



One Identity Data Governance Edition 8.2

Deployment Guide

Copyright 2021 One Identity LLC.

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 One Identity LLC .

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

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

Data Governance Edition Deployment Guide
Updated - 08 November 2021, 07:58
Version - 8.2

Contents

Introduction	7
Data Governance Edition overview	7
Architecture	9
Data Governance Edition Services	11
Data Governance service	11
Data Governance agent	11
One Identity Manager service	12
Deployment overview	13
Available documentation	14
Data Governance Edition system requirements	15
Data Governance server	15
Database server	16
Data Governance agent	21
Resource Activity database server	22
Supported target systems	22
Data Governance Edition minimum permissions	26
Granting SQL Server permissions	28
Granting Active Directory permissions	29
Data Governance Edition required ports	30
Install One Identity Manager Data Governance Edition	32
Deploy Data Governance Edition components	35
Deployment pre-flight check	35
Data Governance service deployment methods	36
Deploying Data Governance service and creating Resource Activity database	37
Deploying multiple Data Governance services	41
Updating One Identity Manager to a Data Governance Edition deployment	45
Post installation configuration	49
Move Service Principal Name in Active Directory	49
Data Governance Edition components	50
One Identity Manager service (job server) - Data Governance connector flag	51

One Identity Manager - Synchronization projects	51
Assign employee to UNIX account	52
Assign employee to cloud account	53
One Identity Manager - Database configuration	53
Configuring Change Auditor to collect resource activity	55
One Identity Manager Application Server	57
One Identity Manager database encryption	58
Authentication using service accounts and managed domains	59
Readying a service account and domains for deployment	60
Adding and editing a service account	60
Adding a managed domain	61
Working with managed hosts and agents	62
Deployment best practices	63
Agent leases	64
Agent deployment pre-flight check	65
Agent deployment methods	65
Adding and configuring managed hosts	67
Adding a local managed host (Windows computer)	68
Adding a Windows cluster / Windows computer as a remote managed host	71
Adding a generic managed host	73
Adding a Distributed File System (DFS) root managed host	77
Adding a SharePoint farm managed host	78
Adding a NetApp CIFS device as a managed host	82
Adding an EMC CIFS device as a managed host	86
Adding an NFS managed host	89
Adding a cloud managed host	93
Managed host configuration settings	96
Managed host settings dialog	100
NIS Host page	103
Credentials page	103
Cloud Provider page	104
Agents page	105
Managed paths page	106
Security Scanning page	107

Resource activity page	110
Editing managed host settings	114
Customizing default host settings	115
Deployment management	117
Verifying managed host system status	117
Determining the state of the data	119
Checking the agent status	120
Viewing agent errors	122
Restarting agents	123
Remove managed hosts (and associated agents)	123
Removing agents	124
Upgrade Data Governance Edition	125
Before you upgrade	126
Upgrading One Identity Manager Data Governance Edition	129
Applying a hotfix to Data Governance Edition 8.x	133
Remove Data Governance Edition	135
Remove managed hosts (and associated agents)	135
Remove service account assignments	136
Delete service accounts	136
Uninstall Data Governance service	136
Uninstall Resource Activity database	137
Troubleshooting	138
Data Governance Edition logs	139
Exporting agent log	143
Getting server logs	143
Job queue shows that database needs to be compiled	144
Receiving unauthorized access violations	144
Cannot save the service account	145
Cannot connect to a managed host	147
DNS error when attempting to add a new managed host	147
Agent not connecting to the Data Governance server	148
Data Governance agents cannot access NAS devices via SMB	148
Agent leases expiring	150
Cannot add managed paths to my EMC server	150

No activity data	151
No activity data available for SharePoint 2010 managed host	152
Resource activity is not displaying in the web portal for a business owner	153
Governed resources are missing from the All my resources view in the web portal	154
Not receiving scheduled reports	154
Groups missing from the Group Memberships tree view	155
Appendix: NetApp managed host deployment	156
Permissions required to access NetApp filer	156
Data Governance agent deployment	156
FPolicy deployment	157
Managed host configuration options	159
Performance considerations	160
Compatibility with Change Auditor for NetApp	160
Appendix: EMC managed host deployment	162
Configuring CEE framework	162
Creating the cepp.conf file (Celerra or VNX devices)	163
Enabling system configuration auditing (Isilon devices)	164
Appendix: SharePoint Farm managed host deployment	166
Permissions required to access SharePoint farms	166
Configure SharePoint to track resource activity	166
Configure auditing on SharePoint farms	167
Install the QAM.SharePoint.Auditing.Monitor farm solution	167
Map SharePoint events to Data Governance events	168
About us	169
Contacting us	169
Technical support resources	169
Index	170

Introduction

The One Identity Manager Data Governance Edition Deployment Guide contains the information required to install and configure One Identity Manager Data Governance Edition and deploy the Data Governance Edition components, including the Data Governance server, Resource Activity database and Data Governance agents. It also explains how to configure the Data Governance Edition components, including adding managed domains and working with managed hosts. It provides deployment requirements and step-by-step instructions to help you set up and configure Data Governance Edition functionality.

This guide is for network administrators, consultants, analysts, and IT professionals responsible for deploying, configuring and maintaining Data Governance Edition in their organization.

This chapter contains the following information to introduce you to Data Governance Edition and the deployment process:

- [Data Governance Edition overview](#)
- [Architecture](#)
- [Data Governance Edition Services](#)
- [Deployment overview](#)
- [Available documentation](#)

Data Governance Edition overview

Control over your organization's data is vital to eliminating issues such as security breaches, loss of sensitive information, or non-compliance with external and internal guidelines. Data Governance Edition provides a systematic approach to managing data access, preserving data integrity, and providing content owners with the tools and workflows to manage their own data resources, removing reliance on IT administrators.

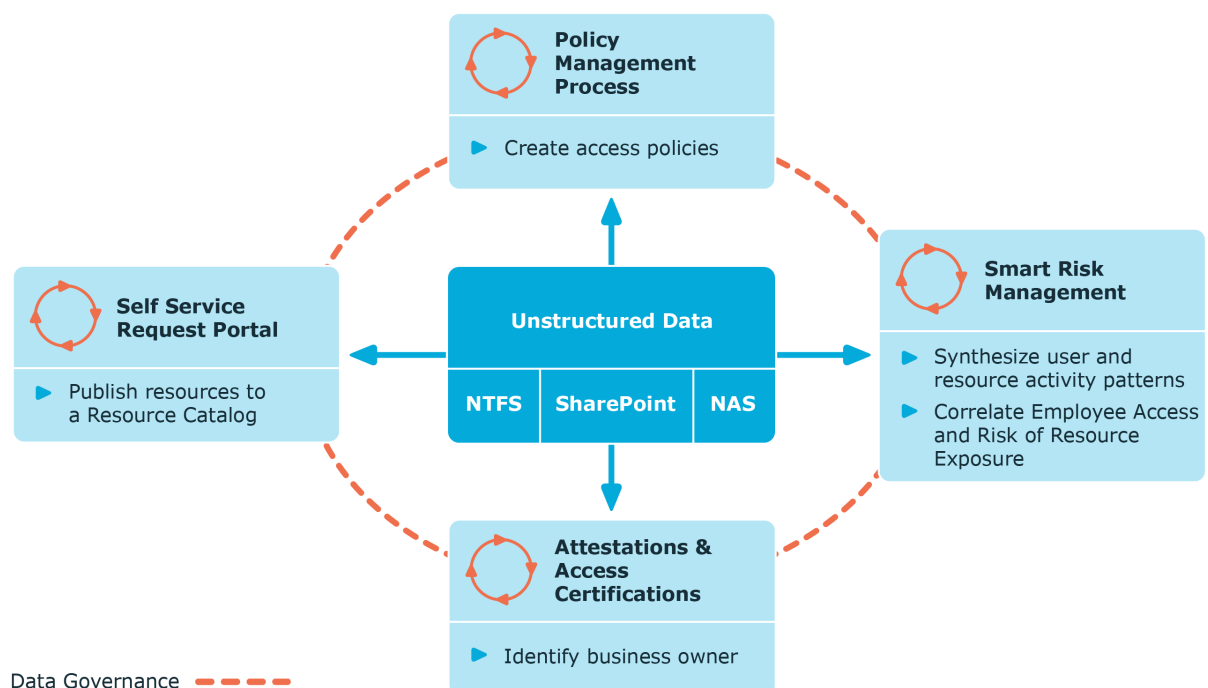
Ultimately, you need a process in place that allows you to:

- Ensure that your business runs efficiently with access to correct information on demand.

- Understand the access levels, patterns, and usage to build and maintain a governance strategy.
- Comply with organizational security and compliance policies.
- Bring accountability to contain damage.
- Review the usage patterns of sensitive information.
- Identify and assign business owners.
- Enable attestations from business owners to the validity of the data and its use.

The governance of unstructured data is accomplished through workflows that cross both the Manager and the web portal. The following diagram identifies the key processes in securing and controlling access to your organization's data.

Figure 1: Data Governance Edition key processes



Architecture

Data Governance Edition consists of the following components:

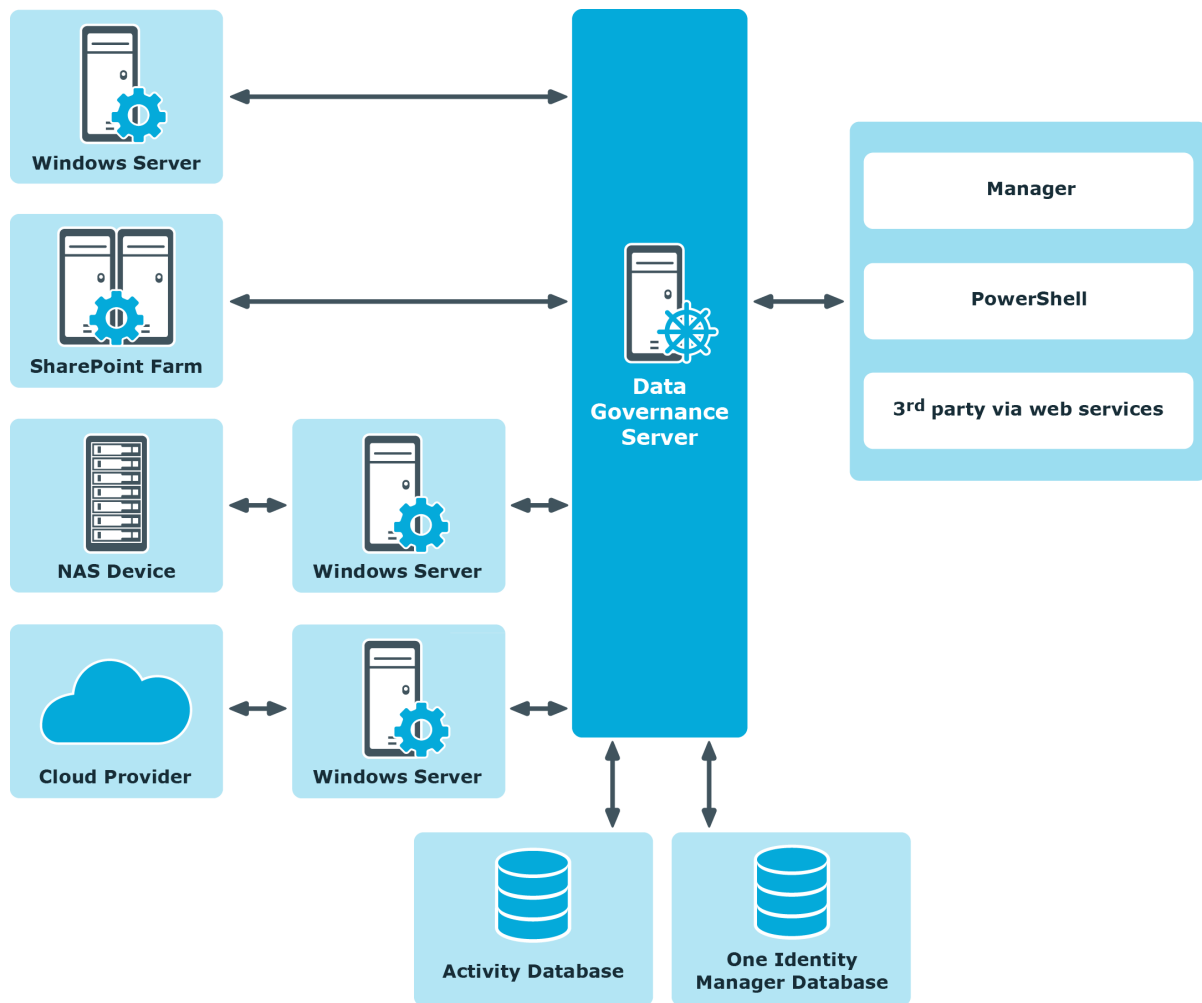
- **Data Governance server:** The server acts as an intermediary between the agents and the databases where information is stored. It coordinates all agent deployments and communication, and manages the security index for each managed host.

