**.
- 2 Select the date and time.
- 3 Select the day of the month on which you want your discovery to run.

- OR -

Select the weekly interval and day of the month.

- 4 Click **+ Add**.

Your schedule appears in the bottom pane of the Wizard. If it is not the schedule you want, click **Remove**.

- 5 Click **Finish** to complete the creation of your discovery.

Best Practices for Creating Discoveries

To get the best performance, and meet the needs of your reporting users, there are a number of things you should consider:

- Group together targets in a discovery based on the data you are collecting.

A discovery should collect generally the same data from all targets. For example, if you have some targets from which you only want to collect the Windows folder, and other targets from which you want to collect both the Windows and Program Files folders, you should create two different discoveries. This makes it easier to design and maintain discoveries.

- Each discovery must be assigned to a cluster. Assign the discovery to the cluster geographically closest to the targets. If necessary, break a discovery up into smaller discoveries to accomplish this.
- The default settings of a discovery are designed to optimize performance. If you are going to change them, ensure that your reporting users require the data you are collecting.
- Make sure you understand how fresh the data needs to be in order to satisfy the needs of your reporting users. Schedule your discoveries to meet these needs.
- A computer should only be in a single discovery of any one type.

For example, you cannot break up a SQL Server® into two SQL discoveries. Or, if you include a domain in an NTFS discovery, a computer contained in that domain should not be in a different NTFS discovery. However, you can collect both SQL and NTFS data from the same computer, since you use two different types of discoveries to accomplish this.

How is a Discovery Processed?

 **VIDEO:** Watch the video: [How Discoveries are Processed](#)

When a discovery runs, the process is as follows:

- The server dispatches the resolution task to an available node in the cluster.
- The resolution task reduces the scope to the smallest possible number of tasks. As the tasks are resolved, they go into the queue and are assigned sequentially to the nodes within the assigned cluster. Nodes can continue to accept tasks until they reach their maximum number of concurrent tasks.

 **NOTE:** A task may be rejected if the target is already being collected by another discovery.

- If no nodes are available to process a task, the discovery is in the queue in a Pending state. When a node becomes available, the discovery will begin processing.
- If the task is a collection task, data is written to the database, the last collected time for the parent object is updated, and if there are changes to any data, the timestamp is updated. The collector examines existing data and compares it to the new data, and only sends changed information to the database. This keeps network traffic to a minimum.

 **NOTE:** You can see the number of items that have been changed, and therefore updated, in the statistics for the task. For more information, see [Viewing Statistics](#) on page 63.

- Once all tasks have been processed, the discovery is finished.

 **NOTE:** For information on configuring nodes, see [Creating Your First Cluster and Node](#) on page 24 and [Improving the Performance of Your Discoveries \(Load Balancing\)](#) on page 30.

Types of Tasks

Each discovery is broken down into tasks for processing. You will see these task types as you manage your discoveries. There are several types of tasks.

Table 12. Types of Tasks in Configuration Manager

Task Type	Description
Resolution	Examines your scope and reduces it to the smallest number of targets. For an Microsoft® SQL discovery, a target is a SQL Server®.
Discovery	Displays as the name of the target. A discovery task collects the data from the target and updates the Enterprise Reporter database.
Group Membership	When the collection requires information from other targets, to improve performance the work is performed at the end of the collection. This can prevent the same data from being repeatedly collected.

Manually Running a Discovery

You can manually run a discovery at any time. Regardless of how you execute a discovery, it is always put in the queue for processing— even if it is already running. This could result in an unintentional drain on your resources, tasks being rejected, or confusion about the age of your data. Before you manually run a discovery, you should check and see when it is next scheduled to run. You can tell when a discovery is scheduled to run again by looking at the Next Run column in the Manage Discoveries main view.

To manually run a discovery

- 1 On the Manage Discoveries pane, select the discovery.
- 2 Click Run.

 **MOBILE:** You can run a discovery from your mobile device using the Enterprise Reporter Mobile IT Pack.

Viewing your Discoveries

Ideally, you can configure and schedule your discoveries, and the Configuration Manager will run discovery jobs to provide fresh data to the Report Manager at the intervals you have specified. However, many things may arise that require your attention. For example, a SQL Server® may go offline, or another user may cancel your discovery. Or, you may receive inquiries from users about the freshness of the data, or whether a particular object is included in the data on which they are reporting.

The main Manage Discoveries pane is a listing of all the discoveries created on any console connected to your Enterprise Reporter server. By default, they are grouped by cluster, and sorted by discovery name. An arrow in the column header indicates the current sort.

A snapshot of the current state of each discovery is shown. For each discovery, you can see:

- A red indicator if there were errors on the last run. This indicates that all of the requested data was not collected.

- How long the discovery took to execute its last run. This time is measured from the time the discovery was submitted to the server until the last task finishes running.
 - ① **NOTE:** The total time for the discovery to complete may actually be longer than the sum of its tasks, as the cluster may have been processing other discoveries at the same time, or there may have been issues on the node or server.
- The results of the last run—whether it finished, finished but was unable to collect all of your data, or canceled.
- When your discovery was last run. This will be empty until the first successful completion of the discovery.
- The next run of the discovery. This is calculated based on the discovery’s schedule.
 - If the discovery is currently running, this column contains a Processing link, which you can click to view the tasks for the discovery. For more information, see [Viewing the Tasks for a Processing Discovery](#) on page 61.
 - If the discovery is waiting to run, this column contains a Pending link that you can click to view the tasks for the discovery.
 - If the discovery is not running, the date and time of the next run is shown.
 - If the discovery is not scheduled, and is not processing or pending this column is empty.
- ① **MOBILE:** You can view your discoveries, including last status and number of errors, on your mobile device using the Enterprise Reporter Mobile IT Pack.

Navigating the Manage Discoveries Pane

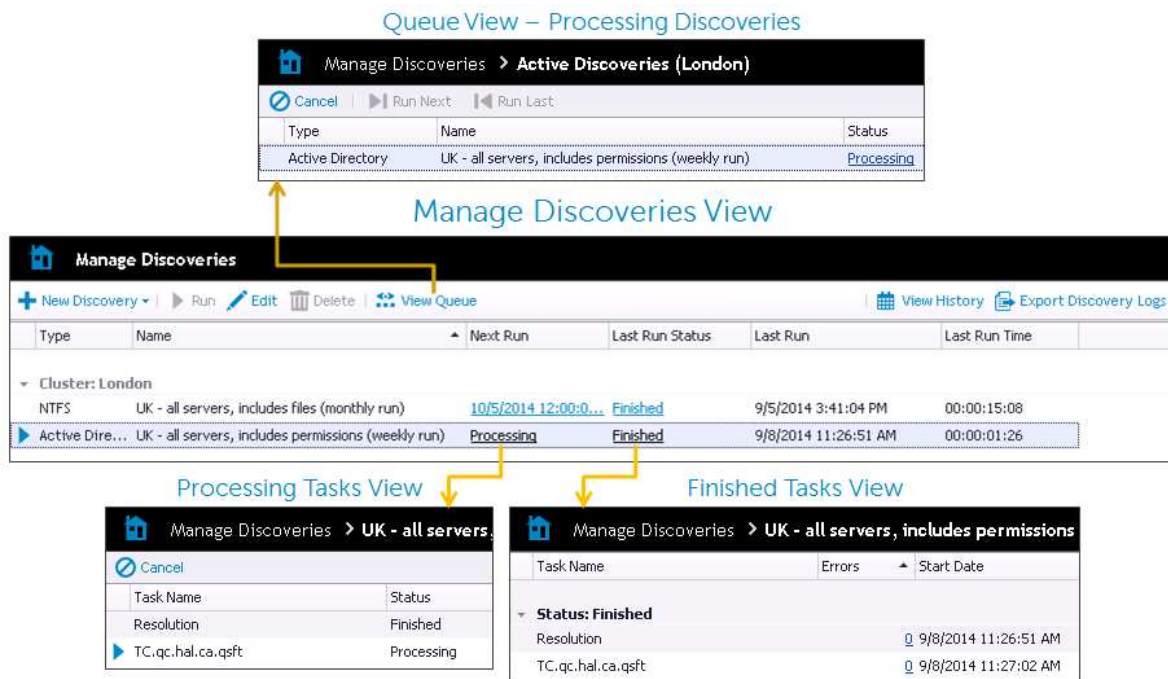
The Manage Discoveries pane is actually a series of views designed to allow you to see the progress of your discoveries and to aid in troubleshooting any issues that arise during a collection. In the main Manage Discoveries view, you can create, edit, and run discoveries.

The Manage Discoveries pane uses a drill down approach:

- You can drill down into the last completed run of the discovery and see the details of each task that was processed.
- You can drill down into a currently processing discovery, and see:
 - The tasks for the discovery being processed. This lets you see all the work currently being processed or waiting to be processed.
 - The activity currently taking place. For each task, you can see details of what is currently being processed by the assigned node.
 - The current state of the tasks in your discovery, along with the errors and statistics for each task.

As you drill down into your processing or completed discoveries, a breadcrumb bar helps you understand the context of the information on your screen. At any time, you can click the Manage Discoveries breadcrumb to return to the main Manage Discoveries view. [Figure 5](#) outlines how you can access the details of your completed or processing tasks.

Figure 5. A summary of the views in the Manage Discoveries pane



To display the main Manage Discoveries pane

- From within the Manage Discoveries pane, click the **Manage Discoveries** breadcrumb.

- OR -

From another pane, on the Navigation pane, click the **Manage Discoveries** button.

Viewing the History of a Discovery

Enterprise Reporter keeps a history of the last ten runs of each discovery. This can be an aid in troubleshooting – for example, you can see where an error first started appearing in a discovery.

To view the history of a discovery

- On the Manage Discoveries page, select a discovery.
- Click **View History**.
- To view the tasks for a discovery, click the status link.

What Does the Discovery Status Indicate?

The status of a discovery is largely dependent on the status of the tasks within the discovery. For more information, see [What Does the Task Status Indicate?](#) on page 62. There are several locations you can view the status of a discovery on the Manage Discoveries page:

- The Last Run Status column tells you the status of the last completed run of the discovery.
- If a discovery is currently being processed, the Next Run column indicates its current status.
- After the first run, when a discovery is running you have access to both the status of the last run and the current run.
- You can see the status of any completed discovery run when you view the history of a discovery.

The following table outlines the available discovery statuses:

- ① **MOBILE:** You can view the status of a discovery on your mobile device using the Enterprise Reporter Mobile IT Pack.

Table 13. Discovery Statuses in Configuration Manager

Discovery Status	Description
Pending	The discovery is in the queue, but has not yet started processing. This can be as a result of manual or scheduled run of the discovery.
Processing	Once the first task of a discovery is processed (the resolution task), the discovery goes into a processing state, and remains there until the discovery is canceled or all tasks complete.
Canceled	Indicates that the discovery has been successfully canceled.
Finished	Indicates that all tasks have finished with no errors.
Finished with Failures	Indicates that all tasks have finished, but at least one task failed.
Failed	Indicates that all tasks have finished, but they all failed.

Viewing the Tasks for a Finished Discovery

Each discovery that has finished at least once has a list of tasks associated with it. Viewing this list is particularly useful if there were errors in your discovery. You can pinpoint exactly which targets are causing errors. The completed tasks are grouped by status, so you can easily see the outcome for each task. For each task, you can also see:

- The type of task. For more information, see [Types of Tasks](#) on page 58.
- The time the task started running.
- The total time it took to process the task.
- Errors and statistics for the task. For more information, see [Viewing Errors](#) on page 63 and [Viewing Statistics](#) on page 63.

To view a finished discovery

- 1 Display the main Manage Discoveries pane.
- 2 Select the discovery.
- 3 Click the status link in the Last Result column for the discovery.

The breadcrumb bar indicates the date and time the discovery was submitted for processing.

Viewing the Tasks for a Processing Discovery

If a discovery is currently running, you can view all tasks for that discovery. You can use this view to troubleshoot issues with your discovery, and to cancel a running task. For each task, you can see:

- A red indicator if errors occurred during the processing of the task.
- An arrow beside a task if it is currently processing.
- The status of the task. This indicates whether the task is currently processing, pending, or finished. For more information, see [What Does the Task Status Indicate?](#) on page 62.
- The number of errors that occurred during the processing of the task.
- The time the task started processing.

- The time it took to process the task, or the current elapsed time.
- The node to which the task was assigned. A node can be configured to process multiple tasks at once. For more information, see [Improving the Performance of Your Discoveries \(Load Balancing\)](#) on page 30.
- The current activity on the node. This is a live stream of the work the node is performing, and you can use this to keep track of the progress of the task.

To view tasks for a processing discovery

- 1 Display the Manage Discovery pane main view.
- 2 Select the discovery.
- 3 In the Next Run column for the discovery, click the **Processing** link.

The breadcrumb bar indicates that you are viewing the processing tasks for the discovery.

You can see all tasks for the discovery, including tasks that have finished processing.

What Does the Task Status Indicate?

The status of the tasks in your discovery give you information about the how your discovery is being processed. You can view the status of a task in both the processing and finished task views of a discovery. By default, tasks are grouped by status. The following table outlines the statuses you may see:

Table 14. Task Statuses in Configuration Manager

Task Status	Description
Pending	When a discovery is run, each task has to be assigned to a node. If the node is already running its maximum number of concurrent tasks, the task is Pending. It is in the queue, and will be assigned to a node when one becomes available.
Dispatching	When a node becomes available, the task is sent to it for processing. While this is happening, the task status is Dispatching.
Processing	The task is running on the assigned node
Canceling	The server has received your request to cancel the task, and is communicating this to the node.
Canceled	The task has been canceled.
Finished	The task has successfully completed.
Failed	The task has completed, but was unable to collect all of the data you requested. For more information, see Viewing Errors and Statistics for Tasks on page 96.
Rejected	A task is rejected if the same target is already being accessed by a node within the cluster. This can happen when the same discovery is run more than once within a short time.

Why is My View Empty?

Two views in the Configuration Manager show currently processing tasks or discoveries: the cluster's queue, and the active tasks view. If there is nothing currently being processed, these views will be empty.

Viewing Errors

When there are errors during the discovery, a red indicator appears beside the discovery. If you drill into a task view, you can identify the exact task that caused the error. Then, for that task, you can view a list of errors, which explains what was happening at the time of the error, and the problem that was encountered. If you are searching for a specific error, you can filter the errors to help narrow your search.

-  **NOTE:** If you have used alternate credentials on a discovery, and your resolution task fails, ensure that you have administrator rights on all node host computer in the assigned cluster.
-  **MOBILE:** You can see the number of errors on a discovery on your mobile device using the Enterprise Reporter Mobile IT Pack.

To view the errors for a task

- 1 Display the tasks for an active or finished discovery.
Tasks with a red indicator have errors and display the number of errors as a link in the Errors column.
- 2 Select a task with errors.
- 3 Click the link in the Errors column.
- OR -
In the bottom pane of the view, click **View Errors** in the red status bar.

To sort a column

- Click  to sort in descending alphabetical order (Z to A).
- Click  to sort in ascending alphabetical order (A to Z).

To filter a column

- Click  in a column heading to display a list of every entry in that column and select a value on which to filter.
 - (Blanks) displays rows with a blank entry in that column.
 - (Non-blanks) displays rows with an entry.
 - (Custom) opens a Custom AutoFilter where you can create a custom filter.
- OR -

If an empty row is displayed under the column headers, enter text in each column of this row to perform an exact-match search to narrow the results.

To clear a filter

- With a filter selected for a particular column, click  in that column heading and choose (All).

Viewing Statistics

Statistics provide information about what was collected during the discovery. Statistics are displayed once all information for that discovery is collected. When the discovery is complete, a full listing of the objects found and a summary of the database changes appears.

Only items that have changed since the last time the discovery ran are updated in the Enterprise Reporter database. This keeps your database up to date, while enhancing performance. You can see how many items

were updated by examining Total Added, Total Changed and Total Deleted. If you see that objects were discovered but not updated, this means that they have been previously added to the database.

- ① **NOTE:** When processing the ACEs in a discovery, only unique ACEs are processed. For example, if 20 ACEs are discovered across all objects, but ten of those ACEs are identical, only one copy of that ACE is actually added to the database.

To view the statistics for a task

- 1 Display the tasks for an active or finished discovery.
- 2 In the bottom pane of the view, click the **Statistics** tab.

Viewing a Cluster's Queue

Each cluster maintains a queue for currently running discoveries. You can see the queue for a cluster whenever you have a processing discovery. The queue is a live view, so only discoveries that are currently processing or waiting to be processed are shown. As discoveries finish processing, they disappear from the queue.

For each discovery being processed, the queue shows the current status, and the number of errors encountered to date during the collection. You can drill into a discovery and see the status of individual tasks. You can also cancel a running discovery. For more information, see [Canceling a Task or Discovery](#) on page 65.

- ① **NOTE:** If a discovery is in a cluster's queue, but not yet processing (in a Pending state) it means that the node is already processing its maximum allowable concurrent tasks. If you find that you often have discoveries queued, you may want to consider increasing this number on the existing nodes, or adding another node. For more information, see [Improving the Performance of Your Discoveries \(Load Balancing\)](#) on page 30.

To view the queue for a cluster

- 1 Click **Discovery Management | Manage Discoveries**.
 - 2 Select the discovery or cluster.
 - 3 On the task bar, click **View Queue**.
- If there are no discoveries being processed, the queue is empty.

Working with Discoveries and Tasks

Occasionally, you may need to modify a discovery, or stop a discovery or task from running. If you want to permanently stop the discovery from running, remember to remove the schedule.

Modifying a Discovery

You can modify all elements of your discovery using the same pages you used to create it, except the assigned cluster.

- ① **NOTE:** If you want to move the discovery to a different cluster, create a new discovery and assign it to the desired cluster. Discoveries should be assigned to the cluster located closest to its targets.

To modify a discovery

- 1 Click **Discovery Management | Manage Discoveries**.
- 2 Select the discovery.
- 3 Click **Edit**.
- 4 Navigate to the desired page of the Edit Discovery dialog box by clicking the desired button. Make your changes.

- 5 Click **OK**.

If you want to save the changes before moving to another page, click **Apply**. For example, you must save your scope changes before you can set scope exclusions. Once you click **Apply**, you cannot cancel the saved changes.

Canceling a Task or Discovery

If you want to stop a discovery or a task in a discovery from running, you can cancel it.

To cancel discoveries

- 1 Click **Discovery Management | Manage Discoveries**.
- 2 Select the discovery you want to cancel.
- 3 Click **View Queue**.
- 4 Ensure your discovery is selected and click **Cancel**.
- 5 Click **Yes** to confirm the cancellation.

① **MOBILE:** You can cancel a discovery on your mobile device using the Enterprise Reporter Mobile IT Pack. You can cancel either the currently processing run, or all runs.

To cancel tasks

- 1 Click **Discovery Management | Manage Discoveries**.
- 2 Select the discovery, and click the **Processing** link for the discovery to access the tasks.
- 3 Select the tasks to cancel.
- 4 Click **Cancel**.
- 5 Click **OK** to confirm the cancellation.

Deleting a Discovery

You can only delete a discovery when there are no tasks currently running. Deleting a discovery does not delete any previously collected data. If the last run status is processing, you must wait until it is finished before you can delete the discovery. Alternatively, you can cancel the running tasks in the discovery, or cancel the discovery, and then delete it. For more information, see [Canceling a Task or Discovery](#) on page 65.

① **NOTE:** If there is more than one Enterprise Reporter administrator in your organization, use caution when deleting a discovery, as it will no longer be available to any user.

To delete a discovery

- 1 Click **Discovery Management | Manage Discoveries**.
- 2 Select the finished discovery.
You can select more than one discovery using Ctrl+click.
If any selected discovery has tasks running, the Delete button is unavailable.
- 3 Click **Delete**.
- 4 Click **Yes** to confirm.

Global Discovery Settings

There are settings which affect all discoveries of a given type:

- [Configuring Change History](#)
- [Managing the Collection of Additional Attributes](#)

Configuring Change History

Change history allows you to report on changes over time to the objects you discover. For example, if you choose to collect the change history for the NTFS discovery type, and a new file is added to a previously collected folder, you can see this reflected in a change history report.

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

In addition to the discoveries you can create and run in Enterprise Reporter, there is additional information that is common to more than one type of discovery, such as user accounts, groups or group members. To collect change history information for this data, enable change history for the Common discovery type.

To enable or disable change history for a discovery type

- 1 Click **Discovery Management | Configuration**.
- 2 Click **Configure global change history settings**.
A button shows the current status of the change history configuration for each discovery type.
- 3 Click the **Enabled** or **Disabled** button to toggle the setting.
- 4 Click **Close**.

Managing the Collection of Additional Attributes

Enterprise Reporter collects a pre-defined set of attributes for each object in a discovery. The attributes collected vary depending on the type of discovery, the object, and the version of Enterprise Reporter you are using. You can add and remove attributes collected by Active Directory® and computer discoveries. You can extend:

- Active Directory® discovery attributes for users, groups, computers and organizational units.
- Computer discoveries with attributes from WMI classes added.

Attributes you extended in previous versions of Enterprise Reporter may become default attributes in newer versions. In this case, the extended attribute is preserved to ensure that your reports continue to work, but only the default attribute is available for new reports.

When you add or remove attributes for a discovery type, Enterprise Reporter has to process them. This can take some time, during which any running discoveries of the type you extended may fail. You should perform the extension only after ensuring that no discoveries of that type are running or scheduled to run. Additionally, any attributes that are no longer being collected should be removed from any reports in which they were included.

TIP: In order to minimize collection time, it is recommended that you only collect attributes that you know are required by your reporting users. You cannot remove attributes that are collected by default.

NOTE: Reporting users will need to restart their consoles in order to have the most up to date list of available attributes in their reports. Consider informing users that data is no longer being collected, so they can remove the associated fields from their reports.

To add or remove Active Directory® attributes

- 1 Ensure that no Active Directory® discoveries are running or scheduled to run while your changes are processed.
- 2 Click **Discovery Management | Configuration**.

- 3 Click **Manage attributes collected by Enterprise Reporter**.
- 4 Click **Yes** in the warning dialog box.
- 5 In the Active Directory® section, click **Extend**.
- 6 If you want to use a different forest to enumerate the schema, click the **Browse** button and select an appropriate domain.

If your logged in user does not have access to a domain in the forest whose schema you want to enumerate, right-click in the dialog box and choose **Connect as user**.
- 7 Click **Get Schema**.

The Extend Enterprise Reporter Attributes dialog box is displayed. Default attributes have grey check marks. Extended attributes have green check marks for easy identification.
- 8 Select the type of attributes to collect from the **Type** menu.
- 9 Select to add or deselect to remove attributes.

To view a list of your currently selected attributes, select **Only show selected attributes**.
- 10 Click **Apply**.
- 11 Click **Close**.

To extend computer attributes (using WMI classes)

- 1 Ensure that no computer discoveries are running or scheduled to run while your changes are processed.
- 2 Click **Discovery Management | Configuration**.
- 3 Click **Manage attributes collected by Enterprise Reporter**.
- 4 Click **Yes** in the warning dialog box.
- 5 In the Computer section, click **Extend**.
- 6 Click **+ Add**.

If you want to use a different computer to enumerate the WMI classes, click the ellipsis and select the computer.

The Extend Enterprise Reporter Attributes dialog box is displayed. Any classes that have been extended are shown.
- 7 Expand the WMI class treeview as necessary to locate the desired classes.
- 8 Select the classes and click the **Add** button.

You can only add entire classes, not individual properties.

To remove classes, select them from the list and click the **Remove** button.
- 9 Click **Add**.

The Extend Enterprise Reporter Attributes dialog box reappears, with the newly added classes bolded.

If you add more than the recommended number of classes, a warning appears. Ensure that you require the selected extended WMI classes, as they will increase your collection time.
- 10 Verify the list and then click **Apply**.

To remove computer attributes (non-default)

- 1 Ensure that no computer discoveries are running or scheduled to run while your changes are processed.
- 2 Click **Discovery Management | Configuration**.
- 3 Click **Manage attributes collected by Enterprise Reporter**.
- 4 Click **Yes** in the warning dialog box.
- 5 In the Computer section, click **Extend**.

The Extend Enterprise Reporter Attributes dialog box is displayed. Any classes that have been extended are shown.

- 6 Select the desired classes and click **Remove**.
- 7 Click **Apply**.

Dell Access Explorer

- [Access Explorer Overview](#)
- [Access Explorer Components](#)

Access Explorer Overview

The management of files, folders, and shares is a complex and time-consuming process. There are numerous manual steps and disconnected management applications that must be leveraged before a resource can be safely deployed and made accessible to the appropriate users. Once deployed, there are concerns that granted access is neither increased nor removed inadvertently.

To ensure network resources are secured in a manner that meets your business needs, you must be able to easily identify who has been given access to those resources and manage that access appropriately. Using the Explore tab in Report Manager, you can quickly see who has access to specific resources (files, folders, and shares) and the explicit permissions associated with those resources. At any point in the exploration of an account, you can run reports on the available information.

Access Explorer takes the following approach to meet the challenge:

- **Unify resource management**
Access Explorer allows you to view and report on overall resource access — both directly applied access and access obtained through group membership. Without this information, visibility is limited and could result in security breaches through inadvertent access.
- **Evaluate resource access**
Access Explorer provides a real-time view of network resource access, providing an immediate and ongoing ability to modify access to resources. This helps enforce your corporate network access policy.

Access Explorer Components

This section defines all of the components that comprise an Access Explorer deployment.

- [Managed Domain](#)
- [Registered Forest](#)
- [Managed Computer](#)
- [Access Explorer Agent](#)
- [Scopes](#)
- [Database](#)
- [Service Accounts](#)

Managed Domain

To ensure that the Access Explorer service can install agents successfully, the Enterprise Reporter Server needs domain user credentials with sufficient access. Access Explorer uses the concept of a managed domain, which is an association of service accounts (user credentials) to Active Directory® domains. When a new service account is added in the configuration, it is automatically granted the required Log On as a Service local user right on the Dell Enterprise Reporter Server. This managed domain service account is used to install the agents. Local agents run as Local System and remote agents run as the service account specified during their installation.

NOTE: Only domains that have a trust relationship with the Access Explorer service domain can be managed.

Once a domain is managed, the application creates a Service Connection Point (SCP) in the domain that provides server location information so that all agents and clients know where to connect.

For more information, see the following:

- [Adding Managed Domains](#) on page 75

Registered Forest

To register a forest, add the forest to Access Explorer, follow the instructions [Adding Forests](#) on page 75. When you add a forest, you must provide a service account with sufficient permissions to perform all Access Explorer configuration tasks. If the application needs to resolve a SID or expand group membership from that forest, it will use the associated service account.

When you add a managed domain and the associated Active Directory® forest is not yet registered, the Enterprise Reporter Server will automatically add the forest and use the domain service account credentials as the forest credentials.

For more information, see the following:

- [Adding Forests](#) on page 75
- [Adding Service Accounts](#) on page 76

Managed Computer

A managed computer is any network object that can host resources such as files, folders, and shares. Currently supported resources include Windows® computers, Windows® clusters, and certain network attached storage (NAS) devices. When the user adds a managed computer, Configuration Manager deploys an Access Explorer agent to scan that computer. The agent may be installed on the computer (local agent) or it may be installed on another computer (remote agent). Detailed access information is maintained on the agent computer, only sending general access information to the server.

NOTE: When adding a remote agent, ensure a trust exists between the agent computer and the resource domains.

For more information, see the following:

- [Setting up a Managed Computer](#) on page 78
- [Managing Managed Computers](#) on page 81
- [Modifying Managed Computer Properties](#) on page 83

Access Explorer Agent

When a managed computer is added, an agent is assigned to that computer. The agent may reside on the computer or it may be a remote agent that resides elsewhere. The primary focus of the agent is to index all the

explicit permissions throughout its assigned scopes. The agent installs a service that allows it to perform all of the necessary functions and to report data to Enterprise Reporter.

The indexing of only explicit permissions is done for the following reasons:

- Indexing every permission would overwhelm the indexing system.
- Indexing every permission would overwhelm the user with information that could not be reported easily.

A managed computer may be scanned by either a local agent or one or more remote agents. Only one local agent can be installed on a managed computer and a managed computer with a local agent cannot be scanned by remote agents.

A local agent does an immediate scan as soon as it is added. Remote agents only scan according to a schedule, but if you want the agent to scan as soon as it is added you can enable the Immediately scan on agent restart or scope change option. This option is cleared by default.

For more information, see the following:

- [Managing Agents](#) on page 84
- [Adding an Agent to a Remotely Managed Computer](#) on page 85
- [Restarting an Agent](#) on page 85

Scopes

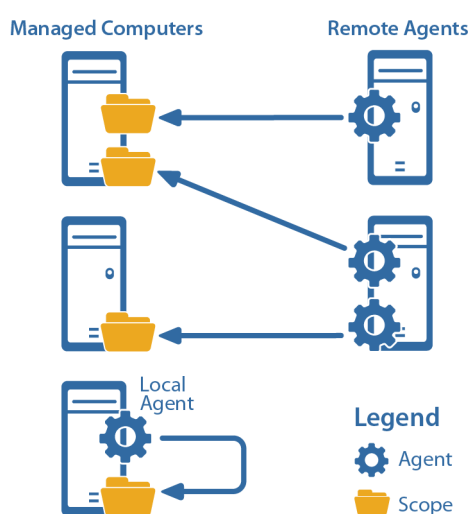
Scopes define the file system targets of the scan on the managed computer. The scopes available for scanning differ for local and remote agents.