The server is the central authority that receives and indexes information from agents deployed on target computers. It only maintains a subset of information for the computers that are being indexed (essentially access to specific resource types on managed computers). When you request detailed access information, the server attempts to contact the local agent and provide information stored in the local agent index.

- **Data Governance agents:** Agents collect security data from your managed hosts, and if configured, can also collect resource activity data. The agent cache stores all the detailed indexed information.
- **Databases:** The One Identity Manager database stores configuration and security information. The Data Governance Resource Activity database stores resource activity information.
- **Managed hosts:** A managed host is any network object that can host resources and can be assigned an agent to monitor security and resource activity. Managed hosts store the data on which users perform actions. Currently supported managed hosts include Windows computers, Windows clusters, certain network attached storage (NAS) devices, SharePoint farms and certain cloud providers, including SharePoint Online and OneDrive for Business.

For more information about component communications and how communication is encrypted, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Figure 2: Data Governance Edition architecture



Data Governance Edition Services

Data Governance Edition is comprised of the following services:

- [Data Governance service](#)
- [Data Governance agent](#)
- [One Identity Manager service](#)

Data Governance service

Table 1: Data Governance service

Service Name	DataGovernanceService
Display Name	One Identity Manager Data Governance Edition Service
Description	The central authority that receives and indexes information from agent services. Acts as the intermediary between the agents and the databases where information is stored.
Default Path	%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\DataGovernanceEdition.Service.exe
Startup Type	Automatic
Exe Name	DataGovernanceEdition.Service.exe

Data Governance agent

Table 2: Data Governance agent service

Service Name	The service name varies depending on the host type: <ul style="list-style-type: none">• Local: DGE_<DeploymentName>_LocalHost• SharePoint farm: DGE_<DeploymentName>_Sharepoint_<nn> Where <nn> is the number appended to the service name when multiple agent services are being used to manage a SharePoint farm.• Remote: DGE_<DeploymentName>_<FQDN of managed host> Where the periods in the FQDN are replaced with underscores.• NFS: DGE_<DeploymentName>_NFS_<ManagedHostName>• SharePoint Online: DGE_<DeploymentName>_SharePointOn-
---------------------	---

	line_<Office 365 Domain> • OneDrive for Business: DGE_<DeploymentName>_ OneDriveBusiness_<Office 365 Host>
Display Name	The display name varies depending on the host type: <ul style="list-style-type: none"> Local: One Identity Manager Data Governance Edition - Local Agent SharePoint farm: One Identity Manager Data Governance Edition - SharePoint Agent - <nn> Where <nn> is the number appended to the display name when multiple agent services are being used to manage a SharePoint farm. Remote: One Identity Manager Data Governance Edition - Agent for <HostName/DNSName> NFS: One Identity Manager Data Governance Edition - Agent for NFS_<ManagedHostName> SharePoint Online: One Identity Manager Data Governance Edition - SharePointOnline (<Office 365 Domain>) OneDrive for Business: One Identity Manager Data Governance Edition - OneDriveBusiness (<Office 365 Domain>)
Description	Provides capabilities for indexing and managing resources for Data Governance Edition.
Default Path	%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services\DataGovernance.Agent.exe
Startup Type	Automatic (Delayed Start)
Exe Name	DataGovernance.Agent.exe

One Identity Manager service

NOTE: The One Identity Manager service refers to a One Identity Manager network server that is declared as a "job server" in the One Identity Manager database to handle the processing of tasks.

Table 3: One Identity Manager service (job server)

Service Name	OneIMService
Display Name	One Identity Manager Service
Description	The job server is used to process some of the Data Governance Edition report requests from the web portal.

Default Path	%ProgramFiles%\One Identity\One Identity Manager-\viNetworkService.exe
Startup Type	Automatic
Exe Name	viNetworkService.exe

Deployment overview

The following activities must be performed to have a fully functional Data Governance Edition deployment:

- Install One Identity Manager Data Governance Edition
- Create and configure the One Identity Manager database
- Install and configure the One Identity Manager service (job server)
- Run the Data Governance Configuration wizard to:
 - Deploy the Data Governance server
 - Create the Data Governance Resource Activity database
- Configure the Data Governance service accounts for managed domains
- Add managed hosts and deploy agents
- Install the web portal

NOTE: New in 7.0: Active Directory synchronization via the One Identity Manager service (job server) is not required for managed host deployment.

In the absence of One Identity Manager target system synchronization, the Data Governance service automatically harvests the forest topology. It creates Employee records for all members found in each domain's Domain Admins group and for the current account running the Data Governance configuration wizard. It also links these accounts to the correct Data Governance application roles, which allows you to add managed hosts and deploy agents.

When additional One Identity Manager functionality is required, including generating complete Data Governance Edition reports, perform the following steps:

- Run the One Identity Manager Synchronization Editor to synchronize your target environments (Active Directory, and if applicable, SharePoint and Unix).

IMPORTANT: Active Directory synchronization MUST be complete before starting the SharePoint synchronization.
- Assign Data Governance application roles to Employees.

Available documentation

Data Governance Edition documentation includes the following manuals:

- *One Identity Manager Data Governance Edition User Guide*
This guide includes Data Governance Edition administration information.
- *One Identity Manager Data Governance Edition Deployment Guide*
This guide includes Data Governance Edition installation, configuration, and deployment information.
- *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide*
This guide includes details about the self-service resource requests related to resources that are governed, including the file system share creation request in the IT Shop.
- *One Identity Manager Data Governance Edition Technical Insight Guide*
This guide is intended for advanced audiences who want a deeper understanding of the Data Governance Edition components and how they communicate with each other. It also provides a description of the configuration file settings, registry key settings and PowerShell commands.

Online versions of the Data Governance Edition guides are available on the technical support web portal: <https://support.oneidentity.com/identity-manager-data-governance-edition/technical-documents>

For supporting One Identity Manager information, see the One Identity Manager documentation. Online versions of the One Identity Manager guides are available on the technical support web portal: <https://support.oneidentity.com/identity-manager/technical-documents>

Data Governance Edition system requirements

NOTE: Some of the system requirements for One Identity Manager have changed in version 8.1. Prior to upgrading Data Governance Edition, ensure that the minimum requirements for all of the One Identity Manager components are met. See the *One Identity Manager Installation Guide* for full details on One Identity Manager's system requirements.

Before installing Data Governance Edition, ensure that your system meets the following minimum hardware and software requirements.

- [Data Governance server](#)
- [Database server](#)
- [Data Governance agent](#)
- [Resource Activity database server](#)
- [Supported target systems](#)

In addition, ensure that the minimum permissions and communication port requirements are met to ensure proper authentication and communication with Data Governance Edition components.

- [Data Governance Edition minimum permissions](#)
- [Data Governance Edition required ports](#)

Data Governance server

The Data Governance server refers to the server where the Data Governance service is installed. This server must meet the following minimum system requirements.

Table 4: Minimum system requirements: Data Governance server

Processor	quad core CPU
-----------	---------------

Memory	16GB RAM
Free drive space	100GB
Operating system	64-bit Windows operating systems: <ul style="list-style-type: none"> • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 <p>NOTE: Only a 64-bit server for Data Governance Edition is supported. Ensure that the server installed on a given computer uses the correct architecture to match the installed operating system.</p>
Software	.NET Framework 4.7.2

Database server

The Database server refers to the server hosting the One Identity Manager database. One Identity Manager supports SQL Server database systems.

The following system requirements must be met in order to install the database on a server for use with Data Governance Edition. Depending on the number of One Identity Manager modules and the accounts managed in One Identity Manager, the requirements for working memory, hard disk space, and processors may be significantly greater than the minimum requirements. For more details on the system requirements for One Identity Manager, see the *One Identity Manager Installation Guide* or *One Identity Manager Release Notes*.

Table 5: Minimum system requirements: Database server

Processor	8 physical cores with 2.5 GHz+ frequency (non-production) 16 physical cores with 2.5 GHz+ frequency (production) NOTE: 16 physical cores are recommended on performance grounds.
Memory	In addition to One Identity Manager's memory requirements of 16 GB+ RAM (non-production) and 64 GB+ (production), Data Governance Edition requires an extra 16 GB of RAM.
Free disk space	In addition to One Identity Manager's database server requirements of 100GB, Data Governance Edition requires an extra 30GB per million resources.

Operating system	<p>64-bit Windows operating systems:</p> <ul style="list-style-type: none"> Note the requirements given by Microsoft for the SQL Server version you are using. <p>NOTE: The 64-bit requirement for Windows Servers is specific to Data Governance Edition.</p> <p>UNIX and Linux operating systems:</p> <ul style="list-style-type: none"> Note the requirements given by the operating system manufacturer for SQL Server databases.
Software	<p>Supported SQL Server versions are:</p> <ul style="list-style-type: none"> SQL Server 2017 Standard Edition (64-bit) with the current cumulative update SQL Server 2019 Standard Edition (64-bit) with the current cumulative update <p>NOTE: The cumulative update 2 for SQL Server 2019 is not supported.</p> <ul style="list-style-type: none"> Azure SQL Managed Instance <p>NOTE: For performance reasons, the use of SQL Server Enterprise Edition is recommended for live systems.</p> <ul style="list-style-type: none"> Compatibility level for databases: SQL Server 2017 (140) Default collation: case insensitive, SQL_Latin1_General_CP1_CI_AS (recommended) SQL Server Management Studio (recommended)

NOTE: The minimum requirements listed above are considered to be for general use. With each custom One Identity Manager deployment these values may need to be increased to provide ideal performance. To determine production hardware requirements, it is strongly recommended to consult a qualified One Identity Partner or the One Identity Professional Services team. Failure to do so may result in poor database performance.

For additional hardware recommendations, read the KB article <https://support.oneidentity.com/identity-manager/kb/290330/how-to-configure-settings-as-per-the-system-information-overview>, which outlines the System Information Overview available within One Identity Manager.

For installation and operation of a One Identity Manager database, the following database server and database settings are required.

Table 6: Database server settings

Property	Value	Comment
Language	English	

Property	Value	Comment
Server Collation	Case insensitive SQL_Latin1_General_CP1_CI_AS (recommended)	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Extreme transaction processing supported (is XTP supported)	True	<p>One Identity Manager uses In-Memory-OLTP (Online Transactional Processing) for memory-optimized data accesses. The database server must support extreme transaction processing (XTP). This function is activated by default in a standard installation.</p> <p>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database. If XTP is not activated, the installation or update is not started.</p>
SQL Server Agent	Started	<p>Start the SQL Server Agent in the SQL Server Service Management Portal. You can log in to a SQL Server Agent as a domain user with Windows authentication or with a local system account.</p> <p>The settings is checked by the Configuration Wizard before installing or updating the One Identity Manager database. If the SQL Server Agent is not started, the installation or update is not started.</p>
Collation	SQL_Latin1_General_CP1_CI_AS	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Recovery model	Simple	<p>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database. If the recovery model is not set to the value Simple, a warning is issued before installing or updating starts. You can ignore this warning.</p> <p>For performance reasons, however, it is recommended you set the database to</p>

Property	Value	Comment
		the Simple recovery model for the duration of the schema installation or update.
Compatibility level	SQL Server 2017 (140)	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Create Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Auto Update Statistics Asynchronously	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Arithmetic Abort enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Quoted Identifiers Enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Broker Enabled	True	The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Is Read Committed Snapshot On	True	The default setting for transactions is AutoCommit . If transactions are required, they are opened explicitly.

Property	Value	Comment
		<p>These settings have proven to provide the best balance between data security and performance for One Identity Manager's massive parallel processing. Other translation modes are not supported by One Identity Manager.</p> <p>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</p>
Parameterization	Forced	<p>The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.</p>
Database file and data file group for memory-optimized tables	Required	<p>One Identity Manager uses In-Memory-OLTP (Online Transactional Processing) for memory-optimized data accesses.</p> <p>For the creation of memory-optimized tables, the following prerequisites must be met:</p> <ul style="list-style-type: none"> • A database file with the Filestream data file type must exist. • A memory-optimized data file group must exist. <p>Before installation or update of the One Identity Manager database, the Configuration Wizard checks whether these requirements are fulfilled.</p> <p>In the Configuration Wizard, repair methods are available to create the database file and the data file group. The database file is created by the repair method in the directory of the data file (*.mdf).</p>

For details about installation and operation of One Identity Manager database using Azure SQL Managed Instance, please refer to [One Identity Manager Installation Guide: Identity Manager - Installation Guide \(oneidentity.com\)](#).

Data Governance agent

The Data Governance agent refers to the server hosting a local or remote Data Governance Edition agent.

This server must meet the following minimum system requirements.

Table 7: Minimum system requirements: Data Governance agent

Processor	500MHz+
Memory	1024MB RAM
Free disk space	20 GB NOTE: The agent will use the required CPU, memory and disk space to perform scans, data synchronizations, queries and activity reporting. Unexpected behavior will occur if any of these resources are depleted.
Operating system	<p>Windows operating systems:</p> <ul style="list-style-type: none">• Windows Server 2008• Windows Server 2008 (R2) (32-bit or non-Itanium 64-bit)• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019 <p>New Dynamic Access Control (DAC) features are not supported.</p> <p>NOTE: When an agent is installed on Windows Server 2012/2012 R2, disable the following local policy: "User Account Control: run all Administrators in Admin Approval Mode".</p> <p>NOTE: The following certificate must be installed as a Trusted Root Certification Authority on the target agent host computer: VeriSign Class 3 Public Primary Certification Authority — G5.cer.</p>
Software	<p>.NET Framework 4.7.2 or later</p> <p>.NET Framework 3.5.1 (SharePoint 2010 agents)</p> <p>NOTE: SharePoint 2010 agents require .NET Framework 3.5.1; all other Windows Servers and SharePoint farms hosting an agent require .NET Framework 4.5 or later.</p> <p>Windows Servers hosting an agent for SharePoint Online or EMC Isilon NFS Device require TLS 1.2.</p>

Resource Activity database server

The Resource Activity Database server refers to the server hosting the Data Governance Edition Resource Activity database.

NOTE: You can use your pre-existing One Identity Manager database server to host the resource activity database.

This server must meet the following system requirements.

Table 8: Minimum system requirements: Resource Activity Database server

Processor	quad core CPU
Memory	16GB RAM
Free disk space	100GB

Supported target systems

The following systems are supported to be scanned.

Table 9: Supported target systems

Target	Version	Additional notes
Windows Server	<p>The following Windows Server versions are supported for scanning (local or remote managed hosts):</p> <ul style="list-style-type: none">• Windows Server 2008• Windows Server 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016• Windows Server 2019 <p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	Resource activity collection is not supported for remotely managed Windows Server hosts.
Windows Cluster	The following failover clusters	Resource activity collection is

Target	Version	Additional notes
	<p>are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> • Windows 2008 • Windows 2008 (R2) • Windows 2012 • Windows 2012 (R2) • Windows 2016 • Windows 2019 <p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	not supported for Windows clusters.
NetApp CIFS Devices	<p>The following NetApp file versions (with CIFS file system protocol enabled) are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> • NetApp ONTAP 7.3 • NetApp ONTAP 8.0 • NetApp ONTAP 8.1 • NetApp ONTAP 8.2 • NetApp ONTAP 8.3 • NetApp ONTAP 9.0 RC1 • NetApp ONTAP 9.1 • NetApp ONTAP 9.2 • NetApp ONTAP 9.3 • NetApp ONTAP 9.4 • NetApp ONTAP 9.5 • NetApp ONTAP 9.6 • NetApp ONTAP 9.7 • NetApp ONTAP 9.8 <p>Both NetApp 7-Mode and Cluster Mode are supported.</p>	<p>Real-time security updates and resource activity collection are not supported on versions of NetApp ONTAP filers earlier than 7.3.</p> <p>NetApp storage devices require additional configuration. See NetApp managed host deployment prior to adding a NetApp managed host.</p>

Target	Version	Additional notes
	<p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	
NetApp NFS Devices	<p>The following NetApp filer versions (with NFS file system protocol enabled) are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> • NetApp ONTAP 7.3 • NetApp OnTAP 8.0 • NetApp ONTAP 8.1 • NetApp ONTAP 8.2 • NetApp ONTAP 8.3 • NetApp ONTAP 9.0 RC1 • NetApp ONTAP 9.1 • NetApp ONTAP 9.2 • NetApp ONTAP 9.3 • NetApp ONTAP 9.4 • NetApp ONTAP 9.5 • NetApp ONTAP 9.6 • NetApp ONTAP 9.7 • NetApp ONTAP 9.8 <p>Both NetApp 7-Mode and Cluster Mode are supported.</p> <p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	<p>NFS managed hosts require the UNIX module to be installed during the One Identity Manager installation and configuration process.</p> <p>For NetApp 7-Mode managed hosts, real-time security updates and resource activity collection require FPolicy; and in order to use FPolicy, CIFS must be installed and running.</p> <p>NetApp storage devices require additional configuration. See NetApp managed host deployment prior to adding a NetApp managed host.</p>
EMC CIFS Devices	<p>The following EMC devices are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> • EMC Celerra 	<p>VNXe is not supported. VNXe does not support CEPA currently and therefore Data Governance Edition will not run successfully in VNXe</p>

Target	Version	Additional notes
	<ul style="list-style-type: none"> • EMC VNX • EMC Isilon <p>The following EMC Framework versions (with CIFS file system protocol enabled) are supported:</p> <ul style="list-style-type: none"> • Common Event Enabler (CEE) 7.1 (or higher) <p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	<p>environments.</p> <p>EMC storage devices require additional configuration.</p> <p>See Appendix: EMC managed host deployment prior to adding an EMC managed host.</p> <p>Common Event Enabler (CEE) versions 8.7.8.1 and 8.7.8.2 are not yet supported.</p>
EMC Isilon NFS Devices	<p>The following EMC Isilon devices (with NFS file system protocol enabled) are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> • EMC Isilon 7.2 • EMC Isilon 8.0 • EMC Isilon OneFS 8.1.2 • EMC Isilon OneFS 8.2 • EMC Isilon OneFS 8.2.1 • EMC Isilon OneFS 8.2.2 • EMC Isilon OneFS 9.0 • EMC Isilon OneFS 9.1 <p>NOTE: The space required depends on the configuration, the number of files, folders and shares scanned with explicit permissions, and the amount of activity processed.</p>	<p>NFS managed hosts require the UNIX module to be installed during the One Identity Manager installation and configuration process.</p> <p>Resource activity collection is not supported for EMC Isilon NFS managed hosts.</p> <p>EMC storage devices require additional configuration. See EMC managed host deployment prior to adding an EMC managed host.</p>
SharePoint	<p>The following SharePoint versions are supported for scanning (local managed host):</p> <ul style="list-style-type: none"> • SharePoint Server 2010 • SharePoint Server 2013 	<p>Agent is installed where the One Identity Manager service (job server) is running for the SharePoint farm.</p> <p>We recommend installing the One Identity Manager service</p>

Target	Version	Additional notes
	<ul style="list-style-type: none"> SharePoint Server 2016 SharePoint Server 2019 <p>100GB disk space on the SharePoint agent computer for data storage and scan post-processing activities.</p> <p>NOTE: The space required depends the number of sites, lists, and document libraries and the number of unique permissions gathered from the farm.</p> <p>8GB RAM for the SharePoint agent computer.</p>	<p>on a dedicated SharePoint Application Server in the farm and not on a Web Front server which prevents extra load processing on that server.</p> <p>Standalone farms are not supported.</p> <p>Farms configured with only Local Users and Groups are not supported.</p>
Cloud	<p>The following cloud providers running on Office 365 are supported for scanning (remote managed host):</p> <ul style="list-style-type: none"> SharePoint Online OneDrive for Business 	<p>Resource activity collection is not supported for Cloud managed hosts.</p> <p>OneDrive for Business support is limited to the Documents folder for the Administrator account. Therefore, all managed paths are selected within the scope of the Administrator's Documents folder.</p>
DFS Root	Windows 2008 Active Directory DFS and higher	

Data Governance Edition minimum permissions

The following table contains the permissions required to properly deploy Data Governance Edition.

Table 10: Required minimum permissions

Account	Permission
System user (Active Directory account)	Must have an associated One Identity Manager Employee.

Account	Permission
logged on to the computer) AND Manager user (Active Directory account running the Manager)	Employee must be assigned the Data Governance Administrators application role or the Data Governance Access Managers application role. NOTE: If the System user does not have the appropriate roles assigned, you will see the Data Governance Edition features in the Manager, but will encounter errors when attempting to perform Data Governance Edition-related tasks. If the Manager user does not have the appropriate roles assigned, you will not see the Data Governance Edition features in the Manager.
Service account assigned to a managed domain	Log On as a Service local user rights on the Data Governance server. Local Administrator rights on Data Governance agent computers. NOTE: If you see errors after granting Local Administrator rights, log off and log on to the computer where Local Administrator was granted. If the service account is not a member of the Domain Users group (for example, a user from domain A is used to manage trusted domain B), additional rights are required. For more information, see Service Account is not a member of the Domain Users group on page 29.
SQL service account for connection with the Data Governance Resource Activity database	dbcreator server role is required to create the database during initial configuration of Data Governance Edition db_owner role is required to work with the database
SQL service account for connection with One Identity Manager database	db_owner role for One Identity Manager database
Service account for an agent on Local Windows managed hosts	The agent runs under the Local System account. No additional rights are required.
Service account for an agent managing remote Windows managed hosts	Local Administrator rights on the managed host. NOTE: If you see errors after granting Local Administrator rights, log off and log on to the computer where Local Administrator was granted. Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.)
Service account for an	Must be the SharePoint farm account (same account that is used

Account	Permission
agent managing SharePoint farms	to run the SharePoint timer service and the One Identity Manager service (job server)). This account also needs to be a member of the administrators group on the SharePoint server. Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.)
Service account for an agent managing NetApp filers	Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.) Must be a member of the local Administrators group on the NetApp filer in order to create FPolicy. Must have permissions to access folders being scanned.
Service account for an agent managing EMC Isilon storage devices	Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.) Must have "run as root" permissions on the Isilon SMB share that has been selected as a managed path.
One Identity Manager service (job server) account used for scheduling Data Governance Edition reports	Must have an associated One Identity Manager Employee. Employee must be assigned the Data Governance Administrators application role or the Data Governance Access Managers application role.
Active Directory account used by the AppServer to establish communication between the Data Governance server and the Manager	Must have an associated One Identity Manager Employee. Employee must be assigned the Data Governance Administrators and the Data Governance Access Managers application roles. NOTE: This account must be added as the AppServer pool identity in Internet Information Services (IIS) Manager. If the AppServer application pool is set to the default Network Security identity, Data Governance Edition reports will fail to generate.