- Local agents scan all local fixed volumes on their host computer. Limiting a local agent to a subset of these volumes is accomplished through the Scopes tab of Agent Properties.
- Remote agents may scan all shares available to agents as well as any user-created shares. The scopes scanned by a remote agent are chosen during the configuration of a new remote agent service. The scanned roots may also be changed through the Scopes tab of the Agent Properties.

More than one remote agent may be configured to scan a managed computer provided each agent scans different scopes. A given scope can be scanned by only one agent.

Figure 6 depicts the possible deployment scenarios for Access Explorer agents and managed computers in remote and local installations.

Figure 6. Possible Access Explorer Deployment Scenarios



For more information, see the following:

- [Installing the Access Explorer Agent Remotely](#) on page 79
- [Modifying the Scope of a Scan](#) on page 83

Database

The Enterprise Reporter server stores all data gathered in a SQL Server® database, including indexed data received from the agents.

For more information, see the following:

- [Setting Up the Access Explorer Database](#) on page 74

Service Accounts

A service account is a set of credentials provided by the user and is used to perform certain deployment and query operations.

Managed Domains Service Account

When you place a domain under management, you must provide a service account for the domain. The service account ensures computers from that domain can be added as managed computers. Each managed domain can only have one associated service account at any time, but the same service account can be used for multiple managed domains.

When a new service account is added in the configuration, it is automatically granted the required Log On as a Service local user right on the Dell Enterprise Reporter Server.

Managed Computer Service Account

When you deploy a remote agent to a managed computer, the agent requires a set of credentials to read information from the remote target computer. The credentials provided are referred to as the managed computer service account and are used only to read information from the remotely targeted computer.

 **NOTE:** Local agents run as Local System.

Account Usage

Various operations within Access Explorer use different credentials. The following table details when various accounts are being used.

Table 15. Account Usage in Access Explorer

Actions	Managed Domain Service Account	Forest Service Account	Managed Computer Service Account
Agent Deployment and Removal ¹	Yes		
Restart Agent	Yes		
Take Domain Under Management	Yes		
Register a Forest and Enumerate		Yes	
Read information from targets			Yes ¹

1: The managed domain service account is used to install, upgrade, or remove the agent on the target computer. In the case where the agent is deployed locally, the agent will run as Local System. In the case where an agent is deployed remotely, the managed computer service account is used to read information from the remote computer.

Security of the Service Accounts

Service account credentials are maintained in the database in a secure encrypted form. In the event that someone gains access to the database, they would not be able to decrypt any of the credentials provided without the encryption key.

Access Explorer uses the Advanced Encryption Standard with a 256-bit key to protect secure data.

For more information see the following:

- [Adding Service Accounts](#) on page 76
- [Editing Service Accounts](#) on page 77
- [Changing the Service Account](#) on page 84

Configuring Access Explorer

- [Setting Up Access Explorer](#)
- [Updating Access Explorer Configuration](#)
- [Collecting Access Explorer Data](#)

Setting Up Access Explorer

The initial configuration of Access Explorer involves a one-time setup of the Access Explorer Database and the first managed domain. For more information, see [Setting Up the Access Explorer Database](#) on page 74 and [Setting Up the First Managed Domain \(includes the Service Account\)](#) on page 74.

Setting Up the Access Explorer Database

The Access Explorer service scans and indexes security access information on files, folders, and shares on managed computers in managed domains. The data is stored in the Access Explorer database.

To set up the Access Explorer database

- 1 Navigate to **Access Explorer Management | Configuration | set up database**.
- 2 Click **set up now**.
- 3 Enter the target SQL Server® instance.
- 4 Enter a name for your database.

The default database name is dbReporter_AccessExplorer.

- 5 Enter database access credentials.

NOTE: These credentials must have the right to create databases on the target SQL Server® instance. They are subsequently used to access the database to store permission information collected from managed computers.

- 6 Click **OK**.

Once the Access Explorer database setup is complete, the database icon is displayed with a green check mark to show that it is configured.

Setting Up the First Managed Domain (includes the Service Account)

Before you can start managing computers, you must first add a domain in which those computers reside. This domain must be associated with a service account with credentials that can perform operations on those computers.

NOTE: Only domains that have a trust relationship with the Access Explorer service domain can be managed.

To set up the first Managed Domain

- 1 Navigate to **Access Explorer Management | Configuration | set up managed domain**.
- 2 Click **set up now**.
- 3 Enter a managed domain DNS name.
- 4 Enter the service account credentials.

The service account must have administrative access to the specified domain.

- 5 Click **OK**.

Once the Access Explorer managed domain setup is complete, the domain icon is displayed with a green check mark to show that it is configured.

An option to Click for more configuration options is displayed. Selecting this option closes the one-time setup screen permanently and opens **Access Explorer Management | Configuration**.

Updating Access Explorer Configuration

Once the database and the first managed domain and service accounts are added, you can continue to add or edit additional managed domains, forests, and service accounts.

Adding Managed Domains

Once you have set up the Access Explorer database and your first managed domain, you may add more managed domains.

To add managed domains

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Configure managed domains for Access Explorer**.
- 3 Click **Add Domain**.
- 4 Enter the Domain name.
- 5 Enter the Service Account.

- OR -

Click **New** to create a service account. For more information, see [Adding Service Accounts](#) on page 76.

- 6 Click **OK**.

Adding Forests

Once you have set up the Access Explorer database and your first managed domain, you may add forests.

To add forests

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Configure managed domains for Access Explorer**.
- 3 Click **Add Forest**.
- 4 Enter the DNS name.
- 5 Enter the Service Account.

- OR -

Click **New** to create a service account. For more information, see [Adding Service Accounts](#) on page 76.

 **NOTE:** The service account must have sufficient access required to query group membership within the forest.

The service account set on the forest will be used as the default service account on any managed domain within that forest.

- 6 Click **OK**

Editing Managed Domains or Forests

Once you have set up the Access Explorer database and your first managed domain, you can change the service accounts on domains or forests.

To edit domains or forests

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Configure managed domains for Access Explorer**.
- 3 Select the domain or forest to edit.
- 4 Click **Edit**.
- 5 Enter the Service Account.
- OR -
Click **New** to create a service account. For more information, see [Adding Service Accounts](#) on page 76.
- 6 Click **OK**.

Adding Service Accounts

Service accounts are sets of credentials used to manage computers in Access Explorer. The service accounts must be configured to access an existing Active Directory® account with sufficient rights to log onto the server.

Once you have set up the Access Explorer database and your first managed domain, you may add service accounts.

To add service accounts

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Configure service accounts for Access Explorer**.
- 3 Click **Add**.
- 4 Enter the Account Name (domain\username).
- 5 Enter matching passwords.
- 6 Click **OK**.

The first service account you add is set as the default account for accessing any domains that cannot be reached through the current configuration. To change the default service account, For more information, see [Editing Service Accounts](#) on page 77. To delete a service account, see [Deleting Service Accounts](#) on page 77.

 **NOTE:** When a new service account is added, it is automatically granted the required Log On as a Service local user right.

Editing Service Accounts

You can change the password on a service account and reassign the default account. A green check mark displays next to the service account that is used as the default account to access any domains that cannot be reached through the current configuration.

For more information on adding and deleting service accounts, see [Adding Service Accounts](#) on page 76 and [Deleting Service Accounts](#) on page 77.

To edit service accounts

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Configure service accounts for Access Explorer**.
- 3 Select a service account to edit.
- 4 Click **Edit**.
- 5 Enter a new password.
- 6 Select or clear the default service account option.
- 7 Click **OK**.

Deleting Service Accounts

Once you have set up the Access Explorer database and your first managed domain, you may delete service accounts.

To delete service accounts

- 1 Navigate to **Access Explorer Management | Configuration**.
- 2 Click **Add new Service Accounts**.
- 3 Select the service account to delete.
- 4 Click **Delete**.
- 5 Click **OK** to confirm deletion of the service account.
- 6 Click **Refresh** to update the display.

Collecting Access Explorer Data

The Access Explorer agents collect data on only the computers you choose to manage. You can choose which folders the Access Explorer agent scans on the managed computer and you can set the schedule when the scan occurs.

 **CAUTION:** It is very important that the service account you choose to use for the Access Explorer agent is one that has the permissions to install the agent and the service on the selected server. Only a member of the Administrator group on the selected server has the necessary permissions to install the agent and the service.

Setting up a Managed Computer

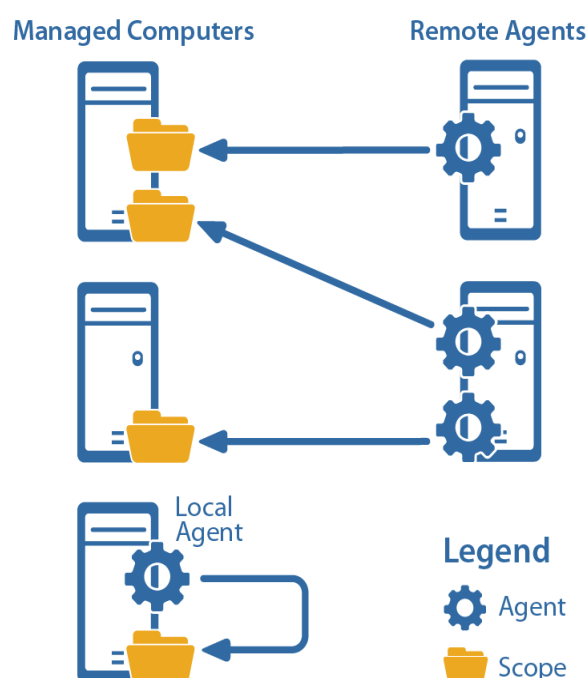
A managed computer is one that is scanned by the Access Explorer agent for security data. When you add a managed computer, you have the option of installing a local agent on the same computer or configuring a

remote agent installed on another computer. If you install a locally managed computer, you can automatically install the agent with the computer, or install the agent manually later.

- ① **NOTE:** Only computers in domains that are managed can be added as managed computers. To add a domain, other than the domain specified during installation, see [Adding Managed Domains](#) on page 75. If you choose to add a remote agent to a managed computer, the first remote agent must be configured during the deployment of the managed computer. You can add more remote agents later, if needed.
- ① **TIP:** More than one remote agent may be used to scan a managed computer. This is useful if the managed computer has a large set of data roots. Multiple agents may not scan the same data root.

Figure 7 depicts the possible deployment scenarios for Access Explorer agents and managed computers in remote and local installations.

Figure 7. Possible Access Explorer Deployment Scenarios



A locally managed computer is one on which the Access Explorer agent is installed and scanning security data on the same server. Local installation is available only for Windows® Servers. With a local installation, you also can choose automatic or manual installation. See [Installing the Access Explorer Agent Locally](#) on page 78.

A remotely managed computer is one that has its security data scanned and collected by Access Explorer agents running on different servers. Other than Windows® Servers, all other server types require remote installation. There is no option to install the agent manually. See [Installing the Access Explorer Agent Remotely](#) on page 79.

Installing the Access Explorer Agent Locally

Currently, the only type of server on which you can install the Access Explorer agent locally is Windows® Server.

To install the Access Explorer agent locally

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer** and choose **Windows Server**.
- 3 Choose **Locally Managed** and click **Next**.

- 4 Choose **Automatic installation by Enterprise Reporter** and click **Next**.

NOTE: If you choose Manual Installation, the managed computer is added to the list but the Access Explorer service is not installed. The status of the computer remains at *Waiting for agent first connection* until the service is installed. To install the Access Explorer service, run the agent installer located in the Enterprise Reporter installation folder (Program Files\Dell\Enterprise Reporter\Access Explorer\Agent Management\Agent).

- 5 Choose the domain that contains the computers you want to manage.

If the domain is not listed, you need to add it as a managed domain. See [Adding Managed Domains](#) on page 75.

If the list of computers is long, you can type in the blank row at the top to sort the list.

NOTE: To quickly add computers to the list, click Import to import a .txt file that contains the fully qualified domain names listed one per line or in a string separated by commas.

- 6 Select the computers you want to manage and click **Add**.

To remove a selected computer from the list, click **Remove**.

- 7 Click **Finish**.

The agent will now be installed on the selected computers.

As the agent is installed, the status changes to reflect the progress of the installation. When the Status column is OK the agent is installed. When the initial scan is complete, the Data State column displays Data Available.

By default, the Access Explorer agent scans the entire root drive of the managed computer. To select specific folders to scan, see [Modifying the Scope of a Scan](#) on page 83.

Installing the Access Explorer Agent Remotely

Install the Access Explorer agent remotely when you cannot install the agent on the computer you want to manage. You can install the agent on more than one remote server, so you can have several different servers collecting security information on the same computer.

NOTE: You can install the Access Explorer agent remotely on only one managed computer at a time. You can, however, install the agent on multiple remote servers to scan a single managed computer. See [Adding an Agent to a Remotely Managed Computer](#) on page 84.

Remote installation of the Access Explorer Agent is available for:

- [Windows® Servers](#) on page 79
- [NAS Servers](#) on page 80
- [Clusters](#) on page 80

Windows® Servers

To install the Access Explorer agent remotely for a Windows® Server

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer** and choose **Windows Server**.
- 3 Choose **Remotely Managed** and click **Next**.
- 4 Choose the domain that contains the computers you want to manage.
- 5 Select the computer to manage and click **Next**.

If the list of computers is long, you can type in the blank row at the top to filter the list.

You cannot select multiple computers to manage. You must install the agent on one computer at a time.

- 6 Select the root folders for the Access Explorer service to scan for data and click **Next**.
Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.
- 7 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 8 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 9 Create a schedule for when the Access Explorer agent scans the managed computer for data.

NOTE: When selecting to "Run On An Interval," it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

For remote agents, you must enable the Immediately scan on agent restart or scope change option if you want the agent to scan immediately when it is added. This option is cleared by default.

- 10 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the Status column is OK the agent is installed. When the initial scan is complete, the Data State column displays Data Available.

NAS Servers

To install the Access Explorer agent remotely for a NAS Server

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer** and choose **NAS Server**.
- 3 Choose the domain that contains the computers you want to manage.
- 4 Select the computer to manage and click **Next**.

If the list of computers is long, you can type in the blank row at the top to filter the list.

You cannot select multiple computers to manage. You must install the agent service on one computer at a time.

- 5 Select the root folders for the Access Explorer agent to scan for data and click **Next**.
Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.
- 6 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 7 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 8 Create a schedule for when the Access Explorer agent scans the managed computer for data.

NOTE: When selecting to "Run On An Interval," it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

For remote agents, you must enable the Immediately scan on agent restart or scope change option if you want the agent service to scan immediately when it is added. This option is cleared by default.

- 9 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the Status column is OK the agent is installed. When the initial scan is complete, the Data State column displays Data Available.

Clusters

To install the Access Explorer agent remotely for a cluster

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Click **New Managed Computer** and select **Cluster**.
- 3 Select the domain containing the cluster from the list.

Once the domain has been selected, the wizard numerates the clusters available in the domain.

NOTE: If the selected cluster name is not correct, click **Edit Cluster Name** to assign the correct name for the rest of the process.