Granting SQL Server permissions

To grant SQL Server permissions

1. Create a new SQL login or use an existing login. (Open SQL Management Studio, connect to the SQL Server, expand the Security node – Logins, and create a new login or select an existing login.)
2. Open the login properties, and select the required server role.

NOTE: The Public role is selected by default.

3. Switch to User Mapping and select a database for which the permissions need to be granted and select the required database roles.

Granting Active Directory permissions

Service Account is not a member of the Domain Users group

Domain users can Read All Properties and List Content in domains to which they belong. However, when a user account is used to manage a trusted domain, they must be assigned permissions to List Content and grant properties through ADSIEDIT.msc.

If the service account is not a member of the Domain Users group (for example, a user from domain A is used to manage trusted domain B), the following additional rights are required in the domain to be managed:

- List Contents and Read All Properties rights on the managed domain.
- List Contents and Read All Properties rights on the system container of the managed domain.
- Read All Properties on the OU containing all domain groups.
- Service connection point should be created manually.

These rights will function for forest-wide authentication. For selective authentication, the service account must be a member of the domain you want to manage.

To assign "List Contents" and "Read All Properties" rights on the managed domain

1. Right-click the domain root and select **Properties**.
2. Click the **Security** tab, and click **Advanced**.
3. Click **Add**, select the required account, and assign **List Contents** and **Read All Properties**.
4. Apply it to **This object only**.

To assign "List Contents" and "Read All Properties" rights on the system container of the managed domain

1. Right-click the system container and select **Properties**.
2. Click the **Security** tab, and click **Advanced**.
3. Click **Add**, select the required account, and assign **List Contents** and **Read All Properties**.
4. Apply it to **This object only**.

To assign "Read All Properties" rights to OUs containing all domain groups

1. Right-click the domain root, select **Properties**.
2. Click the **Security** tab, and click **Advanced**.

3. Click **Add**, select the required account, and assign **Read All Properties** to all descendant group objects.

To manually create a service connection point

NOTE: When the Data Governance service starts up, a Service Connection Point (SCP) is automatically created/updated. The Data Governance Configuration wizard specifies the deployment name assigned to a Data Governance Edition deployment and the Data Governance service will install the SCP with that name. "DEFAULT" is the default deployment name.

When an account from a trusted domain is used, use the following PowerShell command to register the SCP:

```
Register-QServiceConnectionPoint -DomainDNSName <Fully Qualified Domain DNS Name> -DeploymentID <Deployment Name> -ServerDNSName <Fully Qualified DGE Server DNS Name> -ServerNetTcpPortNumber 8722
```

NOTE: To find the DeploymentID run the Get-QDeploymentInfo command.

NOTE: The HTTP port aligns with the net.tcp port; therefore, when you specify the ServerNetTcpPortNumber, the HTTP port automatically selects -1 from the port specified in the ServerNetTcpPortNumber parameter.

If you find it necessary to remove the SCPs from a single Data Governance Edition deployment or all deployments, use the Remove -QServiceConnectionPoint PowerShell command.

Data Governance Edition required ports

NOTE: For agent deployments, open the following file and printer sharing ports:

- TCP 135
- UDP 137
- UDP 138
- TCP 139
- TCP 445

Table 11: Ports required for communication

Port	Direction	Description
8721	Incoming	TCP (HTTP) port opened on the Data Governance server computer. This is the base port for the Data Governance REST API, used for communication with Data Governance server REST services, including the One Identity Manager clients and Windows PowerShell.
8722	Incoming	TCP (net.tcp) port opened on the Data Governance server

Port	Direction	Description
		<p>computer. Used for communication with Data Governance agents, One Identity Manager clients, One Identity Manager web server, and PowerShell.</p> <p>NOTE: The net.tcp port is configurable in the Data Governance Configuration wizard. The HTTP port (8721) listed above should always be 1 less than the net.tcp port. These first two ports align with the base addresses in the DataGovernanceEdition.Service.exe.config file under the IndexServerHost service. It is highly recommended that you only change this port using the Data Governance Configuration wizard to ensure the configuration file, One Identity Manager database and service connection points are updated properly; otherwise, you may lose connection with the Manager, the Data Governance service and/or Data Governance agents.</p> <p>IMPORTANT: Do NOT use the Designer to change the QAMServer configuration parameters, including the Port parameter.</p>
8723	Incoming	HTTP port used for communication with the One Identity Manager web server (/landing and /home pages).
18530 - 18630	Incoming	TCP port range opened on all agent computers. Used for communication with the Data Governance server. (The first agent on an agent host will use port 18530, and each subsequent agent on the same host will take the next available port, i.e., 18531, 18532, and so on.). In addition, this range is used to open a TCP listener for NetApp Cluster Mode hosts if resource activity collection is enabled.

Install One Identity Manager Data Governance Edition

A Data Governance Edition deployment relies on a successfully deployed One Identity Manager. The intent of this guide is to focus on the Data Governance Edition components. For complete details on installing and configuring the One Identity Manager components see the *One Identity Manager Installation Guide*.

NOTE: One Identity Manager Data Governance Edition requires a number of "modules" to be enabled during installation in order to provide the proper connectivity to Active Directory, File System, and SharePoint as well as presenting IT and business functions throughout the product. Installing **One Identity Manager Data Governance Edition** ensures that you have the required modules available.

If you have NetApp or EMC Isilon storage devices with NFS file system protocol enabled and want to add NFS managed hosts to your Data Governance Edition deployment, you must also install the **UNIX** module.

Data Governance Edition requires the **Azure Active Directory** and **SharePoint Online** modules for scanning folders hosted on SharePoint Online or OneDrive for Business host types.

To install One Identity Manager Data Governance Edition:

1. Run the Autorun.exe program. Open the **Installation** page and install **One Identity Manager Data Governance Edition**.
2. The One Identity Manager Data Governance Edition setup wizard appears. Click **Next** to start the installation and follow the prompts on the screens.

NOTE: To install the **UNIX** module required for NFS managed hosts:

1. On the **Installation Settings** page of the setup wizard, select the **Add more modules to the selected edition** check box.
2. On the **Module selection** page, select **Unix** under the **Target Systems** pane.


NOTE: To install the **Azure Active Directory** and **SharePoint Online** modules required for cloud managed hosts:

- a. On the **Installation Settings** page of the setup wizard, select the **Add more modules to the selected edition** check box.
 - b. On the **Module selection** page, select **Azure Active Directory** and **SharePoint Online** under the **Target Systems** pane.
 - c. On the **Assign Machine Roles** page, expand **Server | Job Server** and select **Azure Active Directory** and **O3S**.
3. Once the installation has successfully completed, use the options on the last page of the setup wizard to run the following configuration programs:


- a. Run the **Configuration wizard** to create and configure the One Identity Manager database.
 - b. Run the **Job Service Configuration** to configure the One Identity Manager service.

Once the job service configuration is completed, perform the following steps to ensure that the One Identity Manager service (job server) is successfully configured for use with Data Governance Edition.

- i. Run the Windows Services snap-in and locate the One Identity Manager Service.
 - i. Double-click to open the properties dialog.
 - ii. Open the Log On tab and select the **This account** option. Enter the user account and credentials to be used for the service.
 - iii. Click **Apply** and then click **OK** to close the properties dialog.
 - ii. Open the Designer.
 - i. In the lower pane of the navigation view, select **Base Data**.
 - ii. In the Base Data navigation view, select **Installation | Job server**.
 - iii. At the bottom of the right pane, select the **Server functions** tab. Ensure that the following server functions are checked (Double-click a server function to select it.)
 - Active Directory connector
 - CSV connector
 - Data Governance connector
 - Default report server
 - One Identity Manager connector
 - SharePoint connector
 - SMTP host
 - Unix connector (if scanning NFS managed hosts)

After ensuring these server functions are selected, click the  **Commit to database** toolbar button.

- iv. Select the **One Identity Manager Service configuration** tab (bottom of the right pane). Ensure the job server configuration file previously created is being used.

- Click the  **File open** toolbar button.
- Locate and select the JobService.cfg file and click **Open**.

After ensuring the correct job server configuration file is being used, click the **Commit to database** toolbar button.

- iii. Run the Services snap-in and start the One Identity Manager Service.
- c. Run the **Data Governance Configuration** to deploy the Data Governance server and create the Data Governance Resource Activity database. For more information, see [Deploy Data Governance Edition components](#) on page 35.

NOTE: At this point in the process, you can use the Manager to configure Data Governance service accounts and managed domains, add managed hosts and deploy agents. For more information on service accounts and managed domains, see [Authentication using service accounts and managed domains](#). For more information on managed hosts and agents, see [Working with managed hosts and agents](#).

4. Back on the **Installation** page of the Autorun, install the Web based components. For more information, see the *One Identity Manager Installation Guide*.
5. To get a complete view of your environment, run the One Identity Manager Synchronization Editor to synchronize your target environments (Active Directory and if applicable, SharePoint, UNIX, Azure Active Directory, and SharePoint Online). For more information, see [One Identity Manager - Synchronization projects](#) on page 51.

Deploy Data Governance Edition components

[Deployment pre-flight check](#)

[Data Governance service deployment methods](#)

[Deploying Data Governance service and creating Resource Activity database](#)

[Deploying multiple Data Governance services](#)

[Updating One Identity Manager to a Data Governance Edition deployment](#)

Deployment pre-flight check

Prior to deploying the Data Governance Edition components, including the Data Governance service and Resource Activity database:

- Identify the server where you intend to install the Data Governance service and the associated credentials required. This information is required to complete the installation process.
- Ensure servers meet minimum hardware and software requirements. For more information, see [Data Governance Edition system requirements](#) on page 15.
- Ensure appropriate ports are opened on the Data Governance server computer. For more information, see [Data Governance Edition required ports](#) on page 30.
- Ensure One Identity Manager has been successfully installed. For more information, see [Install One Identity Manager Data Governance Edition](#) on page 32.

Data Governance service deployment methods

This table lists the methods that can be used to deploy Data Governance Edition components, including the Data Governance service and Resource Activity database.

Table 12: Data Governance service deployment methods

Deployment method	Description	Notes/Additional information
Data Governance Configuration wizard	<p>The recommended method for deploying the Data Governance service and Data Governance Resource Activity database.</p> <p>The wizard can be accessed using the following methods:</p> <ul style="list-style-type: none">• On the last page of the One Identity Manager setup wizard, click the Run button to the left of the Data Governance Configuration option.• Select the %ProgramFiles%\One Identity\One Identity Manager\Data Governance Configuration Wizard.exe file. Ensure that you right-click and Run as administrator.	<p>Running the Data Governance Configuration wizard:</p> <ul style="list-style-type: none">• launches the Data Governance service installer• configures the Data Governance service• establishes the required connections between the Data Governance service and One Identity Manager• initializes the Data Governance Resource Activity database <p>For more information on using the Data Governance Configuration wizard, see Deploying Data Governance service and creating Resource Activity database.</p>
Windows Installer	<p>Use to manually install the Data Governance service.</p> <p>Use this method, to install the Data Governance service to a different location other than the default directory.</p> <p>Once installed, use the following PowerShell cmdlets in the OneIdentity.DataGovernance snap-in to manually configure and initialize the Data Governance Edition components:</p>	<p>The Data Governance service installer is included in the autorun and can be found in the QAM module's directory. For example, C:\<DGE Build>\Modules\QAM\dvd\DataGovernance_ServerComponentsInstaller_x64.msi.</p> <p>Only a 64-bit version is available.</p> <p>For more information on the Windows Installer options available and instructions on manually deploying the Data Governance service, see the <i>One Identity Manager Data Governance</i></p>

Deployment method	Description	Notes/Additional information
	<ul style="list-style-type: none"> • Set-QServiceConnection: To set the server name and port information used by the Data Governance Edition commands to connect to the Data Governance server. • Initialize-QDataGovernanceServer: To establish the database connection between One Identity Manager and Data Governance Edition. • Initialize-QDataGovernanceActivity: To initialize the database to store data generated when a managed host has resource activity tracking enabled. 	<p><i>Edition Technical Insight Guide.</i></p> <p>For more information on using Windows PowerShell to manage your Data Governance Edition deployment, see the <i>One Identity Manager Data Governance Edition Technical Insight Guide</i>.</p>

Deploying Data Governance service and creating Resource Activity database

Using the Data Governance Configuration wizard is the recommended method for deploying and configuring the Data Governance service and creating the Data Governance Resource Activity database.

IMPORTANT: When you follow the steps outlined in the [Deployment overview](#) and run the Data Governance Configuration wizard before you run the One Identity Manager Synchronization Editor, the Data Governance service will perform the following tasks allowing you to add managed hosts and deploy agents:

- automatically harvest forest topology to populate the appropriate One Identity Manager Active Directory (ADS) components in the Manager with all of the domains and all of the enabled 'server' computer objects, including NetApp and EMC servers.
- automatically create One Identity Manager Employee records for all members found in each domain's Domain Admins group membership, including linking the

Active Directory accounts to the employees and assigning the Data Governance application roles and target system role.

- automatically create a One Identity Manager Employee record for the current user account that was used to run the configuration wizard, including linking the Active Directory account to the employee and assigning the Data Governance application roles and the target system role in each domain found during the forest topology harvest.

However, if you run the One Identity Manager Synchronization Editor prior to running the Data Governance Configuration wizard, the Data Governance service will NOT perform the automated steps mentioned above. Meaning that you must wait for the Active Directory synchronization process to finish each domain project before you can configure Employee records and assign One Identity Manager application roles, configure Data Governance service accounts and managed domains, and add managed hosts and deploy agents.

NOTE: The following procedure details installing the Data Governance service to a default location. However, if required, you can install the service to another location by running the Data Governance server msi. For more information, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

This should be performed before running the Data Governance Configuration wizard so that it is available for the **Connect to the existing Data Governance service** option.

To deploy a new Data Governance service and resource activity database

1. Run the Data Governance Configuration wizard using one of the following methods:
 - If you still have the One Identity Manager Data Governance Edition setup wizard open, click the **Run** button to the left of the **Data Governance Configuration** option on the last page of the wizard.
 - Otherwise, locate and select the Data Governance Configuration Wizard.exe file, which is located in the %ProgramFiles%\One Identity\One Identity Manager\ directory. Ensure you right-click and select **Run as Administrator**.
2. Read the **Configuration wizard welcome** page and click **Next**.
3. On the **One Identity Manager database** page, specify the information required to connect to the One Identity Manager database.
 - a. **Server:** Select the server where the One Identity Manager database is installed.
 - b. **Windows authentication:** If you selected Windows authentication for the One Identity Manager database, select this check box. If you selected SQL authentication for the One Identity Manager database, make sure this check box is cleared.
 - c. **User:** Enter the user account to be used to access the One Identity Manager database server.
 - d. **Password:** Enter the password associated with the user account.
 - e. **Database:** Select the One Identity Manager database.

Click **Next**.

4. On the **Data Governance Edition Configuration** page, select **Install or Upgrade the Data Governance service** and provide the following information:

- a. **Server:** Enter the fully qualified domain name of the server where the Data Governance service will be installed.
- b. **Port:** This field displays the net.tcp port opened on the Data Governance server computer. In a new Data Governance Edition deployment, the default net.tcp port is 8722. To change this value, enter the port number to be used to communicate with the Data Governance service.

NOTE: The HTTP port aligns with the net.tcp port and automatically selects -1 from the port specified here. The HTTP port is used by the Data Governance agents if WCF fails.

- c. **Deployment:** This field displays the deployment name assigned to the Data Governance Edition deployment. In a new Data Governance Edition deployment, the default deployment name is DEFAULT.

To change this value, enter the name to be associated with this deployment of Data Governance Edition. The deployment name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

NOTE: The deployment name is also used in the Data Governance Resource Activity database name (that is, DGE_<DeploymentName>) and that name also has a limit of 30 characters. So, if you specify a 30 character deployment name, the new activity database name will only use <DeploymentName>.

NOTE: When deploying multiple Data Governance Edition deployments in a forest, specify a different server for the Data Governance service and a unique deployment name for each deployment. For more information, see [Deploying multiple Data Governance services](#) on page 41.

Leave the **Add the current user to the One Identity Manager Employees with Data Governance application roles** check box selected. The Data Governance service automatically assigns the current user account the Data Governance application roles and target system role in each domain found during the forest topology harvest.

NOTE: The Data Governance service obeys the current One Identity Manager "Edit Configuration Parameters"\TargetSystem\ADS\PersonExcludeList, which by default is:

ADMINISTRATOR | GUEST | KRBTGT | TSINTERNETUSER | IUSR_.* | IWAM_.* | SUPPORT_.* |.*\

This means that ANY Active Directory account sAMAccount name that matches any of the names specified in this exclude list, including 'administrator' will not be added as a One Identity Manager Employee with the assigned Data Governance application roles, even if the current user running the configuration wizard is the administrator account.

Click **Next**.

5. In the **Service Account Setting** dialog, specify the account to be used to run the Data Governance service.
 - a. When SQL authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is cleared on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is selected by default indicating the local system account will be used to run the Data Governance service.
 - To use a service account other than the local system account, clear the **Use LocalSystem account** check box and enter the Windows credentials of the service account to be used.

NOTE: If you specify a service account, you must move the Service Principal Name (SPN) from the computer object. For more information, see [Move Service Principal Name in Active Directory](#) on page 49.
 - b. When Windows authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is selected on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is disabled and you must enter the Windows credentials of the service account to be used.

After specifying the account to be used for the Data Governance service, click **OK**.

6. Wait for the installation process to complete, click **Finish** to close the **Data Governance server installation** dialog.
7. On the **Data Governance activity database server - Create connection** page, enter the connection information for the server where the Data Governance Resource Activity database will be created:
 - a. **Server:** Select the server where the Data Governance Resource Activity database is to be created.
 - b. **Windows Authentication:** If you select **Windows Authentication** for the One Identity Manager database authentication method, enter the Windows credentials for the account that will run the Data Governance service.

NOTE: If you selected SQL server authentication for the One Identity Manager database authentication method, use SQL authentication here as well. If you selected Windows authentication for the One Identity Manager database authentication method, you can select either SQL authentication or Windows authentication for the resource activity database.
 - c. **User:** Enter the user account to be used to access the Data Governance Resource Activity database server.
 - d. **Password:** Enter the password associated with the user account.

Click **Next**.

8. On the **Data Governance activity database server - Database Properties** page, click **Next** to accept the default database name for which the schema for the

Data Governance Resource Activity database should be created and to accept the default database options.

The **Database name** field is pre-populated with DGE_<DeploymentName>. Where <DeploymentName> is the name assigned to the Data Governance Edition deployment on the previous wizard page. If the total length of the activity database name exceeds 30 characters, then the new default activity database name will only use <DeploymentName>.

To change the name, enter the new name to be assigned to the database. The database name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

IMPORTANT: When installing multiple Data Governance Edition deployments in the same forest, ensure that each deployment is connecting to a database with a unique name. Do NOT connect a new deployment to an existing database.

9. Once the installation and configuration has completed, click **Next**.
10. Click **Finish** to close the Data Governance Configuration wizard.
11. If applicable, click **Finish** to close the One Identity Manager setup wizard.

Before you can gather information on the data in your environment, perform the necessary post-installation configuration tasks. For more information, see [Post installation configuration](#) on page 49.

Deploying multiple Data Governance services

When deploying multiple Data Governance services within the same forest in your organization, each Data Governance Edition deployment is responsible for managing specific servers and there is no cross-over between Data Governance services; therefore, data from one deployment is not available in another deployment.

Keep the following considerations in mind when deploying multiple Data Governance services in a single forest:

One Identity Manager:

- Each One Identity Manager installation can only have one Data Governance service and one Data Governance Edition deployment.
- Each Data Governance Edition deployment must connect to a separate One Identity Manager database.
- Each Data Governance Edition deployment uses different One Identity Manager services (job servers).

Data Governance services:

- Each Data Governance service must be installed on a separate server and be assigned a unique deployment name.

Data Governance agents:

- Agent-hosted servers belong to one Data Governance Edition deployment, and cannot be accessed by other deployments.
- You can deploy multiple Data Governance agents on a server; however, all of these agents must belong to the same Data Governance Edition deployment.

The following procedure assumes that a Data Governance Edition deployment has been installed following the procedures described in [Deploying Data Governance service and creating Resource Activity database](#). This procedure explains how to install additional Data Governance Edition deployments:

To install subsequent Data Governance Edition deployments

1. Run the Autorun.exe and install a new One Identity Manager Data Governance Edition installation.
2. Once the installation has successfully completed, use the options on the last page of the setup wizard to run the following:
 - a. Run the **Configuration Wizard** to create and configure a new One Identity Manager database.
 - b. Run the **Job Service Configuration** to configure a new One Identity Manager service.
3. Run the Data Governance configuration wizard using one of the following methods:
 - If you still have the One Identity Manager Data Governance Edition setup wizard open, click the **Run** button to the left of the **Data Governance Configuration** option on the last page of the wizard.
 - Otherwise, locate and select the Data Governance Configuration Wizard.exe file, which is located in the %ProgramFiles%\One Identity\One Identity Manager\ directory. Ensure you right-click and select **Run as Administrator**.
4. On the **One Identity Manager database** page, specify the information required to connect to the One Identity Manager database. This must be a different One Identity Manager database for each Data Governance Edition deployment.
5. On the **Data Governance Edition Configuration** page, select the **Install or Upgrade the Data Governance service** option and provide the following information:
 - a. **Server:** Enter the fully qualified domain name of the server where this Data Governance service will be installed. Ensure that you specify a server that does NOT already host a Data Governance service.

- b. **Port:** Enter the port number to be used to communicate with the specified Data Governance service. In a new Data Governance Edition deployment, this field displays the default net.tcp port of 8722.
- c. **Deployment:** Enter a unique name to be assigned to this Data Governance Edition deployment. Ensure that this name is unique and is not being used by another Data Governance Edition deployment in the forest.

The deployment name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

NOTE: The deployment name is also used in the Data Governance Resource Activity database name (that is, DGE_<DeploymentName>) and that name also has a limit of 30 characters. So, if you specify a 30 character deployment name, the new activity database name will only use <DeploymentName>.

- d. Leave the **Add the current user to the One Identity Manager Employees with Data Governance application roles** check box selected to have the Data Governance service assign the current user account the Data Governance application roles and target system role in each domain found during the forest topology harvest.

Click **Next**.

NOTE: If the **Next** button is disabled, ensure that you have selected a server that does not already host a Data Governance service and have entered a unique deployment name that is not being used by another Data Governance Edition deployment in the forest.

6. In the **Service Account Setting** dialog, specify the account to be used to run the Data Governance service.
 - a. When SQL authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is cleared on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is selected by default indicating the local system account will be used to run the Data Governance service.
 - To use a service account other than the local system account, clear the **Use LocalSystem account** check box and enter the Windows credentials of the service account to be used.
 - b. When Windows authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is selected on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is disabled and you must enter the Windows credentials of the service account to be used.

NOTE: When you use a service account, you must move the Service Principal Name (SPN) from the computer object. For more information, see [Move Service Principal Name in Active Directory](#) on page 49.