- 4 Select the cluster to be added to the managed domain and click **Next**.

The managed cluster has been added to the domain.

- 5 Select the root folders for the Access Explorer agent to scan for data and click **Next**.

Only the root folder is marked as selected, but all folders and files beneath the root are included in the selection.

- 6 Click **Browse** to select a server (Agent Computer) on which to install the Access Explorer agent.
- 7 Select a service account that has the necessary permissions to install the Access Explorer agent on the designated Agent Computer.
- 8 Create a schedule for when the Access Explorer agent scans the managed computer for data.

NOTE: When selecting to "Run On An Interval," it is possible to choose a frequency such that the agent is still busy completing the last scan when the next scan should start. In this case, the scan that could not start on time will be skipped and the next scan will be started as normal.

For remote agents, you must enable the Immediately scan on agent restart or scope change option if you want the agent service to scan immediately when it is added. This option is cleared by default.

- 9 Click **Finish**.

As the agent is installed, the status changes to reflect the progress of the installation. When the Status column is OK the agent is installed. When the initial scan is complete, the Data State column displays Data Available. For information on adding an agent to the cluster, see [Adding an Agent to a Remotely Managed Computer](#) on page 84.

Managing Managed Computers

You can monitor your list of managed computers easily on the Managed Computers page.

The Managed Computer page is organized by domain name. Next to the domain name, you can quickly see how many of the managed computers are healthy or unhealthy. An unhealthy computer is indicated by a large red dot next to the Name column. Check the Status column for an indicator of the issue causing the unhealthy status.

Table 16. Descriptions of the Columns on the Managed Computer Page

Column	Description
Name	The name of the computer being managed, which is the computer that the agent is scanning and reporting data to the Access Explorer database.
Domain	The name of the domain in which the managed computer resides.
Management Method	The type of management used on the managed computer, either Locally Managed or Remotely Managed. - Locally Managed indicates the managed computer and the agent computer are the same. - Remotely managed indicates the managed computer and agent computer are different.

Table 16. Descriptions of the Columns on the Managed Computer Page

Column	Description
Agent Computer	The name of the server on which the Access Explorer agent is installed.
Status	The status of the agent. The status updates automatically, but you also can click Refresh to update the Status column. If the status is OK, the agent is running successfully.
Data State	The status of the data obtained by the agent. The status updates automatically, but you also can click Refresh to update the Data State column. If the data state displays data available, the last scan performed was successful and data is in the Access Explorer database.
Keyword	An optional word that you can add to the Managed Computer properties to help you filter the list. See Modifying Managed Computer Properties on page 82.

Sorting and Filtering Columns

Use the sort and filter capabilities to help you locate managed computers in the list.

To sort a column

- Click  to sort in descending alphabetical order (Z to A).
- Click  to sort in ascending alphabetical order (A to Z).

To filter a column

- Click  in a column heading to display a list of every entry in that column and select a value on which to filter.
 - (Blanks) displays rows with a blank entry in that column.
 - (Non-blanks) displays rows with an entry.
 - (Custom) opens a Custom AutoFilter where you can create a custom filter.

- OR -

If an empty row is displayed under the column headers, enter text in each column of this row to perform an exact-match search to narrow the results.

To clear a filter

- With a filter selected for a particular column, click  in that column heading and choose (All).

Modifying Managed Computer Properties

The properties that you can change depend on the type of installation you selected for the Access Explorer agent.

- For a locally managed computer, you can add a keyword and modify the scope of the scan.
- For a remotely managed computer, you can add a keyword, modify the scope of the scan, change the service account, and change the scanning schedule.

Adding a Keyword

You can assign a keyword to a managed computer to help you sort and filter the list of managed computers.

To add a keyword to a managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 3 On the Details page, type a keyword to identify the managed computer.
- 4 Click **OK**.

The keyword displays in the Keyword column. You can sort and filter the Keyword column to help you quickly find a managed computer.

Changing the Scan Schedule

You can change only the schedule of a remotely managed computer.

To change the scan schedule of a remotely managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a remotely managed computer and click **Edit**.
- OR -
Right-click a remotely managed computer and select **Edit**.
- 3 Open the Agent page and change the schedule.
- 4 Click **OK**.

Modifying the Scope of a Scan

By default, the Access Explorer agent scans all folders on a locally managed computer. Once the agent service is installed and running, you can modify the scope to specify specific folders and shares for the agent to scan.

During setup of a remotely managed computer, you set the scope for the Access Explorer agent, but you can modify it at any time.

To modify the scope of the Access Explorer agent scan

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 3 Open the Scopes page.
- 4 If you are modifying a locally-managed computer, clear the All Folders check box and then select the folders or shares to scan.
- OR -
If you are modifying a remotely-managed computer, select the folders or shares to scan.
- 5 Click **OK**.

Managing Agents

The Access Explorer agent scans selected folders, files, and shares on managed computers.

Viewing Agent Details

The Details page of the managed computer properties lists information about the agent that might be helpful in troubleshooting. You can see the date and time of the last scan performed, the port used by the agent service, and the version of the agent service.

To view agent details

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 3 Open the Details page, if necessary.

Changing the Service Account

You can change the service account only on a remotely managed computer. If you need to change the service account on a locally managed computer, you must remove the installed agent first and then reinstall the agent with a new service account.

To change the service account on a remotely managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a remotely managed computer and click **Edit**.
- OR -
Right-click a remotely managed computer and select **Edit**.
- 3 Open the Agent page, and select a Service Account.
If the service account you want is not listed, you need to add it. See [Adding Service Accounts](#) on page 76.
- 4 Click **OK**.
The agent automatically updates. You also can click **Refresh** to update the Status column.

Adding an Agent to a Locally Managed Computer

When setting up locally managed computers, you can choose to install the Access Explorer agent automatically. If you choose to install the agent manually, the locally managed computer is added to the list but the Access Explorer agent is not installed. The status of the computer remains at *Waiting for agent first connection* until the agent is installed.

To install the agent manually on a locally managed computer

- Run the agent installer located in the Enterprise Reporter installation folder (Program Files\Dell\Enterprise Reporter\Access Explorer\Agent Management\Agent).

Adding an Agent to a Remotely Managed Computer

You can have multiple computers running the Access Explorer agent to scan a managed computer.

To add an agent to a remotely managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a remotely managed computer and click **Add Agent**.
- OR -
Right-click a remotely managed computer and select **Add Agent**.
- 3 On the **Scopes** page, select which folders or shares you want the agent to scan.
Folders, files, or shares assigned to other agents are unavailable for selection. If you need to reassign which folders or shares to scan, see [Modifying the Scope of a Scan](#) on page 83.
- 4 Click **Next**.
- 5 On the **Agent** page, assign an Agent Computer and Service Account.
- 6 Set the schedule.
- 7 Click **Finish**.

Removing a Managed Computer

Removing the Access Explorer agent does not affect the contents of the Access Explorer database. Once the agent is removed, no new data is entered into the database, but the existing data remains.

To remove a managed computer

- 1 Navigate to **Access Explorer Management | Manage Computers**.
If a managed computer has multiple agents, the managed computer will be listed once for each agent.
- 2 To remove only one agent, select that agent and click **Remove**.
- OR -
If the entire managed computer needs to be removed, select all of its rows and click **Remove**.
- 3 Click **Yes**.
- 4 Click **OK**.
The Status column reflects the Deconfiguration and Uninstall of the Access Explorer agent. The status updates automatically, but you also can click **Refresh** to update the Status column.

Restarting an Agent

Restarting the agent causes a full rescan of the selected managed computer. A full scan occurs with a restart if you have enabled this option on the Agent page in the managed computer's Properties. For more information, see [Changing the Scan Schedule](#) on page 83.

 **NOTE:** To determine whether data in the client is the most current from the agent, ensure that the data state of the managed computer being examined is marked as "Data Available."

To restart an agent

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select the managed computer and click **Restart**.
- 3 Click **Yes**.
- 4 Click **OK**.
A red dot appears next to the managed computer and the status becomes Agent unregistered while the agent is restarted. The status updates automatically, but you also can click **Refresh** to update the status. When the restart is complete, the status is OK.

Understanding the Status of your Agent

When an agent is installed and scanning data, the Status column indicates *OK* and the Data State column indicates *Data Available*. If there is anything wrong with the agent, the state of the agent becomes unhealthy and the Status column displays text that may help with your troubleshooting.

Agent Status Descriptions

The following table details the possible entries in the Status field:

Table 17. Agent Statuses in Access Explorer

Agent States	Description
Agent Unregistered	Agent has unregistered.
Configuration Failed	An error has occurred while creating the agent on the agent host computer.
Configuration in Progress	Agent is being configured.
Deconfiguration Failed	An error occurred while removing the agent from the agent host computer.
Deconfiguration in Progress	The agent is being removed.
Deleting	The agent is being deleted.
Deleting and Uninstalling	The agent software is being uninstalled.
Expired Lease	The agent has failed to renew its lease. This is often an indication of an error on the agent computer. Ensure that the agent is capable of communicating with the server.
Incompatible Agent Version	An unsupported agent version has attempted to register with the server.
Install Failed	An error occurred while installing the agent.
Install in Progress	The agent installation is in progress.
OK	The agent is in a good state and not experiencing any problems.
Registration Failed	An error occurred while the agent was attempting to register with the server.
Resolved	The agent computer has been resolved. This is a temporary state.
Uninstall in Progress	The agent is being uninstalled.
Uninstalled	The uninstall has finished. This is a temporary state.
Unresolvable	The agent computer has not yet been resolved.
Upgrading Agents	The agents for this host are being upgraded to a newer software version.
Waiting for Agent First Connection	The management server is waiting for the agent to register with the server for the first time.

Data State Descriptions

The following table details the possible entries in the Data State column:

Table 18. Data State Descriptions in Access Explorer

Data State	Description
A scanner error has occurred	A scanner error has occurred with one or more of the agent scanners for this managed computer.
Data Available	Agents deployed to this managed computer have completed their initial scans and returned their data.
Performing an initial scan	Agents deployed to this managed computer report that the scanners have begun their initial scans.
Waiting for scanner status	Agents have been deployed for this managed computer but they have not yet reported their scanner status to the server.
Waiting for scanners to start	Agents for this managed computer have reported back to the server but not all of the scanners have started up.

Troubleshooting Issues with Enterprise Reporter

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

Problems Opening the Consoles

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

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

For more information, see Role Based Security in Enterprise Reporter in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

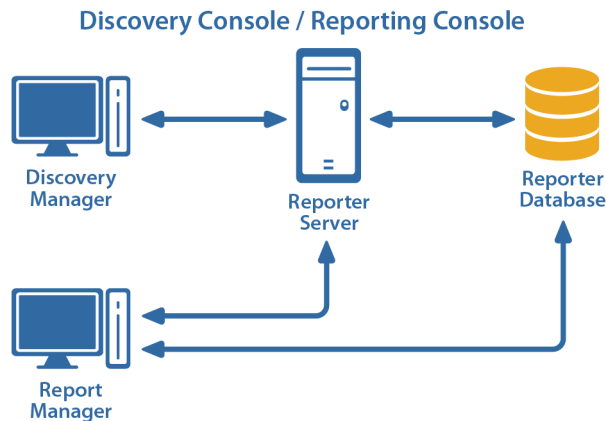
If you are unable to log into the Configuration Manager, verify the type of groups you have selected during installation and how you are adding accounts to those groups to give them access to Enterprise Reporter.

For more information, see Configuring the Database and Security Groups in the [Dell Enterprise Reporter Installation and Deployment Guide](#).

Troubleshooting Connectivity Issues

Each console maintains connections to the Enterprise Reporter server and to the SQL database that stores Enterprise Reporter data. A loss of either connection causes problems. [Figure 8](#) outlines the connections between the components and the server and databases.

Figure 8. Connections between components and the server and databases.



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:

- The computer hosting the server is turned on and running properly.
- The Enterprise Reporter server service is running. If necessary, restart it using the Services console.
- You can reach the host computer over your network.
- 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 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 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.

There are two types of database timeout settings in the Configuration Manager:

- **Enterprise Reporter Server timeout**
You can increase the timeout between the Enterprise Reporter server and the database. If a timeout occurs, you will see a warning dialog box, indicating that this has occurred.
- **Cluster timeout**
You can increase the timeout between the nodes in the cluster and the database. This is useful when a collection fails due to a timeout, which is indicated by an error on the discovery task. For information on viewing the error, see [Viewing Errors](#) on page 64. For information on changing the cluster timeout, see [Modifying a Cluster](#) on page 26.

To change the database timeout settings for the Enterprise Reporter Server

- 1 Click **System | Configuration**.
- 2 Click **Manage database settings used by Enterprise Reporter Server**.
- 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**.

To change the database timeout settings for a specific cluster

- 1 Click **Manage Discovery Clusters**.
- 2 Select the cluster to update.
- 3 Click the **Cluster Details** tab.
- 4 To change the time allowed to establish a connection, modify the **Connection Timeout**.
- 5 To change the time allowed to process a database command, modify the **Command Timeout**.

Troubleshooting Credential Change Failures

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

If you have to manually change a credential on a node, you should ensure that there are no discoveries running or queued before making the change. Change the credentials using the Services console on the host computer, then restart the service. Verify that the node started in the bottom pane of the Manage Discovery Clusters page. Restart any discoveries you canceled.

Once you have changed credentials:

- If a node fails to start, ensure the credentials have local administrator access on the node host computer, and check that the credentials you provided are valid.

- If a discovery fails, ensure that the new credentials have read access on the targets of any discovery. Check the discovery to see if it is using the default node credentials or if credentials are specified. Ensure that the credentials you provided are valid.

Access Explorer credentials are not stored in the Credential Manager. For more information on Access Explorer service accounts, see [Service Accounts](#) on page 72.

Resolving Issues in the Configuration Manager

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

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

Node Issues

- [Node Deployment Issues](#)
- [Dealing with Unassociated Nodes](#)
- [Dealing with Faulted Nodes](#)
- [Problems Deleting a Node](#)
- [Changing the Node Logging Level](#)
- [Changing the Size of the Node Log Files](#)

Node Deployment Issues

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

 **NOTE:** You must have administrative permissions on the node host computer to install the node.

 **NOTE:** If the node host computer is behind a firewall, you must manually install the node.

Before you begin:

- Note the port being used by the Enterprise Reporter server service.
- For nodes requiring an alternate port, make note of an available port.
The default port is 7737.
- If applicable, remove the node in the Configuration Manager. For more information, see [What does the status of a node or cluster indicate?](#) on page 31.
- If necessary, use the Control Panel to uninstall the node.

To manually install or upgrade a node

- 1 If you are installing the node on a 32-bit operating system, locate the node installer, Enterprise ReporterNode 2.5.0.xxxx x86.msi (where xxxx is a unique 4-digit code), in the Dell\Enterprise Reporter\Server folder in the install location.
- OR -

If you are installing the node on a 64-bit operating system, locate the node installer, Enterprise ReporterNode 2.5.0.xxxx x64.msi (where xxxx is a unique 4-digit code), in the Dell\Enterprise Reporter\Server folder in the install location.