After specifying the account to be used for the Data Governance service, click **OK**.

7. Wait for the installation process to complete, click **Finish** to close the **Data Governance server installation** dialog.
8. On the **Data Governance activity database server - Create connection** page, specify the connection information for the server where a new Data Governance Resource Activity database is to be created.
9. On the **Data Governance activity database server - Database Properties** page, click **Next** to accept the default database name for which the schema for the Data Governance Resource Activity database should be created and to accept the default database options.

The **Database name** field is pre-populated with DGE_<DeploymentName>. Where <DeploymentName> is the name assigned to the Data Governance Edition deployment on the previous wizard page. If the total length of the activity database name exceeds 30 characters, then the new default activity database name will only use <DeploymentName>.

To change the name, enter the new name to be assigned to the database. The database name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

If you change the database name, ensure that it is unique and is not being used by any other Data Governance Resource Activity database. Do NOT connect a new deployment to an existing database.

10. Once the installation and configuration has completed, click **Next**.
11. Click **Finish** to close the Data Governance Configuration wizard.
12. If applicable, click **Finish** to close the One Identity Manager Data Governance setup wizard.

Before you can gather information on the data in your environment, perform the necessary post-installation configuration tasks. For more information, see [Post installation configuration](#) on page 49.

Tips for connecting to and installing agents in a multi-Data Governance Edition deployment:

- When launching the Manager, in the **Select Connection** field, select the One Identity Manager database to which the required deployment is connected.
- If you attempt to install an agent to a server that already has an agent on it, and that agent already belongs to another Data Governance Edition deployment, you will receive a status of 'Installing agent failed'. Open the **Agents** view and you will see an agent status of 'Agent host belongs to another deployment'. The Configuration Message property on the **Agent Details** master data page will contain additional information, including the name of the deployment that is already using this agent.

Updating One Identity Manager to a Data Governance Edition deployment

If you already have One Identity Manager 8.2 installed, you can add Data Governance Edition using the following steps:


- Enable the Data Governance (QAM) components in the Designer
- Run the Data Governance Configuration wizard to deploy the Data Governance Edition components

NOTE: If you are running the Designer from the computer hosting the One Identity Manager database or a job service, you must stop the One Identity Manager service when prompted to update. Once the update has completed, restart the service.

Administrative access is required on the local computer for this process to complete successfully.

NOTE: Use the job server editor in the Designer application to confirm the "Data Governance connector" flag is set for any job server to be used to run Data Governance Edition report requests from the web portal. For more information, see [Post installation configuration](#) on page 49.

To enable Data Governance Edition components

1. Open the Designer and select **Base Data | General | Configuration parameters**.
2. In the Tasks view, select **Edit configuration parameters**.
3. Expand **TargetSystem | ADS | QAM**.
4. Select the **QAM** check box and click the  **Commit to database** toolbar button.
5. Click **Save** on the confirmation dialog.
6. Select the **Database** menu, then **Compile database** and follow the wizard.

To configure and deploy Data Governance Edition components

1. Run the Data Governance Configuration wizard from the One Identity Manager installation directory: %ProgramFiles%\One Identity\One Identity Manager\Data Governance Configuration Wizard.exe.
2. Read the **Configuration wizard welcome** page and click **Next**.
3. On the **One Identity Manager database** page, specify the information required to connect to the One Identity Manager database.
 - a. **Server:** Select the server where the One Identity Manager database is installed.
 - b. **Windows authentication:** If you selected Windows authentication for the One Identity Manager database, select this check box. If you selected SQL

authentication for the One Identity Manager database, make sure this check box is cleared.

- c. **User:** Enter the user account to be used to access the One Identity Manager database server.
- d. **Password:** Enter the password associated with the user account.
- e. **Database:** Select the One Identity Manager database.

Click **Next**.

4. On the **Data Governance Edition Configuration** page, select **Install or Upgrade the Data Governance service** and provide the following information:

- a. **Server:** Enter the fully qualified domain name of the server where the Data Governance service will be installed.
- b. **Port:** This field displays the net.tcp port opened on the Data Governance server computer. In a new Data Governance Edition deployment, the default net.tcp port is 8722. To change this value, enter the port number to be used to communicate with the Data Governance service.

NOTE: The HTTP port aligns with the net.tcp port and automatically selects -1 from the port specified here. The HTTP port is used by the Data Governance agents if WCF fails.

- c. **Deployment:** This field displays the deployment name assigned to the Data Governance Edition deployment. In a new Data Governance Edition deployment, the default deployment name is DEFAULT.

To change this value, enter the name to be associated with this deployment of Data Governance Edition. The deployment name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

NOTE: The deployment name is also used in the Data Governance Resource Activity database name (that is, DGE_<DeploymentName>) and that name also has a limit of 30 characters. So, if you specify a 30 character deployment name, the new activity database name will only use <DeploymentName>.

NOTE: When deploying multiple Data Governance Edition deployments in a forest, specify a different server for the Data Governance service and a unique deployment name for each deployment. For more information, see [Deploying multiple Data Governance services](#) on page 41.

Leave the **Add the current user to the One Identity Manager Employees with Data Governance application roles** check box selected. The Data Governance service automatically assigns the current user account the Data Governance application roles and target system role in each domain found during the forest topology harvest.

NOTE: The Data Governance service obeys the current One Identity Manager "Edit Configuration Parameters"\TargetSystem\ADS\PersonExcludeList, which by default is:

ADMINISTRATOR | GUEST | KRBTGT | TSINTERNETUSER | IUSR_.* | IWAM_.* | SUPPORT_.* |.*\

This means that ANY Active Directory account sAMAccount name that matches any of the names specified in this exclude list, including 'administrator' will not be added as a One Identity Manager Employee with the assigned Data Governance application roles, even if the current user running the configuration wizard is the administrator account.

Click **Next**.

5. In the **Service Account Setting** dialog, specify the account to be used to run the Data Governance service.
 - a. When SQL authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is cleared on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is selected by default indicating the local system account will be used to run the Data Governance service.
 - To use a service account other than the local system account, clear the **Use LocalSystem account** check box and enter the Windows credentials of the service account to be used.

NOTE: If you specify a service account, you must move the Service Principal Name (SPN) from the computer object. For more information, see [Move Service Principal Name in Active Directory](#) on page 49.
 - b. When Windows authentication is being used for the One Identity Manager database authentication method (that is, the **Windows authentication** check box is selected on the **One Identity Manager database** page):
 - The **Use LocalSystem account** check box is disabled and you must enter the Windows credentials of the service account to be used.

After specifying the account to be used for the Data Governance service, click **OK**.

6. Wait for the installation process to complete, click **Finish** to close the **Data Governance server installation** dialog.
7. On the **Data Governance activity database server - Create connection** page, enter the connection information for the server where the Data Governance Resource Activity database will be created:
 - a. **Server:** Select the server where the Data Governance Resource Activity database is to be created.
 - b. **Windows Authentication:** If you select **Windows Authentication** for the One Identity Manager database authentication method, enter the Windows credentials for the account that will run the Data Governance service.

NOTE: If you selected SQL server authentication for the One Identity Manager database authentication method, use SQL authentication here as well. If you selected Windows authentication for the One Identity Manager database authentication method, you can select either SQL authentication or

| Windows authentication for the resource activity database.

- c. **User:** Enter the user account to be used to access the Data Governance Resource Activity database server.
- d. **Password:** Enter the password associated with the user account.

Click **Next**.

8. On the **Data Governance activity database server - Database Properties** page, click **Next** to accept the default database name for which the schema for the Data Governance Resource Activity database should be created and to accept the default database options.

The **Database name** field is pre-populated with DGE_<DeploymentName>. Where <DeploymentName> is the name assigned to the Data Governance Edition deployment on the previous wizard page. If the total length of the activity database name exceeds 30 characters, then the new default activity database name will only use <DeploymentName>.

To change the name, enter the new name to be assigned to the database. The database name is required; has a maximum length of 30 characters; and can only contain alphanumeric characters and underscores (no spaces allowed).

IMPORTANT: When installing multiple Data Governance Edition deployments in the same forest, ensure that each deployment is connecting to a database with a unique name. Do NOT connect a new deployment to an existing database.

9. Once the installation and configuration has completed, click **Next**.
10. Click **Finish** to close the Data Governance Configuration wizard.
11. If applicable, click **Finish** to close the One Identity Manager setup wizard.

Before you can gather information on the data in your environment, perform the necessary post-installation configuration tasks. For more information, see [Post installation configuration](#) on page 49.

Post installation configuration

Ensure the following post installation configuration tasks have been completed to ensure a successful Data Governance Edition deployment.

- [Move Service Principal Name in Active Directory](#)
- [Data Governance Edition components](#)
- [One Identity Manager service \(job server\) - Data Governance connector flag](#)
- [One Identity Manager - Synchronization projects](#)
- [Assign employee to UNIX account](#)
- [Assign employee to cloud account](#)
- [One Identity Manager - Database configuration](#)
- [Configuring Change Auditor to collect resource activity](#)
- [One Identity Manager Application Server](#)
- [One Identity Manager database encryption](#)

NOTE: When deploying multiple Data Governance services in a forest, be sure to perform these post installation configuration tasks for each Data Governance Edition deployment.

Move Service Principal Name in Active Directory

If you use a service account other than "LocalSystem" for the Data Governance server, you must move the Service Principal Name (SPN) in Active Directory.

NOTE: This applies if you specify a service account other than "LocalSystem" during the initial configuration or if you change the Data Governance service account after the initial configuration.

To move the SPN in Active Directory

1. Stop the Data Governance service.
2. Run the following setspn commands from a Command line prompt on a domain controller or any machine with the AD tools installed:

Run the following command to remove the SPN from the computer object:

```
setspn -D DataGovernance.Server(DEPLOYMENT)/SERVER.DOMAIN.TLD SERVERNAME
```

For example:

```
setspn -D DataGovernance.Server(DEFAULT)/MYDGESERVER.MYDOMAIN.local  
MYDGESERVER
```

Run the following command to add the SPN of the service account:

```
setspn -A DataGovernance.Server(DEPLOYMENT)/SERVER.DOMAIN.TLD USERNAME
```

For example:

```
setspn -A DataGovernance.Server(DEFAULT)/MYDGESERVER.MYDOMAIN.local  
MYUSER
```

Where:

- *DEPLOYMENT* is the deployment name assigned to the Data Governance deployment.
- *SERVER.DOMAIN.TLD* is the fully qualified domain name of the Data Governance server where the Data Governance service is installed.
- *SERVERNAME* is the short name of the Data Governance server.
- *USERNAME* is the SAM account name of the service account.

3. Restart the Data Governance service.

Data Governance Edition components

Before you can gather information on the data in your enterprise, you must set up and configure the Data Governance Edition components. Open the Manager application to configure the following Data Governance Edition components:

- Service accounts

Add and assign the credentials (service account) to ensure that you can access resources on the computers within the domain. For more information, see [Authentication using service accounts and managed domains](#) on page 59.

- Managed domains

Assign a service account to the domains that contain the computers hosting the data you want to manage. This link between a service account and an Active Directory domain makes it a "managed domain." For more information, see [Readying a service account and domains for deployment](#) on page 60.


- Managed hosts

Add managed hosts which are network objects that can host resources and can be assigned an agent to monitor security and collect resource activity. For more information, see [Working with managed hosts and agents](#) on page 62.

One Identity Manager service (job server) - Data Governance connector flag

In order to process some of the Data Governance Edition report requests and to process self-service requests for governed data from the web portal, a One Identity manager service must be running as an account that is able to access the Data Governance service (that is, either a Data Governance service account or an account mapped to an employee with the appropriate One Identity Manager application roles). The job servers that host these One Identity Manager services must be marked in the database with the "Data Governance connector" flag using the job server editor in the Designer application.

To set the connector flag in the database

1. Open the Designer.
2. In the lower pane of the navigation view, select **Base Data**.
3. In the Base Data navigation view, select **Installation | Job server**.
4. At the bottom of the right pane, select the **Server functions** tab.
5. Double-click **Data Governance connector**. The icon to the left of the name will change to a check mark.
6. Click the  **Commit to database** toolbar button.
7. Select the **Database | Compile database** menu command to display the Database Compilation wizard.

One Identity Manager - Synchronization projects

To get a complete view of your environment, you must first run the One Identity Manager Synchronization Editor to configure the synchronize between the One Identity Manager database and your target environments (Active Directory and if applicable, SharePoint, UNIX, Azure Active Directory, and SharePoint Online).

1. Run the One Identity Manager Synchronization Editor to set up a synchronization project to load Active Directory objects into the One Identity Manager database.

For more information, see *Setting up synchronization with an Active Directory environment* in the *One Identity Manager Administration Guide for Connecting to Active Directory*.

2. If applicable, once your Active Directory synchronization projects have completed, set up a synchronization project to load SharePoint objects into the One Identity Manager database.

IMPORTANT: Active Directory synchronization MUST be complete before beginning the SharePoint synchronization project.

For more information, see *Setting up synchronization with a SharePoint environment* in the *One Identity Manager Administration Guide for Connecting to SharePoint*.

3. If you are planning on using NFS managed hosts, set up a synchronization project to load UNIX objects into the One Identity Manager database.
4. If you are planning on scanning folders hosted on cloud providers, set up the following synchronization projects:

- a. Azure Active Directory to configure the synchronization between the One Identity Manager database and Azure Active Directory.

NOTE: To have One Identity Manager automatically create employees for Azure Active Directory users at synchronization time, ensure that the **TargetSystem | AzureAD | PersonAutoFullSync** configuration setting is set to SEARCH AND CREATE.

If this configuration setting is set to NO, use the Designer to change it BEFORE you run the Azure Active Directory synchronization project.

For more information on setting up a synchronization project for an Azure Active Directory tenant, see the *One Identity Manager Administration Guide for Azure Active Directory*.

- b. SharePoint Online to configure the synchronization of data between the SharePoint Online database and the One Identity Manager Service.

NOTE: Azure Active Directory synchronization MUST be complete before beginning the SharePoint Online synchronization project.

For more information, see the *One Identity Manager Administration Guide for Connecting to SharePoint Online*.

Assign employee to UNIX account

In order to assign ownership to an NFS Export resource, ensure that an Active Directory employee is assigned to the UNIX account.

To assign a One Identity Manager Employee to a UNIX account

1. In the Manager, select **Employees | Employees**.
2. Locate and select the employee, right-click and select **Tasks | Assign Unix user accounts**.
3. In the lower pane, locate and double-click the account to be assigned to the selected employee.

Assign employee to cloud account

In order to assign ownership to a cloud resource, ensure that an Active Directory employee is assigned to the SHAREPOINTONLINE or ONEDRIVEBUSINESS account.

To assign a One Identity Manager Employee to a cloud account:

1. In the Manager, select **Employees | Employees**.
2. Locate and select the employee, right-click and select **Tasks | Assign user accounts**.
3. In the lower pane, locate and double-click the account to be assigned to the selected employee.

One Identity Manager - Database configuration

The following table lists the One Identity Manager Database configuration parameters that must be set in the Designer to use various features.

NOTE: In the table, parameters marked as (Optional) may not need to be modified in order to enable email notifications. All other parameters listed must be modified with the proper information.

Table 13: One Identity Manager database configuration

If you want to:	Edit these parameters:
Receive email notifications from Data Governance Edition	Common MailNotification Common MailNotification DefaultAddress Common MailNotification DefaultCulture Common MailNotification DefaultLanguage Common MailNotification DefaultSender


If you want to:	Edit these parameters:
	Common MailNotification SMTPAccount (Optional) Common MailNotification SMTPDomain (Optional) Common MailNotification SMTPPassword (Optional) Common MailNotification SMTPRelay
Use report subscriptions and schedule reports using the web portal	Common MailNotification Common MailNotification DefaultAddress Common MailNotification DefaultCulture Common MailNotification DefaultLanguage Common MailNotification DefaultSender Common MailNotification SMTPAccount (Optional) Common MailNotification SMTPDomain (Optional) Common MailNotification SMTPPassword (Optional) Common MailNotification SMTPRelay QER RPS DefaultSenderAddress
Receive email notifications regarding attestation cases	QER Attestation DefaultSenderAddress QER Attestation MailApproval (Optional) QER Attestation MailApproval Account (Optional) QER Attestation MailApproval DeleteMode (Optional) QER Attestation MailApproval Domain (Optional) QER Attestation MailApproval ExchangeURI (Optional) QER Attestation MailApproval Inbox (Optional) QER Attestation MailApproval Password (Optional)
Receive email notifications regarding IT	QER ITShop DefaultSenderAddress

If you want to:	Edit these parameters:
Shop requests	QER ITShop MailApproval (Optional) QER ITShop MailApproval Account (Optional) QER ITShop MailApproval DeleteMode (Optional) QER ITShop MailApproval Domain (Optional) QER ITShop MailApproval ExchangeURI (Optional) QER ITShop MailApproval Inbox (Optional) QER ITShop MailApproval Password (Optional)

To edit configuration parameters

1. Open the Designer.
2. In the lower pane of the navigation view, select **Base Data**.
3. In the far right column, select **Edit configuration parameters**.
4. Click the expansion box to the left of a parameter (or double-click a parameter) to expand and display individual configuration parameters.
5. Navigate to the required configuration parameter and click the check box to the left of the entry to enable the parameter.

NOTE: Some configuration parameters will already be enabled (check box is selected) and others need to be enabled.
6. Select the required parameter to display the parameter's properties in the bottom pane. Enter the required value in the Properties tab at the bottom of the pane. Click the **Edit** button to save your settings, which will then appear in the top pane.

NOTE: The parameter must be enabled (check box is selected) and the proper value must be specified.
7. Once you have finished editing the required configuration parameters, click the  **Commit to database** toolbar button.

Configuring Change Auditor to collect resource activity

When Quest Change Auditor is installed, you can configure Data Governance Edition to collect resource activity directly from the Change Auditor database. When enabled, Change

Auditor collects the selected activity events every 15 minutes on all managed hosts. The events received from Change Auditor are harvested by the Data Governance server, aggregated and placed directly into the Data Governance Resource Activity database.

The following considerations should be taken into account to determine whether Change Auditor should be used to collect resource activity:

- At least one Data Governance agent must reside on the same machine as the Change Auditor agent in order to retrieve activity from the Change Auditor database.
- Data Governance Edition uses the Change Auditor SDK to read the existing event data. Administrators for Data Governance Edition and Change Auditor should collaborate to determine what data Change Auditor is collecting.
- The Change Auditor SDK authentication uses the same credentials as the Data Governance Edition managed domain service account. In this initial release of the feature, this is the user name and password used to connect to the Change Auditor SDK public port. There is no way of entering different Change Auditor SDK credentials at this time.

NOTE: This Change Auditor SDK account must have the "View Sdk" permission set.

You can define an application group using the **Application User Interface** page in Change Auditor to assign users to roles with the proper permissions. For more information, see the *Quest Change Auditor User Guide*.

- The Change Auditor event collection feature only collects activity for file system, SharePoint farm and NAS events.

NOTE: Change Auditor does not always contain enough information to map to Data Governance Edition resources. Therefore, the following SharePoint farm events are not included in Data Governance Edition activity reports:

- All permission levels revoked
 - Site collection ownership granted
 - Permission level created
 - Permission level permissions modified
 - Member added to security group
 - Security group created
 - Security group deleted
 - Auditing solution deployment changed.
- If Change Auditor is configured to collect activity from your EMC storage device using the Quest Shared EMC Connector, and you would like activity collection/aggregation in Data Governance Edition, you **MUST** configure Data Governance Edition to collect activity directly from Change Auditor. You will not be able to collect activity directly from your EMC device with both Change Auditor and Data Governance Edition.
 - When using Change Auditor to collect resource activity, NetApp managed hosts will not place an FPolicy for Data Governance Edition on the NetApp filer.
 - When using Change Auditor to collect resource activity, the default settings for resource activity collection and aggregation for all managed hosts will be a bit

different:


- **Collect and aggregate events** is selected by default.
NOTE: Read events are disabled by default; however, each managed host can specify the types of events to be collected.
- **Aggregation** setting is not available; Change Auditor uses the collection interval defined in the `CAAggregationIntervalMinutes` configuration parameter. Default is every 15 minutes and applies to all managed hosts.
- **Resource Activity Exclusions** is not available.
- When using Change Auditor to collect resource activity, it is not recommended to enable the **Collect activity for real-time security updates** on EMC or NetApp managed hosts. The agents managing these host types should be configured to scan on a schedule and not run once. The performance gain in using Change Auditor's event collection will be lost if the Data Governance agent is also collecting activity from these storage devices for security updates.

To use Change Auditor to collect resource activity

1. Open the Designer.
2. In the lower pane of the navigation view, select **Base Data**.
3. In the far right column, select **Edit configuration parameters**.
4. Navigate to and expand **TargetSystem | ADS | QAM**.
5. Click the check box to the left of **UseChangeAuditor**.

When enabled, Change Auditor collects events every 15 minutes on all managed hosts. To change this collection interval, modify the **CAAggregationIntervalMinutes** parameter.

TIP: If you have large amounts of real-time Change Auditor events, you may want to reduce the aggregation interval to every five minutes. Check the Data Governance service log for the Change Auditor query results to determine the number of events returned to Data Governance Edition. In this scenario, do NOT increase the aggregation interval (for example, to 24 hours), as this will cause Data Governance Edition to try and accept millions of events from Change Auditor, which could cause the Data Governance service to fail or timeout.

6. Click the  **Commit to database** toolbar button.
7. Restart the Data Governance service.

One Identity Manager Application Server

If you install the One Identity Manager Application Server under IIS, you must add an account that is able to access the Data Governance server (that is, an Active Directory user account that is mapped to a One Identity Manager employee with the **Data Governance** |

Administrators and **Data Governance | Access Managers** application roles applied) as the application pool identity.

To modify the application pool identity

1. Open Internet Information Services (IIS) Manager.
2. In the left pane, navigate to and select **Application Pools**.
3. In the middle pane, select the application pool for the application server (AppServer_POOL is the default name).
4. In the right pane, click **Advanced Settings**.
5. In the **Advanced Settings** dialog, edit the **Identity** value (under the Process Model section). This value must contain an account that is able to access the Data Governance server (i.e., an Active Directory user account mapped to an employee with both the **Data Governance | Administrators** and **Data Governance | Access Managers** application roles).

If the Application Server application pool is set to the default Network Security identity, Data Governance Edition reports will fail to generate.

One Identity Manager database encryption

If you encrypted the One Identity Manager database, you must perform the following steps to ensure Data Governance Edition can find and use the same key file.

NOTE: If the One Identity Manager database is encrypted and the encryption key file is not provided (or updated) in Data Governance Edition, you will encounter the following error when trying to add a service account to Data Governance Edition: Error: "Logon failure: unknown user name or bad password".

1. After encrypting the One Identity Manager database, locate the key file that was generated.
2. Run the following Data Governance Edition PowerShell cmdlet so Data Governance Edition can find and use this same key file:
`Set-QEncryptionOptions -File <path to .key file>`

Authentication using service accounts and managed domains

Most organizations running a network of Windows computers have multiple Active Directory domains and forests to be managed. Users expect seamless integration and IT administrators need an all-encompassing view of their network security to make that happen.

Data Governance Edition consolidates security information across many domains and forests by accessing these network entities using stored credentials (service accounts). These service accounts are Active Directory users granted the appropriate permissions in their respective domains and registered with Data Governance Edition.