 **NOTE:** If you are installing the node on a remote computer, copy the appropriate Enterprise Reporter Node 2.5.0.xxxx (x86/x64).msi file to that computer.

- 2 Run the node installer.
- 3 On the Welcome screen of the Setup Wizard, click **Next**.
- 4 Accept the license agreement and click **Next**.
- 5 To install Dell Enterprise Reporter Node in the default folder, click **Next**.
- OR -
Click **Change** to choose another folder, then click **Next**.
- 6 Specify the credentials and port number that will be used by the Enterprise Reporter Node service, then click **Next**.

This user account must be granted the 'Log on as a service' right and must have permission to access the Reporter server. For more information about the service credentials required by the node, see [Node Credential Details](#) on page 17.
- 7 Enter or browse to the computer that hosts the Enterprise Reporter Server.
Specify the fully qualified distinguished name of the computer.
- 8 Specify the port being used by the Enterprise Reporter Server service, then click **Next**.
- 9 Click **Install**, then click **Finish**.
- 10 When the node is installed, associate it with a cluster. For more information, see [Dealing with Unassociated Nodes](#) on page 92.

Dealing with Unassociated Nodes

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

To uninstall a node

- Use the Control Panel, and uninstall Dell Enterprise Reporter Node 2.5.0.xxxx (where xxxx is a unique 4-digit code)

To associate a node with a cluster

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

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

Dealing with Faulted Nodes

A faulted node has lost contact with the server. You should ensure that the host computer is available on the network and that the service is started.

Problems Deleting a Node

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

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

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

Changing the Node Logging Level

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

IMPORTANT: Use caution when increasing the logging level. We recommend that you do not increase the level permanently, as it may affect node performance. The logging levels are cumulative.

- Fatal contains fatal errors.
- Errors contains errors and fatal.
- Warnings contain warnings, errors, and fatal errors.
- Information contains information, warnings, errors, and fatal errors.
- Debug contains debug, information, warnings, errors and fatal errors.

If you increase the node logging level, you might want to increase the node file size temporarily as well. See [Changing the Size of the Node Log Files](#) on page 93.

To change the node logging level

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 On the Cluster Details tab in the bottom pane, change the node logging level.

NOTE: The cluster must be enabled to change the node logging level.

- 3 Click **Apply**.

Changing the Size of the Node Log Files

Enterprise Reporter writes to log files. By default, the node logging level is set to Warning and the cumulative size of the log files is set to 1000 MB. You can manage the log files within each discovery cluster by setting the node logging level and the cumulative size of the log files. For information on changing the node logging level, see [Changing the Node Logging Level](#) on page 93.

To change the size of the node log files

- 1 In the Manage Discovery Clusters pane, select the cluster.
- 2 On the Cluster Details tab in the bottom pane, change the size of the log files.
The default is 1000 MB and the maximum is 2000 MB. The increments can be set from 100 MB to 2000 MB.
- 3 Click **Apply**.

Scope Enumeration Issues

When you are selecting scopes in a discovery, the credentials in use determine the available scopes. Depending on your discovery, you may be:

- using the default node credentials, in which case your logged in user account determines the available scopes.
- using alternate credentials, in which case these credentials determine the available scopes.

If you are using alternate credentials, and no scopes are available, this may indicate a DNS issue. Ensure the credentials you are using are fully qualified.

Data Collection Issues

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

- The errors generated for a task provide a good starting point for troubleshooting. For more information, see [Viewing Errors and Statistics for Tasks](#) on page 96.
- If your discovery fails for all tasks, it is possible that your shared data location is the problem. The shared data location may no longer exist, or the node may not have adequate access to it. Check the errors on the discovery task to investigate. For more information, see [Viewing Errors](#) on page 64. If this is the issue, ensure the shared data location belonging to the cluster exists and is properly permissioned.
- If your discovery fails for a particular task:
 - The node may not have access to that server. Check your credentials, and change them if necessary. For more information see [Node Credential Details](#) on page 17 and [Modifying Node Credentials](#) on page 27.
 - If you have used alternate credentials for the discovery, ensure that they are permissioned properly. For more information, see [Node Credential Details](#) on page 17.
 - WMI may be disabled, or your credentials are inadequate. WMI is used to query for SQL instances that are not broadcasting
 - The task may have been rejected. If a task is rejected, it means that it is currently being collected by another discovery. Due to the way the Enterprise Reporter collects data, collecting from a SQL Server® in more than one discovery can result in data loss. You could only create one discovery for each SQL scope.
 - A discovery can fail if it runs at the same time attributes are being extended for that discovery type. Run the discovery again once the extension has been processed.
 - If a particular task is timing out, you can increase the amount of time allowed to connect to the database or process a command. For more information, see [Troubleshooting Connection Timeouts](#) on page 89.
 - A task may fail because the target computer cannot be pinged. The ping setting is available for computer, NTFS and registry discoveries. If a target computer cannot be pinged, for example due to network settings or firewall configurations, or if you know that all computers in the discovery are online and available, you can disable the ping. However, if you have added a domain or OU as your scope, and there is a chance that any computer in the container is not available, setting the ping time ensures that no time is spent preparing to collect from these computers. If a computer unexpectedly fails a ping check, try increasing or disabling the ping for the discovery.
 - If your reporting users are experiencing unexpected data fluctuation, check your discovery configuration. If the same target (computer) is in more than one discovery, the data available for reporting reflects the last configuration that was run. Enterprise Reporter's recommended practice is to include a target in only one discovery of a given type. If you have accidentally included a target in more than one place, remove it from all but the desired discovery, and then run that discovery. If for some reason you choose to leave the target in more than one discovery, you can mitigate this issue by using the same settings in both discoveries.
 - The node may be running an unsupported operating system. Check the system requirements, and if necessary, remove the node from the cluster, then rerun the discovery.

- If your Enterprise Reporter database is hosted on a SQL cluster which has experienced a node failure, this can occasionally result in a task that cannot finish processing. In this case, you may need to recreate the discovery.
- Try running the discovery, and monitoring the Activity column in the Processing Tasks view, or looking at the history of the discovery. This may help you identify the specific activity that is causing performance or data collection issues with the discovery. For more information, see [Viewing the Tasks for a Processing Discovery](#) on page 62, and [Viewing the History of a Discovery](#) on page 61.
- If your scheduled discovery does not run, there may be system issues that prevent the job from being created based on the schedule. In this case there is no error reported in the Configuration Manager. To address this issue check that your Enterprise Reporter server service is running, validate your license and check the state of any nodes on the system.

If a discovery disappears, it is likely that another administrator deleted it. You will have to recreate the discovery.

Troubleshooting Features in Enterprise Reporter

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

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

Exporting Logs from the Configuration Manager

Exporting Discovery Management Logs

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

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

To export discovery logs

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

Exporting the Configuration Manager Logs

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

To export Configuration Manager logs

- 1 Click **System | Information**.
- 2 Under Client Logging Information, click **Export Configuration Manager logs**.
- 3 Click **Export**.
- 4 Click the link to locate your zip file.

You can now email your log files to your Dell Support representative.

- 5 Click **Close**.

Viewing Information About Your Enterprise Reporter Configuration

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

To view system information in the Configuration Manager

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

Viewing Errors and Statistics for Tasks

For each task of a discovery, you can view errors and statistics. These may be helpful when you experience failed collections, data that does not match your expectations, or when working on performance issues. For more information, see [Viewing Errors](#) on page 64 and [Viewing Statistics](#) on page 64.

Disaster Recovery

The following backup/restore procedure is the Enterprise Reporter 2.5.0 strategy for disaster recovery. This strategy will help ensure that Enterprise Reporter will be available for use as soon as possible. With regularly scheduled backups of the Enterprise Reporter databases, recovery requires re-installing Enterprise Reporter, restoring the data, restoring a registry key, and restarting Enterprise Reporter.

Back Up of Enterprise Reporter

Two SQL Server® databases are created and used by Enterprise Reporter and should be included with the regular SQL Server® backup. The Discovery Management database has a default name of dbReporter. The Access Explorer database and has a default name of dbReporter_AccessExplorer.

In addition to the databases, Enterprise Reporter has a registry key that needs to be backed up. This key is used by Access Explorer to connect to the database and the Manager Host Agents. If the backup software being used can back up a registry key, point it to the key listed below. If not, on the system where Enterprise Reporter is

installed, run regedit and export the key below. Keep this key in a safe place and include it in the regular file backups.

The registry key to back up is

- HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software\Broadway

Make sure that all data under this key is included in the backup as this data is used to connect to the Access Explorer database and the Managed Host computers.

If regedit is used to export the key, the data will be in a .REG file that can be included in a backup. Once restored, the registry key can be applied by double-clicking on the file.

To back up the registry key using regedit

- 1 Start regedit.
- 2 Locate and select the key to back up.
- 3 Click **File | Export**.
- 4 In the Save In box, select where to save the backup copy, enter a name for the backup, and click **Save**.

How to Deploy Enterprise Reporter to Another Computer After a Disaster

If the original computer is unavailable due to disaster or hardware failure, Enterprise Reporter may need to be deployed on a new computer. The two Enterprise Reporter databases and the backed up registry key will be required.

To deploy Enterprise Reporter on a new computer

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

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

- 2 Recover the Enterprise Reporter databases.

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

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

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

Import the Enterprise Reporter Registry Key

Next, apply the Enterprise Reporter registry key so that Access Explorer can connect to the database, dbReporter_AccessExplorer.

To import the Enterprise Reporter registry key

- 1 Stop the Enterprise Reporter services, the Enterprise Reporter Server, and the Enterprise Reporter Access Explorer if they are running.
- 2 Open regedit.
- 3 Click **File | Import**.
- 4 Browse to the location for the .REG file, select it, and click **Open**.
Import the entire HKEY_LOCAL_MACHINE\SOFTWARE\Quest Software registry key and all subkeys from the backup.
- 5 Start the Enterprise Reporter services, the Enterprise Reporter Server, and the Enterprise Reporter Access Explorer.

Checking the Enterprise Reporter Configuration After a Recovery

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

To check the Enterprise Reporter Configuration after a recovery

- 1 Start the Configuration Manager.
- 2 Select **System | Information**.
Review and confirm all of the settings that Enterprise Reporter is currently using.
- 3 Select **Discovery Management | Manage Discoveries** and then click on the **Discovery Nodes** tab.
All the nodes are displayed.
- 4 Remove any node with a status of Faulted by selecting the node and clicking **Remove Node**.
- 5 Select **Yes** on the popup message.
- 6 Select **Discovery Management** and then click **Manage Discoveries**.
All of the discoveries should be available for use.
- 7 Select **Access Explorer Management** and click **Manage Computers**.
Some of the managed computers may be reporting errors. This is because the Access Explorer service has not heard from the computers. Wait for at least 15 minutes so that the Managed Host Agents have time to load on each computer and contact Access Manager.
- 8 After 15 minutes, if there are still computers not reporting Data Available, then select each computer and click **Restart** to establish the communications channel.
 **NOTE:** If a Shared Data Location is being used with the Clusters, then delete files located in the share as the data in this share will be out of date and will cause errors in the data in reports.

Troubleshooting Access Explorer

- [Agent Events](#)
- [Where are the Logs?](#)
- [Exporting Logs](#)
- [Why is an Agent not Connecting to the Access Explorer Service?](#)
- [Why are Agent Leases Expiring?](#)

Agent Events

During normal operation, Access Explorer agents can encounter issues that cause normal indexing operations to be interrupted. When these events occur, they are written to the Events list. This list is viewable in Agent Properties and can help diagnose problems.

To view agent events

- 1 Navigate to **Access Explorer Management | Manage Computers**.
- 2 Select a managed computer and click **Edit**.
- OR -
Right-click a managed computer and select **Edit**.
- 3 Open the Events page.

Where are the Logs?

Access Explorer Service Logs

The Access Explorer service log files are located in the program directory, which is by default:

`\Program Files\Dell\Enterprise Reporter\Access Explorer`

At any given point, you will see the following files:

- ER Service Log.txt
- ER Group Resolution Log.txt
- ER Lease Manager Log.txt
- ER Machine Local Group Log.txt

There may be two files because the service maintains rolling logs, in an effort to save space on the hosting computer. The first log file is the active log, and is constantly being maintained. When this file reaches its threshold (20 MB), it is renamed with the current year, and a new one is started. This second log file is overwritten each time the server starts a new log. Both files are generally necessary when troubleshooting issues.

You may also export the Access Explorer log files. For more information, see [Exporting Logs](#) on page 100.

Agent Logs

Local agent log files are stored on the agent computer in a subdirectory of the agent installation folder:

```
\Program Files\Dell\Access Manager\Agent Service\BroadwayAgentService
```

Remote agent instance logs are in subdirectories of the agent installation folder, named after the agent ID on the host computers. A specific agent ID for a managed host can be found on the Details tab in Agent Properties.

 **NOTE:** Note that the identity being used by each agent must be capable of creating sub-folders and files beneath the agent's installation directory.

Agent log files are maintained as a binary file with the file extension .bwalog. To view their contents, Dell has provided a command line tool, BWAgentLogReader.exe. To convert an Agent log file into readable text, enter the following from the command prompt:

```
bwagentlogreader /f <path to logfile> /full >> outputfile.txt
```

You may also export the Access Explorer log files. For more information, see [Exporting Logs](#) on page 100.

Exporting Logs

You can choose to export all the Access Explorer logs to two files that you can send to your Dell Support Representative. The two files (AE_Agents.zip and AE_Server.zip) can be found in a subdirectory identified by the generation date in the Exported Logs folder on the Enterprise Reporter server. The path to the two files is presented when you initiate the export. Click the link to access the two files.

To export logs

- 1 Navigate to **Access Explorer Management | Configuration** and click **Export Access Explorer related logs**.
- OR -
Navigate to **Access Explorer Management | Manage Computers** and click **Export Logs**.
- 2 Click **Export**.
- 3 Click the link to the path where the AE_Agents.zip and AE_Server.zip files are located.
- 4 Send the files to your Dell Support Representative.

For more information on the Access Explorer log files, see [Where are the Logs?](#) on page 99.

Why is an Agent not Connecting to the Access Explorer Service?

Probable Cause

- A firewall is active on the agent hosting computer, which is preventing the Agent from connecting to the service.
- The proxy settings on the agent computer are preventing it from connecting to the service.

Resolution

- Configure the firewall on the Agent to allow outgoing traffic on TCP port 8721, as well as incoming traffic on TCP port 18530. Also, ensure that the Access Explorer service firewall has the following exceptions configured: incoming TCP 8721, 8722 and outgoing 18530.
- Configure the proxy settings on the Agent computer to either store credentials for accessing your corporate HTTP proxy, or allow bypassing of the proxy for local addresses.

Why are Agent Leases Expiring?

Probable Cause

- The computer on which the agent is running has rebooted.
- The agent service has been stopped or disabled.
- The agent service has been restarted.

Resolution

- Ensure the agent service is running on the agent computer.

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](#)
- [Extracting help for Access Explorer cmdlets](#)
- [Using cmdlets to manage clusters and nodes](#)
- [Using cmdlets to manage jobs \(discoveries\)](#)
- [Using cmdlets to run reports](#)
- [Using cmdlets to set up Access Explorer](#)
- [Using cmdlets to get information about Access Explorer objects](#)
- [Using cmdlets to manage Access Explorer agents](#)
- [Using cmdlets to remove Access Explorer objects](#)

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 can be installed on Windows® XP, Windows Vista®, and Windows Server® 2003, and is included with Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2.

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 Dell 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 version 2.5. These cmdlets allow you to perform many of the functions of Enterprise Reporter in an automation environment. The cmdlets also can be of great use in any environment where a repetitive process involving Enterprise Reporter is needed.

NOTE: The examples in this section are based on the cmdlets available in Enterprise Reporter version 2.5. While most of these example are valid for the version 2.0 family of Enterprise Reporter, please note that the names of the cmdlets have changed.

Registering Enterprise Reporter cmdlets

If you installed Windows PowerShell® on your computer after you installed Dell 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 Dell.Reporter.Configuration`
`Add-PSSnapin Dell.Reporter.Reporting`
`Add-PSSnapin Dell.Reporter.AccessExplorer`
- 2 Type the following at the command prompt to verify that the snap-in was added:
`Get-PSSnapin`
All registered snap-ins are listed.

Adding the snap-ins automatically to new sessions

If you do not want to add the Dell™ 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 the 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 Dell.Reporter.Configuration
Add-PSSnapin Dell.Reporter.Reporting
Add-PSSnapin Dell.Reporter.AccessExplorer
```

- The location of the Windows PowerShell profile file is as follows:

```
WINDOWS\system32\windowspowershell\v1.0
```

NOTE: If you get 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 Dell™ Enterprise Reporter.

Table 1. Enterprise Reporter cmdlets for use with Windows PowerShell®

Cmdlet	Module
Add-AEManagedComputer	Dell.Reporter.AccessExplorer
Add-AEManagedDomain	Dell.Reporter.AccessExplorer
Add-AEServiceAccount	Dell.Reporter.AccessExplorer
Add-ERADDiscoveryAttribute	Dell.Reporter.Configuration
Add-ERComputerDiscoveryWMIClass	Dell.Reporter.Configuration
Add-ERNode	Dell.Reporter.Configuration
Connect-AEService	Dell.Reporter.AccessExplorer
Connect-ERConfigurationServer	Dell.Reporter.Configuration
Connect-ERReportingServer	Dell.Reporter.Reporting
Disable-ERCluster	Dell.Reporter.Configuration
Disable-ERNode	Dell.Reporter.Configuration
Enable-ERCluster	Dell.Reporter.Configuration
Enable-ERNode	Dell.Reporter.Configuration
Export-AEResourceAccessAsCSV	Dell.Reporter.AccessExplorer
Export-ERReportDefinition	Dell.Reporter.Reporting
Get-AEAccessibleComputersForAccount	Dell.Reporter.AccessExplorer
Get-AEAccountsForComputer	Dell.Reporter.AccessExplorer
Get-AEAgentInstances	Dell.Reporter.AccessExplorer
Get-AEDatabases	Dell.Reporter.AccessExplorer
Get-AEGroupMemberOf	Dell.Reporter.AccessExplorer
Get-AEGroupMembersDG	Dell.Reporter.AccessExplorer
Get-AEGroupMembersMLG	Dell.Reporter.AccessExplorer
Get-AEIndexedAccounts	Dell.Reporter.AccessExplorer
Get-AEIndexedComputers	Dell.Reporter.AccessExplorer
Get-AEManagedComputers	Dell.Reporter.AccessExplorer
Get-AEManagedDomains	Dell.Reporter.AccessExplorer
Get-AERemoteDeploymentMapping	Dell.Reporter.AccessExplorer
Get-AEResourceAccess	Dell.Reporter.AccessExplorer
Get-AEResourceSecurity	Dell.Reporter.AccessExplorer
Get-AEServiceAccounts	Dell.Reporter.AccessExplorer
Get-AEServiceConnectionPoints	Dell.Reporter.AccessExplorer
Get-ERCluster	Dell.Reporter.Configuration
Get-ERDeploymentSddl	Dell.Reporter.Configuration
Get-ERJobDefinition	Dell.Reporter.Configuration
Get-ERJobRun	Dell.Reporter.Configuration
Get-ERLastJobRun	Dell.Reporter.Configuration
Get-ERNode	Dell.Reporter.Configuration
Get-ERReport	Dell.Reporter.Reporting
Get-ERReportSQL	Dell.Reporter.Reporting

Table 1. Enterprise Reporter cmdlets for use with Windows PowerShell®

Cmdlet	Module
Get-ERUnassociatedNode	Dell.Reporter.Configuration
Initialize-Services	Dell.Reporter.Reporting
Invoke-ERReport	Dell.Reporter.Reporting
New-ERCluster	Dell.Reporter.Configuration
New-ERJobDefinition	Dell.Reporter.Configuration
Register-ERLicense	Dell.Reporter.Configuration
Remove-AEManagedComputer	Dell.Reporter.AccessExplorer
Remove-AEManagedDomain	Dell.Reporter.AccessExplorer
Remove-AEServiceAccount	Dell.Reporter.AccessExplorer
Remove-ERCluster	Dell.Reporter.Configuration
Remove-ERJobDefinition	Dell.Reporter.Configuration
Remove-ERNode	Dell.Reporter.Configuration
Restart-AEAgent	Dell.Reporter.AccessExplorer
Restart-AEAgentForComputer	Dell.Reporter.AccessExplorer
Set-AEAccountPassword	Dell.Reporter.AccessExplorer
Set-AEAgentConfiguration	Dell.Reporter.AccessExplorer
Set-AEDatabase	Dell.Reporter.AccessExplorer
Set-AEDBAccessAccount	Dell.Reporter.AccessExplorer
Set-ERConfigurationManagerOptIn	Dell.Reporter.Configuration
Set-ERDeploymentSddl	Dell.Reporter.Configuration
ASet-ERJobDefinitionSchedule	Dell.Reporter.Configuration
Set-ERNodeCluster	Dell.Reporter.Configuration
Set-ERReportManagerOptIn	Dell.Reporter.Reporting
Submit-ERJobDefinition	Dell.Reporter.Configuration

Enabling Enterprise Reporter cmdlets

Before you can use any of the Enterprise Reporter cmdlets, you need to configure the systems 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 Dell™ 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 Dell.Reporter.Configuration`
`add-pssnapin Dell.Reporter.Reporting`
`add-pssnapin Dell.Reporter.AccessExplorer`
`Connect-ERConfigurationServer localhost`
`Connect-ERReportingServer localhost`
`Connect-AEService localhost`
`get-command -Module dell*`
- 6 Save the profile and exit Notepad.
- 7 Exit Windows PowerShell, and then open it.
The snapins load and a list of commands display.

Extracting help for Access Explorer cmdlets

Use the following Windows PowerShell® code to extract help for the Access Explorer module.

```
$x = get-command -Module Dell.Reporter.AccessExplorer
$file = "c:\PowerShell-Help-AccessExplorer.txt"
```

```
foreach ($y in $x)
{
    $y.Name.ToUpperInvariant() >> $file
    "" >> $file
    get-help -Full $y.Name >> $file
    "" >> $file

    "*****" >> $file
    "*****" >> $file
    "" >> $file
}
```

The code first gets all the cmdlets for Access Explorer. Next an output file is created. For each cmdlet, the get-help cmdlet is executed with the -Full parameter set so all of the help info is returned. Finally, the help is

written into the file along with a line used to separate the help for each cmdlet. This process continues until all of the help is read for the cmdlets.

To extract the help for the `Dell.Reporter.AccessExplorer` cmdlets

- 1 On the system where Enterprise Reporter is installed, open a PowerShell window.
- 2 Copy the code from this document, and paste it into Notepad to remove any hidden characters. Make sure you copy everything from the \$ (dollar sign) to the last } (closing bracket).
- 3 Copy and paste the code from Notepad into the Windows PowerShell command line.
- 4 Press **Enter**.
- 5 If you see >>, press **Enter** again.

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 execute. Nodes are associated with this cluster, which can be installed on systems in remote locations to allow jobs to execute 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 execute 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. Iso a computer can 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 the 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 execute 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 executed 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 jobs (discoveries)

An important aspect of Dell™ 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](#)
- [Deleting a job](#)

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" inx="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" inx="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 of 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, MSSQL, Computer, 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. See [Getting job information](#).

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" inx="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="CollectChildACL Differences"><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>'
-ClusterId af0e6da4-10b9-4b20-bf5a-f19f0d71b589 -Schedule '<Trigger
Type="RunDailyTrigger"
StartDateTime="2014-07-17T04:00:00Z" Expression="2014-07-17T04:00:00Z@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](#)

- [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. 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:\
```

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. 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:\
```

Using cmdlets to set up Access Explorer

Before Access Explorer can be used to manage computers or servers, you must at least create a service account, create a database, and add a domain.

This section contains the following topics:

- [Creating the Access Explorer database](#)
- [Adding a service account](#)
- [Adding a domain to manage](#)
- [Adding managed computers](#)
- [Adding managed computers](#)

Creating the Access Explorer database

The Access Explorer database stores all the data that Access Explorer needs to manage computers and servers.

Syntax

```
Set-AEDatabase [-DatabaseServer] <String> [-DatabaseName] <String> [-DatabaseAccount] <String> [-DatabaseAccountPassword] <SecureString> [[-ConnectToExistingDatabase] [<SwitchParameter>]]
```

Example

In this example, the first step encrypts the password used by the service account before sending it across the network. Next, the database used by Access Explorer is created on the SQL Server identified in the DatabaseServer parameter and given the name dbReporter_AccessExplorer, which is the default name provided when creating a database in Access Explorer. The service account used to create the database needs to have permission to create and access the database. If the cmdlet creates the database successfully, Operation Complete is returned.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force
Set-AEDatabase -DatabaseServer AMERGEN01 -DatabaseName dbReporter_AccessExplorer -DatabaseAccount AMER\Administrator -DatabaseAccountPassword $secpasswd
```

Adding a service account

A service account is used to access the database, install agents, and access domains. The service account needs the necessary credentials to create the SQL Server database.

Syntax

```
Add-AEServiceAccount [-AccountDomain] <String> [-AccountName] <String> [-Password] <SecureString> [[-IsDefaultObjectResolution] [<Boolean>]]
```

Example

This example involves a two-step process. The first step encrypts the password used by the service account before sending it across the network. The second step supplies the password, along with the domain and the account for that domain.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force
Add-AEServiceAccount -AccountDomain AMER1 -AccountName Administrator -Password $secpasswd
```

Adding a domain to manage

The next main step to setting up Access Explorer is to add a managed domain. You can manage any domain that your service account can access, including a remote domain. A trust needs to be established between domains and it is useful to have a service account in the trusted domain that you add to Access Explorer.

You need the ID of the service account to add a managed domain. See [Adding a domain to manage](#).

Syntax

```
Add-AEManagedDomain [-DomainName] <String> [-ServiceAccountId]
```

Example 1

In this example, a managed domain is added to Access Explorer. Use the `Get-AEServiceAccounts` cmdlet to obtain the value for the `ServiceAccountId` parameter. Make sure the service account belongs to the domain specified by the `DomainName` parameter.

```
Add-AEManagedDomain -DomainName AMER1 -ServiceAccountId ca94cd34-7c83-46ed-8f7d-34af19b98a1e
```

Example 2

In this example, a new trusted domain is added to Access Explorer. First, a password is created and stored in the `$secpasswd` variable. Next, a service account with the password stored in the `$secpasswd` variable is added for the AMER1 domain. Next, the `Get-AEServiceAccounts` cmdlet is used to return the ID for the service account. Finally, the AMER1 domain is added.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force

Add-AEServiceAccount -AccountDomain AMER1 -AccountName Administrator -Password $secpasswd

Get-AEServiceAccounts
ServiceAccountId      : 0602bedd-b081-45e2-92cf-44ed8cb3b374
AccountSid            : S-1-5-21-102124880-1633684138-1207526451-500
UserDomainName        : AMER1
UserName              : Administrator

Add-AEManagedDomain -DomainName AMER1 -ServiceAccountId 0602bedd-b081-45e2-92cf-44ed8cb3b374
```

Adding managed computers

Once the service accounts, domain, and database are created, you can add managed computers so data can be retrieved. The data can be seen in the Report Manager on the Explorer tab, or you can use a cmdlet to retrieve data for a specific share, folder, or file.

The cmdlet for adding a managed computer has several parameters, but we will show the minimum you need to accomplish the task.

Syntax

```
Add-AEManagedComputer [-ComputerAccountName] <String> [[-Keyword] <String>] [[-DeploymentType] <DeploymentMethodType>] [[-ResourceActivityEnabled] <SwitchParameter>] [[-Granularity] <Int32>] [[-ExcludedTrusteesImportFile] <String>] [[-ExcludedFileTypesImportFile] <String>] [[-ExcludedFoldersImportFile] <String>] [[-AgentHostName] <String>] [[-SelectedDataRoots] <List`1[String]>] [[-ScheduleType] <AgentInfo+DataRootScanSchedule+ScanScheduleType>] [[-ScheduledDays] <List`1[String]>] [[-ScheduledTime] <String>] [[-ScanInterval] <Int32>] [[-ServiceAccountId] <String>] [[-EnableRemoteFileSystemChangeWatching] <SwitchParameter>] [[-PerformImmediateScanOnWatchError] <SwitchParameter>] [[-OverrideScanScheduleOnStartup] <SwitchParameter>] [[-AccountNameSpecifiedIsSID] <SwitchParameter>] [[-AgentHostNameSpecifiedIsSID] <SwitchParameter>]
```

Example

This example deploys an agent to the AMERGENDC server with a deployment type of ManagementServerInstall, which automatically deploys an agent. The other deployment type, External, marks the managed computer as requiring an external agent installation. In most cases you will want to deploy as ManagementServerInstall.

All of the other parameters are not necessary and the default setting for those options (parameters) are correct for a normal install of the agent on the managed computer. In this case with a local install, all of the files (data roots) on the managed computer will be scanned for file access permission, which is the normal setting if done using **Configuration Manager | Access Explorer | Manage Computers**.

```
Add-AEManagedComputer -ComputerAccountName AMERGENDC -DeploymentType  
ManagementServerInstall
```

Using cmdlets to get information about Access Explorer objects

Most of the parameters used by Access Explorer cmdlets are identifications or IDs. To aid you in getting these IDs, there are of Get cmdlets that return the ID in a GUID format that you use in other cmdlets.

This section contains the following topics:

- [Getting service account information](#)
- [Getting managed domain information](#)
- [Getting managed computer information](#)
- [Getting security information for a resource](#)
- [Getting resource access information](#)

Getting service account information

You need the service account ID to add a managed domain. The Get-AEServiceAccount cmdlet returns the information for all of the service accounts that are available.

Syntax

```
Get-AEServiceAccounts
```

Example

```
Get-AEServiceAccounts
```

Output

```
ServiceAccountId      : 9787f160-56e1-4095-88c2-51ae62a60f78  
AccountSid            : S-1-5-21-3504372180-144029308-885861804-500  
UserDomainName        : AMER  
UserName              : Administrator  
UserPrincipalName     : Administrator@AMER.amer.sitraka.com  
Description           :  
IsDefaultObjectResolution : True  
StatusDetailMessage   :  
Status                : OK  
CanManageDomains      : True  
ServiceAccountName    : AMER\Administrator
```

Getting managed domain information

The Get-AEManagedDomains cmdlet returns information for all managed domains, along with the name of the service account used to access the domain.

Syntax

```
Get-AEManagedDomains
```

Example

In this example, information for all managed domains is returned. In addition to the managed domain ID, you also get the ID for the service account, which is used as input for other cmdlets.

```
Get-AEManagedDomains
```

Output

```
ManagedDomainId      : 9d95d834-0b13-4ada-b42d-981261a96560
DomainDnsName          : AMER.amer.sitraka.com
ForestDnsName          : AMER.amer.sitraka.com
Status                 : OK
NetbiosName            : AMER
DomainSid              : S-1-5-21-3504372180-144029308-885861804
ServiceAccountId       : ca94cd34-7c83-46ed-8f7d-34af19b98a1e
AccessGroupSid         : S-1-5-21-3504372180-144029308-885861804-1
ServiceAccountInfo     : AMER\Administrator
DomainControllerName   :
ExtendedRightsCreated  : False
ServiceConnectionPointsCreated : True
```

Getting managed computer information

Now that there is a managed computer you will want to know the status of the agent and the identification for the managed computer.

An important field to note in the output is the Status field as it provides information as to the status of the agent. For example if you see the Status is still reporting DeployingAgent 15 minutes after you deployed the agent, then something is wrong as deployment should only take a few minutes.

Syntax

```
Get-AEManagedComputers [-ManagedComputerName <String>] [-ManagedComputerId <String>]
```

Examples

In this example, because a managed computer is not specified, the cmdlet returns information on all managed computers.

```
Get-AEManagedComputers
```

Output

```
Agents                : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
ManagedHostId        : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid       : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid        :
ManagedDomainId      : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName              : AMERGENDC
SamAccountName        : AMERGENDC
HostDnsName           : AMERGENDC.AMER.amer.sitraka.com
HostDomainName        : amer.amer.sitraka.com
SiteName              :
HostType              : 1
Management            : Local
Features              : 0
Status                : DeployingAgent
```

```

InternalStatus           : Ok
ResourceNodeId           : 3
Keywords                 :
ResourceActivityTrackingSupported : True

```

Example 2

In this example, a managed computer is specified, so the cmdlet returns information on only the AMERGENDC managed computer.

```
Get-AEManagedComputers -ManagedComputerName AMERGENDC
```

Output

```

Agents                  : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
ManagedHostId          : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid         : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid          : S-1-5-21-2573059503-884258253-2950429726
ManagedDomainId        : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName                : AMERGENDC
SamAccountName           : AMERGENDC
HostDnsName              : AMERGENDC.AMER.amer.sitraka.com
HostDomainName           : amer.amer.sitraka.com
SiteName                 :
HostType                 : 1
Management               : Local
Features                 : 0
Status                   : Ok
InternalStatus           : Ok
ResourceNodeId           : 3
Keywords                 :
ResourceActivityTrackingSupported : True

```

Example 3

In this example, information about the managed computer specified by the ManagedComputerId (also known as the ManagedHostId) is returned.

```
Get-AEManagedComputers -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Output

```

Agents                  : {AMER\AMERGENDC S-1-5-21-3504372180-144029308-885861804-1001}
ManagedHostId          : f13a510b-dc5d-43f6-815b-0020f3da275d
ManagedHostSid         : S-1-5-21-3504372180-144029308-885861804-1001
ComputerSamSid          : S-1-5-21-2573059503-884258253-2950429726
ManagedDomainId        : da4e1710-f80b-4fc5-84fb-2582f9519995
HostName                : AMERGENDC
SamAccountName           : AMERGENDC
HostDnsName              : AMERGENDC.AMER.amer.sitraka.com
HostDomainName           : amer.amer.sitraka.com
SiteName                 :
HostType                 : 1
Management               : Local
Features                 : 0
Status                   : Ok
InternalStatus           : Ok
ResourceNodeId           : 3
Keywords                 :
ResourceActivityTrackingSupported : True

```

Getting security information for a resource

All of the components needed for Access Explorer are now in place so now you can start to retrieve security information in the form of the ACL (access control list) about specific resources (shares, folders, and files) on your managed computers. The resource in question is to be in the format \\computer\share\folder\file.ext and wild characters are not permitted. Note that the cmdlet requires not only the computer name, but also the domain in which the computer resides, because the service account for the domain is needed to access the resource.

Syntax

```
Get-AEResourceSecurity [-ResourceUri] <String> [-ResType] <String> [-DomainDNSName] <String>
```

Example

In this example, the cmdlet returns the ACL for the file specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\files\SmallClassDataset\test4.txt -
ResType Files -DomainDNSName AMER.amer.sitraka.com
```

Output

```
0:BAG:DUD:AI(A;ID;FA;;;S-1-5-21-3504372180-144029308-885861804-1106)
(A;ID;FA;;;SY)(A;ID;FA;;;BA)(A;ID;0x1200a9;;;BU)
```

Example 2

In this example, the cmdlet returns the ACL for the folder specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\files\SmallClassDataset -ResType
Folders -DomainDNSName AMER.amer.sitraka.com
```

Output

```
0:BAG:DUD:AI(A;OICI;FA;;;S-1-5-21-3504372180-144029308-885861804-
1106)(A;OICIID;FA;;;SY)(A;OICIID;FA;;;BA)(A;OICIID;0x1200a9;;;BU)
(A;CIID;LC;;;BU)(A;CIID;DC;;;BU)(A;OICIIID;GA;;;CO)
```

Example 3

In this example, the cmdlet returns the ACL for the share specified in the ResourceUri parameter.

```
Get-AEResourceSecurity -ResourceUri \\AMERGENDC\Files -ResType Shares -DomainDNSName
AMER.amer.sitraka.com
```

Output

```
D:(A;;FA;;;WD)
```

Getting resource access information

In addition to the security information ACL for a resource, you also can get information on who currently has access to the resource. Since the information obtained by the Get-AEResourceAccess cmdlet cannot be read from the command line, you must use the Export-AEResourceAccessAsCSV cmdlet to export the information to a CSV file.

Exporting access information to a CSV file

Syntax

```
Export-AEResourceAccessAsCSV [-ResourceAccessResults] <ResourceAccessQueryResults>
[-OutputPath] <String> [[-DisplayInheritedSecurity] [<SwitchParameter>]] [[-
OptimizeForExcel] [<SwitchParameter>]]
```

Example

In this example as this cmdlet works in conjunction with the cmdlet used to get access information the first thing and not shown here, is to get some information on a resource stored into a variable, \$resourceAccess. The variable is then piped into the Export-AEResourceAccessAsCSV, which outputs the CSV file. In this case the variable is used as an input parameter for the cmdlet and CSV file is optimized for Excel.

```
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath
"C:\ResourceAccessInfo.csv"
Export-AEResourceAccessAsCSV -ResourceAccessResults $resourceAccess -OutputPath
"C:\ResourceAccessInfo.csv" -OptimizeForExcel
```

Syntax

Now that you have seen how to get the information out to a file in any location you wish, let's look at how to get the access information for a resource. With the cmdlet used to get the access information you can retrieve file, folder, share, and service identity rights.

```
Get-AEResourceAccess [-ManagedComputerId] <String> [-ResourceType]
<ResourceAccessQueryResourceType> [[-Resources] <String[]>] [-
ExcludeSubObjectDeviations [<SwitchParameter>]]
```

Example 3

In this example, the Get-AEResourceAccess cmdlet gets resource access (folder security) for the folder SmallClassDataset that resides on a locally managed computer with the id f13a510b-dc5d-43f6-815b-0020f3da275d. The results are saved to the \$resourceAccess variable, which is then exported to a file using the Export-AEResourceAccessAsCSV cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-
0020f3da275d -ResourceType Folder -Resources \\AMERGENDC\Files\SmallClassDataset -
ExcludeSubObjectDeviations
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath
"C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (folder security) is obtained for two folders, \\AMERGENDC\C\$\Test1 and \\AMERGENDC\C\$\Test2, that are located on a remotely managed computer with the ID 973c7042-c413-45fb-9f52-057c64d4f800. The results are placed in the \$resourceAccess variable and exported to a CSV file using the Export-AEResourceAccess cmdlet.

```
$resourceAccess = Get-AEResourceAccess 973c7042-c413-45fb-9f52-057c64d4f800 Folder
"\\AMERGENDC\C$\Test1", "\\AMERGENDC\C$\Test2"
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath
"C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (share security) is obtained for the share, Files, that is located on a managed computer with the ID f13a510b-dc5d-43f6-815b-0020f3da275d. The results are placed in the \$resourceAccess variable and exported to a CSV file using the Export-AEResourceAccessAsCSV cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-
0020f3da275d -ResourceType Share -Resources "Files"
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath
"C:\ResourceAccessInfo.csv"
```

Example

In this example, resource access (security identities) is obtained for the services, TermService (Remote Desktop Services) and SessionEnv (Remote Desktop Configuration), that are located on a managed computer with the ID f13a510b-dc5d-43f6-815b-0020f3da275d. The results are placed in the \$resourceAccess variable and exported to a CSV file using the Export-AEResourceAccessAsCSV cmdlet.

```
$resourceAccess = Get-AEResourceAccess -ManagedComputerId f13a510b-dc5d-43f6-815b-
0020f3da275d -ResourceType ServiceIdentity -Resources TermService, SessionEnv
$resourceAccess | Export-AEResourceAccessAsCSV -OutputPath
"C:\ResourceAccessInfo.csv"
```

Output of the Export-AEResourceAccessAsCSV cmdlet

The following is an example of the information in an output CSV file from the Export-AEResourceAccessAsCSV cmdlet.

```
*****
Resource Access Report (CSV Format)
*****
```

```
"C:\Files - dummy files for scanning\SmallClassDataset"
"Uri","C:\Files - dummy files for scanning\SmallClassDataset",
```

```

"DisplayName", "",
"ResourceType", "NTFS\Folder",
DataRoot, "True"
ParentUri, ""

TrusteeName, TrusteeSid, TrusteeType, "Rights", "RightType", "Inheritance", "AppliesTo", "Explicit",
"CREATOR OWNER", "S-1-3-0", "WellKnownGroup", "Full Control", "Allow Access", "Inherited", "Subfolders and Files
Only", "False",
"NT AUTHORITY\SYSTEM", "S-1-5-18", "WellKnownGroup", "Full Control", "Allow Access", "Inherited", "This Folder,
Subfolders, and Files", "False",
"RPTCH\ABARCAK", "S-1-5-21-3504372180-144029308-885861804-1106", "User", "Full Control", "Allow
Access", "Explicit", "This Folder, Subfolders, and Files", "True",
"BUILTIN\Administrators", "S-1-5-32-544", "Alias", "Full Control", "Allow Access", "Inherited", "This Folder,
Subfolders, and Files", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Create Files / Write Data", "Allow Access", "Inherited", "This Folder
and Subfolders", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Create Folders / Append Data", "Allow Access", "Inherited", "This
Folder and Subfolders", "False",
"BUILTIN\Users", "S-1-5-32-545", "Alias", "Read And Execute", "Allow Access", "Inherited", "This Folder,
Subfolders, and Files", "False",

*****End*****

```

Using cmdlets to manage Access Explorer agents

You use Enterprise Reporter to install the Access Explorer agents, but you can manage the installed agents using the Access Explorer cmdlets.

This section contains the following topics:

- [Identifying agents on a managed computer](#)
- [Changing the agent configuration on a managed computer](#)
- [Restarting the agent](#)
- [Updating an agent](#)
- [Changing the service account password](#)
- [Changing the SQL account password](#)

Identifying agents on a managed computer

A managed computer may have more than one agent installed on it. Not only could there be a local agent, there could be an agent for a remote computer, or an agent for a Net-App server or a cluster. The Get-AEAgentInstances cmdlet finds all agent instances registered with Enterprise Reporter Access Explorer. A filter can be specified to retrieve agent instance information for only a single hosting system. Only managed computers with at least one agent instance (either local or remote) are returned. Note that the computers returned by this cmdlet are not the same as managed hosts; they are the computers that physically host the agent service.

Syntax

```
Get-AEAgentInstances [[-HostingSystem] <String>]
```

Example 1

In this example, the cmdlet returns the agents installed on the managed computer identified in the HostingSystem parameter.

```
Get-AEAgentInstances -HostingSystem AMERGENDC.AMER.amer.sitraka.com
```

Output

AgentComputer	AgentComputerDnsName	RecommendedAgentInstanceCap	Agents
-----	-----	-----	-----

Example 2

In this example, the cmdlet returns all managed computers with their installed agents.

Get-AEAgentInstances

Output

AgentComputer	AgentComputerDnsName	RecommendedAgentInstanceCap	Agents
AMER\AMERGENDC	AMERGENDC.AMER.amer.sitraka.com	20	{AMER\AMERGENDC S-1-5-21-35...
AMER\AMERGEN02	AMERGEN02.AMER.amer.sitraka.com	20	{AMER\AMERGEN02 S-1-5-21-3...

Example 3

In this example, we look at how to expand the information returned by the Get-AEAgentInstances cmdlet as it is used in other cmdlets, such as the Restart-AEAgent cmdlet. To use the Restart-AEAgent cmdlet to restart an agent on a computer, you need to specify the Agent ID.

The first line stores information on the agent in the \$a variable. The second line displays the information stored in the \$a.agents property, which is where you find the agent Id, BW_aaab11494ed4f19921a91b92ee0979d, that you need for the Restart-AEAgent cmdlet.

The \$a | Get-Member (in the example output) displays the member types available for the data returned by Get-AEAgentInstances cmdlet.

```
$a = Get-AEAgentInstances -HostingSystem AMERGENDC.AMER.amer.sitraka.com
$a.agents
```

Output

```
Id : BW_aaab11494ed4f19921a91b92ee0979d
ManagedHostId : f13a510b-dc5d-43f6-815b-0020f3da275d
Management : Local
AgentComputer : AMER\AMERGENDC
AgentComputerDnsName : AMERGENDC.AMER.amer.sitraka.com
AgentComputerActiveDirectorySid : S-1-5-21-3504372180-144029308-885861804-1001
AgentComputerManagedDomainId : da4e1710-f80b-4fc5-84fb-2582f9519995
AgentDetails : Quest.Broadway.Common.Interfaces.AgentDetails
UserNotes :
ServiceAccountId : 00000000-0000-0000-0000-000000000000
IsPrimaryAgent : True
ScanSchedule : Quest.Broadway.Common.Interfaces.AgentInfo+DataRootScanSchedule
DataRoots : {Quest.Broadway.Common.Interfaces.AgentInfo+DataRoot}
ConfigurationSettings :
ScannerStates : {NTFS : NamespaceState_DatasetComplete, Service Identities
NamespaceState_DatasetComplete, Windows Computer :
NamespaceState_DatasetComplete}
EnableRemoteFileSystemChangeWatching : False
PerformImmediateScanOnWatchError : True
OverrideScanScheduleOnStartup : False
UsageConfiguration : Quest.Broadway.Common.Interfaces.ResourceUsageConfiguration
QceeServers :
```

\$a | Get-Member

TypeName: Quest.Broadway.Common.Interfaces.AgentHostInfo

Name	MemberType	Definition
Equals	Method	bool Equals(System.Object obj)
GetHashCode	Method	int GetHashCode()
GetType	Method	type GetType()
ToString	Method	string ToString()
AgentComputer	Property	string AgentComputer {get;set;}
AgentComputerDnsName	Property	string AgentComputerDnsName {get;set;}
Agents	Property	System.Collections.Generic.List[Quest.Broadway.Common.Interfaces.AgentInfo] A...
RecommendedAgentInstanceCap	Property	int RecommendedAgentInstanceCap {get;set;}

Changing the agent configuration on a managed computer

At some point you may want to look at specific folders and files on a managed computer. The data roots for the agent can be changed with an Access Explorer cmdlet. Note that the cmdlet overwrites the current data roots selection, so if you are already scanning a folder called Files1, and you want to include a folder called Files2, you cannot just add the new folder with the cmdlet. You need to specify both Files 1 and Files 2 in the cmdlet. Also the ID for the agent is required, which can be found using the Get-AEAgentInstances cmdlet. See [Identifying agents on a managed computer](#).

Syntax

```
Set-AEAgentConfiguration [-AgentId] <String> [-DataRoots <List`1[String]>] [-ManagedComputerId <String>]
```

Example 1

In this example, the agent with the ID BW_aaabd11494ed4f19921a91b92ee0979d is set to another location for the data roots selection. Any previous setting will be removed as this cmdlet does not add a new data root location, but replaces the current one. Because the managed host ID is provided, the cmdlet does not need to search all of the deployed agent to see if any match the one provided.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots  
"\\AMERGENDC\C$\Photos" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Example 2

In this example, three separate folders on the C:\ Drive are selected for the data roots settings. You can add any number of folders as long as they are separated by a comma. Note that the data root locations are enclosed in quotation marks. The first two data root locations do not need the quotation marks, but the third one does as it contains spaces. It is a good habit to enclose all items like this in quotation marks whether they need them or not.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots  
"\\AMERGENDC\C$\Photos", "\\AMERGENDC\C$\BGinfo", "\\AMERGENDC\C$\Documents and  
Settings" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Example 3

In this example, the complete C:\ drive is being set as the data root.

```
Set-AEAgentConfiguration -AgentId BW_aaabd11494ed4f19921a91b92ee0979d -DataRoots  
"\\AMERGENDC\C$" -ManagedComputerId f13a510b-dc5d-43f6-815b-0020f3da275d
```

Restarting the agent

There are two cmdlets that allow you to restart a single agent or restart all the agents on a managed computer.

Restarting a single agent

The restart operations for the specified agent instances are performed asynchronously by the management server. This cmdlet will not wait for the service restart operations to complete before returning.

Syntax

```
Restart-AEAgent [-AgentId] <AgentId>
```

Example

The agent with the ID BW_aaabd11494ed4f19921a91b92ee0979d is restarted. Use the Get-AEAgentInstances cmdlet to obtain the agent Id for the AgentId parameter. This cmdlet does not return any values.

```
Restart-AEAgent BW_aaabd11494ed4f19921a91b92ee0979d
```

Restarting all agents

Restart operations for the agent instances associated with the specified managed computer are performed asynchronously by the management server. This cmdlet will not wait for the service restart operations to complete before returning.

Syntax

```
Restart-AEAgentForComputer [-ManagedComputerId] <Guid>
```

Example

The agent on the managed computer with the ID 33bf3e5b-5edf-4b28-9eee-7fff84de2bca is restarted. Use the Get-AEManagedComputers cmdlet to obtain the value for the ManagedComputerId parameter. This cmdlet does not return any values.

```
Restart-AEAgentForComputer -ManagedComputerId
```

Updating an agent

There are times when an agent update may be require or may be available. An update can be performed with a cmdlet.

Syntax

```
Update-AEAgent [-AgentId] <AgentId>
```

Example

This example updates the agent specified if there is an agent update available. See the Get-AEAgentInstances cmdlet on how to get the agent Id for the AgentId parameter. See

```
UpdateAEAgent -AgentId BW_b0c49eb3f8364a37b56be1a92e0deba4
```

Changing the service account password

You may have a requirement to change the password for account on a regular bases for security purposes. Changing the password for the service account can be done using a cmdlet. In addition you have the option of also re-synchronizing the agents with the new password.

Syntax

```
Set-AEAccountPassword [-AccountName] <String> [-Password] <SecureString> [[-Resynchronize] [<SwitchParameter>]]
```

Example 1

In this example, the first command secures the password to the \$secpasswd variable. The second command applies the new password to the service account.

```
$secpasswd = ConvertTo-SecureString 'template$PWD' -AsPlainText -Force  
Set-AEAccountPassword -AccountName AMER\Administrator $secpasswd
```

Example 2

In this example, the password is resynchronized on the agents associated with the service account.

Set-AEAccountPassword -Resynchronize

Changing the SQL account password

As with changing the password for the service account, you can change both the account and password used by the Enterprise Reporter Access Explorer server to communicate with the SQL Server database.

Syntax

```
Set-AEDBAccessAccount [-DomainName] <String> [-AccountName] <String> [-Password] <SecureString>
```

Example

In this example, a service account is added to the AMER domain with the password stored in the \$secpasswd variable.

```
Set-AEDBAccessAccount -DomainName AMER -AccountName Administrator -Password $secpasswd
```

Using cmdlets to remove Access Explorer objects

There are a number of cmdlets that allow you to remove objects, such as service account, domains and managed computers, from Access Explorer.

This section contains the following topics:

- [Removing a managed computer](#)
- [Removing a managed domain](#)
- [Removing a service account](#)

Removing a managed computer

To remove a managed computer that is no longer required, use the Remove-AEManagedComputer cmdlet. First all agents installed on the computer are removed, and then the computer is removed from Access Explorer. When unregistered, any agent instances associated with the managed computer are removed. If the computer does not have any agent instances, the Enterprise Reporter Access Explorer agent software is removed.

Syntax

```
Remove-AEManagedComputer [-ManagedComputerId] <String>
```

Example

In this example, the computer with the Id 6e1f518f-cc9a-4915-86e5-894f47767556 is removed as a managed computer.

```
Remove-AEManagedComputer -ManagedComputerId 6e1f518f-cc9a-4915-86e5-894f47767556
```

Removing a managed domain

Once domains are no longer required in Access Explorer, they can be removed. Only domains which do not contain any registered managed Computers can be removed. Note that the Forest will not be removed with this cmdlet. Remove the Forest using Configuration Manager | Access Explorer | Configuration | Managed Domains.

Syntax

```
Remove-AEManagedDomain [-ManagedDomainId] <String>
```

Example

In this example, the domain with the Id 422dcede-3314-4d6c-9f8d-27abc65ada72 is removed. The forest is not removed

```
Remove-AEManagedDomain -ManagedDomainId 422dcede-3314-4d6c-9f8d-27abc65ada72
```

Removing a service account

The Remove-AEServiceAccount cmdlet removes the specified service account from the list of registered service accounts. To retrieve the ID of the service account, use the Get-AEManagedDomains or Get-AEServiceAccounts cmdlets. Only service accounts that are no longer referenced by managed domains and registered forests can be removed.

Syntax

```
Remove-AEServiceAccount [-ServiceAccountId] <String>
```

Example

In this example, the service account with the Id f0bafac5-46c3-4c52-a28b-6fdf5eb0a3b1 is removed.

```
Remove-AEServiceAccount -ServiceAccountId f0bafac5-46c3-4c52-a28b-6fdf5eb0a3b1
```

A

- Access Explorer
 - add forest, 75
 - add managed domain, 75
 - add service accounts, 76
 - agent events, 99
 - agent leases, 101
 - agent logs, 100
 - agents, 84
 - database, 72, 74
 - delete service accounts, 77
 - edit managed domain, 76
 - edit service account, 77
 - install local agent, 78
 - install remote agent, 79
 - managed domain, 75
 - modify scan scope, 83
 - service logs, 99
 - set up managed computers, 78
- adding a node, 30
- agent
 - data roots, 71
 - data state, 87
 - lease expired, 101
 - logs, 100
 - not connecting, 100
 - restarting, 85
 - service account, 72
 - viewing details, 84
- agent events, 99
- agent scans
 - modifying scope, 83
- agent service
 - installing locally, 78
 - installing manually, 78
 - installing remotely, 79
- agents, 84
 - adding, 84, 85
 - change scan schedule, 83
 - changing service accounts, 84
 - status, 86

C

- canceling
 - discovery, 66
 - task, 66
- change history, 35
- cluster
 - creating your first, 24
 - deleting, 26
 - described, 23
 - disabled, 27
 - enabling, 26, 27
 - modifying, 26
 - offline, 27
 - sample implementation diagram, 23
 - status, 31
 - when to add another, 25
- collecting DFS, 49
- connecting to a server, 15
- create
 - discovery, 38
- Create Cluster Wizard, 24
- credential manager, 32, 35
- credentials
 - add service account, 76
 - and service accounts, 72
 - changing agent service, 84
 - edit service accounts, 77
 - node, 24

D

- daily schedule
 - discoveries, 56
- data roots, 71
- data state
 - agents, 87
- database
 - Access Explorer, 72, 74
 - deployment, 72
- delete
 - cluster, 26
 - node, 28
- deploying status, 32
- deployment

- database, 72
- deployment failed status, 32
- determining your software version, 96
- DFS

- collecting, 49
- disabled status, 31, 32
- discovery
 - canceling, 66
 - described, 37
 - improving performance, 30
 - modify, 65
 - troubleshooting, 94
 - types, 37
- distributed file shares, 49

E

- enable
 - cluster, 27
- enabled status, 31, 32
- error
 - discovery indicator, 59
 - task, 60
- errors, 96
 - viewing, 64
- events, agent, 99
- export
 - logs, 95
- exporting
 - logs, 100

F

- failed to start status, 32
- failed to stop status, 32
- filters
 - clearing, 64, 82
- finished tasks, 62
- firewall, 100
- forest, 70
- forests, 70
 - adding, 75
 - editing, 76

G

- global settings, 35

H

- history
 - discovery, discovery history, view history, 61

I

- import

- scopes, 53
- initializing status, 32
- installation
 - server, 92
- installing
 - agent service locally, 78
 - agent service remotely, 79

K

- keywords
 - adding, 83

L

- lease expired, 101
- locally managed computer, 78
 - installing, 78
- locally managed computers
 - adding agents, 84
- logs
 - Access Explorer, 99
 - Access Explorer agent, 100
 - agent service, 99
 - Discovery Manager, 95
 - exporting, 95, 100

M

- managed computer
 - adding, 78
 - adding agents, 84, 85
 - local, 78
 - remote, 78
- managed computers, 70
 - add keyword, 83
 - filtering, 82
 - NAS servers, 80
 - sorting, 82
 - status, 81
 - Windows clusters, 81
 - Windows servers, 79
- Managed Domain, 70
 - service account, 72
- managed domain, 70
 - adding, 75
 - editing, 76
 - set up, 75
- manual node deployment, 91
- minimum
 - deployment, 22
- modify
 - cluster, 26
 - discovery, 65

- monthly schedule
 - discoveries, 57

N

- NAS servers

- installing agent, 80

- NetApp filers, 49

- node

- adding, 30
 - creating your first, 23, 24
 - credentials, 24
 - deleting, 28
 - disabling, 28
 - enable, 29
 - manually deploying, 91
 - manually install, 91
 - status, 31
 - stopping, 28, 29
 - troubleshooting, 91
 - unassociated node, 92

P

- performance, 30

- task slot, 30

- port

- current port, 96

- ports, 100

- processing tasks, 62

Q

- queue, 65

- drill down, 60

R

- registered forest, 70

- remotely managed computer, 78

- installing, 79

- remotely managed computers

- adding agents, 85

- removal failed status, 32

- Reporter server

- connecting to, 15

- restarting

- agents, 85

- rights

- account usage, 72

S

- schedules

- changing agent scan, 83

- scheduling

- discoveries, 56

- scope

- Active Directory, 39

- computer, 41

- file storage analysis, 43

- importing, 53

- modifying, 83

- NTFS, 46

- registry, 50

- selecting, 38

- scopes, 71

- security

- of Service Accounts, 73

- Service Account, 72

- account usage, 72

- for managed domains, 72

- for managed hosts, 72

- security, 73

- service account

- deleting, 77

- editing, 77

- service accounts, 72

- adding, 76

- changing, 84

- shared data location

- locating, 23

- SQL Server

- deployment database, 72

- SQL server

- current database, 96

- starting status, 32

- statistics, 64, 96

- status

- agents, 86

- cluster, 31

- node, 31

- stopped status, 32

- stopping a node, 29

- stopping status, 32

- system

- information, 96

- system configuration, 35

T

- task

- canceling, 66

- errors, 60

- viewing finished, 62

- viewing processing, 62

- task slots

- configuring, 31

- performance, 30

- timeout
 - cluster, 26, 90
 - server, 90
- troubleshooting, 99

U

- UAC, 88
- unassociated node, 92
- undeploying status, 32

V

- viewing
 - errors, 64
 - queue, 65
 - statistics, 64

W

- weekly schedule
 - discoveries, 57
- Windows clusters
 - installing agent, 81
- Windows servers
 - installing remote agent, 79
- WMI, 94

Dell listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.software.dell.com.

Contacting Dell

Technical Support:

[Online Support](#)

Product Questions and Sales:

(800) 306-9329

Email:

info@software.dell.com

Technical Support Resources

Technical support is available to customers who have purchased Dell software with a valid maintenance contract and to customers who have trial versions. To access the Support Portal, go to <http://software.dell.com/support/>.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. In addition, the portal provides direct access to product support engineers through an online Service Request system.

The site enables you to:

- Create, update, and manage Service Requests (cases)
- View Knowledge Base articles
- Obtain product notifications
- Download software. For trial software, go to [Trial Downloads](#).
- View how-to videos
- Engage in community discussions
- Chat with a support engineer