By elevating to the service accounts as necessary, the Data Governance server is able to deploy agents and retrieve security information across the organization. All communication is secure and all credential information is encrypted and protected.

Administrators responsible for the Data Governance Edition deployment must register service accounts with the system and link them with domains that have been previously synchronized with One Identity Manager. The link between a service account and an Active Directory domain makes it a "Managed Domain".

Administrators link a service account to an Active Directory domain through the Manager. For more information, see [Readying a service account and domains for deployment](#) on page 60.

How are the credentials stored securely?

Service account credentials are stored in the central One Identity Manager database. These credentials can be encrypted using the Crypto-Configuration tool. For more information, see *Encrypt Data in a Database* in the *One Identity Manager Installation Guide*.

What permissions do service accounts need and why?

For details on the required permissions, see [Data Governance Edition minimum permissions](#) on page 26.

NOTES:

- Remote managed hosts (EMC, NetApp, Windows cluster, Cloud) require a service account with sufficient permissions to access target computers.
- SharePoint farms are similar to remote managed hosts in that they require a service account with sufficient permissions to access the data, even though they are installed locally.
- NetApp managed hosts require a service account with sufficient permissions to create and maintain FPolicy on a NetApp filer.

Readying a service account and domains for deployment

Before you can gather information on the data in your enterprise, you must:

- Add and assign the credentials (service account) used to access resources on the computers within the domain. For more information, see [Adding and editing a service account](#) on page 60.
- Select the domains that contain the computers and data that you want to manage. For more information, see [Adding a managed domain](#) on page 61.

You can specify these credentials on a per domain basis. Each domain can only have one associated service account at any time, but the same service account can be used for multiple domains. Service accounts are also used to run remote agent services on agent host computers and must be specified during remote agent deployment.

When a domain is managed, a Data Governance container is created in the domain's System container. This container holds a Service Connection Point object, which is used by the Data Governance Edition components to find one another. Agents use this information to determine where the Data Governance server they should connect to exists.

NOTE: Only domains that have had Active Directory synchronized with One Identity Manager can be managed. For details, see *Setting up Synchronization with an Active Directory Environment* in the *One Identity Manager Administration Guide for Connecting to Active Directory*.

Adding and editing a service account

To add a service account

1. In the Navigation view, select **Data Governance**.
2. Right-click **Service accounts** and select **New**.
3. In the **Change master data** form, select the Active Directory account, enter the

password associated with the selected account and optionally enter comments.

4. Click the **Save** toolbar button to add the service account.

To edit a service account

1. In the Navigation view, select **Data Governance | Service accounts**.
2. In the **Service Accounts** result list, double-click the required service account.
From the service account overview, you can view the domains associated with the selected service account.
3. From the Tasks view, select **Change master data**.
4. Select the Active Directory account, and enter the password and comment.
5. Click the **Save** toolbar button to save your changes.

Adding a managed domain

The rights needed to perform operations and scan computers are established by assigning a service account to the required domain.

The service account must already be created in Data Governance Edition to be assigned to a domain. For more information, see [Adding and editing a service account](#) on page 60.

To enable the Data Governance server to interact with computers in a domain

1. In the Navigation view, select **Data Governance | Service accounts**.
2. In the **Service Accounts** result list, right-click the service account, and select **Tasks | Assign domains**.
3. In the **Add assignments** pane (lower pane), double-click the required domain. You can also right-click the managed domain and select **Assign** or **Assign all objects**.
The managed domain now appears in the top pane.
4. Click the **Save** toolbar button to save your selection.

NOTE: From the **Managed hosts** view, if you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Working with managed hosts and agents

A managed host is any network object that can host resources and can be assigned an agent to monitor security and resource activity. For more information, see [Adding and configuring managed hosts](#) on page 67.

NOTE: Any objects that you want to manage through Data Governance Edition must first be added to Active Directory.

Depending on the type of managed host, you may be deploying different agents. There are two types of agents — local and remote.

Table 14: Differences between local and remote agents

Agent	Description
Local agent	<p>Local agents reside on the same computer as the managed host.</p> <p>When you deploy a local agent, it immediately scans all fixed volumes on the host computer by default. If you do not want everything scanned, you can define the paths to be scanned.</p> <p>You can only use a single agent on a local managed host; however local agents provide the best performance and the most functionality.</p>
Remote agent	<p>Remote agents reside on a remote computer other than the managed host, and require a service account with adequate credentials to read the security information.</p> <p>Remote agents scan only the configured managed paths on a defined schedule, in order to maximize performance. The default security scanning schedule is daily at 2:00 A.M.</p> <p>You can use remote agents on Windows computers, and you must use them on Windows clusters, NetApp devices (with CIFS or NFS file system protocols enabled), EMC devices (with CIFS or NFS file system protocols enabled), Generic host types, and Cloud host types.</p> <p>Remote agents cannot collect resource activity on remotely managed Windows, Windows clusters, Generic, or Cloud host types.</p>

NOTE: SharePoint farm agents are remotely managed and require a service account for the agents. They must be installed on a SharePoint server. Ensure that the service account configured for the SharePoint managed host is a SharePoint Farm Account (same account that is used to run the SharePoint timer service).

NOTE: A DFS root managed host does not have an agent installed. Once a root is added as a managed host, the Data Governance server periodically synchronizes the DFS structure into the One Identity Manager database making the DFS path available within the Resource browser. You are able to quickly see where all the data has been replicated throughout your network.

You must have enough free space on the agent computer in the installation directory to store the data collected by the agent. Contact Software Support for details on estimating the disk space usage.

To optimize searches for access points, agents send security index information for resources under managed paths to the Data Governance server for storage in the One Identity Manager database. This allows clients to quickly determine the hosts where detailed access queries are to be directed.

NOTE: All detailed security information for resources placed under governance is sent to the Data Governance server and stored in the One Identity Manager database.

Detailed access information is maintained on the agent computer, only sending general access information to the server.

The server acts as an intermediary between the agents and the databases where information is stored. It coordinates all agent deployments and communication, and manages the security index for each managed host. Only indexing direct-access points is done for several reasons:

- Security information that is not explicit is, by definition, inherited from a resource higher in the hierarchy. Unless the resource is the managed path, the agent has already indexed the explicit security on the parent resource that is causing the inherited security to be present.
- Not including inherited access points greatly reduces the total size of the index.
- Resources with only inherited access are not interesting from a security standpoint. Data Governance Edition is interested in the resources that have had security applied directly to them.

Deployment best practices

When deploying Data Governance agents, local agents are preferable to remote agents. Local agents reduce network bandwidth and increase responsiveness. When it is not possible to deploy local agents to a system (such as when using a network attached storage device, or a virtual cluster node), the following best practices should be considered:

- When deploying multiple remote agents to an agent host computer, the number of agents a host computer can handle is limited by several factors:
 - The total number of resources being scanned by all hosted agents.
 - The total number of resources with explicit security being indexed by all hosted agents.
 - All the queries that are serviced by agents hosted concurrently are executed on that local hardware.
- Overwhelming the host computer with too many agents can result in slow indexing performance and intermittent failures in agent queries or in indexing operations.
- When deploying remote agents, ensure that the agents are hosted on computers that have low latency, high-bandwidth connections to their targets. This ensures that agents that have real-time change watching enabled will not suffer from periodic watch failures.
- When possible, avoid deploying agents to the computer hosting the Data Governance service itself. The server requires significant network resources to perform its various operations. When agents are deployed to this system, they compete for these network resources. Leaving the server with as few agents as possible ensures that it will not suffer performance degradation due to resource scarcity.
- More than one remote agent may be used to scan remote Windows computers, Windows clusters, and NAS devices. This is useful if the managed host has a large set of managed paths. Multiple agents may not scan the same managed paths.
- Manually installing agents is not supported. You must use the Manager client to deploy and configure Data Governance agents because you need access to the Data Governance application roles within One Identity Manager.
- When adding a remote agent, ensure that a trust exists between:
 - the domains of the agent host and the agent service account
 - the domains of the agent service account and the computer being scanned
- When deploying multiple agents to manage a SharePoint farm, One Identity recommends that you manage the lowest resources in the SharePoint hierarchy that you plan on governing or reporting on. Also, divide these managed resources across as many agent services as your SharePoint server can handle. This will provide the fastest scanning and the least amount of downtime when running reports.

Once you have added a managed host, you can begin to manage the data contained within it.

Agent leases

Data Governance Edition includes a mechanism that enables the server to determine what agents are functioning without needing each agent to maintain a persistent connection to the Data Governance server.

Every few minutes the agent contacts the server to renew its lease. If the server has not received a lease renewal from an agent in the expected time frame, the agent goes into the "No communication from agent" state. This state indicates that the server is unable to receive information from the agent.

If an agent is in this state, you can attempt to restart the agent. For more information, see [Restarting agents](#) on page 123. It is important to understand why the agent allowed its lease to expire. Leases may expire because the agent service stopped unexpectedly or the agent host computer lost its network connection so the agent could not contact the server to renew its lease.

NOTE: You can also review lease expiration information in the Data Governance server log (DataGovernanceEdition.Service.exe.dlog) in the Data Governance service installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\).

For a complete list of possible agent states, see [Verifying managed host system status](#) on page 117 or [Checking the agent status](#) on page 120.

Agent deployment pre-flight check

Prior to deploying Data Governance agents:

- Ensure agents meet minimum hardware and software requirements. For more information, see [Data Governance Edition system requirements](#) on page 15.
- Ensure appropriate ports are opened on the agent. For more information, see [Data Governance Edition required ports](#) on page 30.
- Ensure disk space is sufficient on the drive hosting the agent files.
- Ensure service account can access admin\$ share on the agent.
- Identify other programs that may impact agent security scanning and security update monitoring.
- Identify target paths. Refrain from scanning entire file system immediately.
- Identify peak hours for schedule purposes.
- Ensure agent can query domain naming context on a domain controller.
- Ensure agent can connect to `http://<server>:8721/Broadway/IndexServerAgentPort`.
- Ensure the trusted root certificates on the agent are up to date.

NOTE: The agent requires VeriSign Class 3 Public Primary Certification Authority - G5.cer.

Agent deployment methods

This table lists the methods that can be used to deploy Data Governance agents.

NOTE: As of Data Governance Edition version 7.0.2, manually deploying agents is NOT allowed. You must use the Manager client to deploy and configure Data Governance agents because you need access to the Data Governance application roles within One Identity Manager.

Table 15: Agent deployment methods

Deployment method	Description	Notes/Where to find additional information
Manager - single agent deployment	<p>The recommended method for adding a managed host.</p> <ol style="list-style-type: none"> 1. Select the host computer from the Managed host view (must have already been synchronized into One Identity Manager). 2. Select the Manage host task. 3. In the Managed Host Setting dialog, select the managed host configuration settings. <p>Use the Managed DFS host task to add a Distributed File System (DFS) root managed host.</p> <p>Use the Manage NFS host task to add an NFS managed host for scanning supported NAS devices with NFS file system protocol enabled.</p> <p>Use the Manage Cloud host task to add a SharePoint Online or OneDrive for Business managed host.</p>	<p>For more information on determining the type of agent to be deployed, see Working with managed hosts and agents.</p> <p>For more information on deploying the different types of managed hosts, see Adding and configuring managed hosts.</p> <p>For more information about the configuration settings available, see Managed host configuration settings.</p>
Manager - multiple agent deployment	<p>Use to add and configure multiple managed hosts at once.</p> <ol style="list-style-type: none"> 1. Select multiple host computers of the same host type from the Managed host view. 2. Select the Manage multiple hosts task. 3. Set the appropriate managed host configuration settings that will be applied to all selected hosts. 	<p>Not available for adding SharePoint managed hosts.</p> <p>Does not apply to DFS, NFS, or Cloud host types (you do not select host computers when adding these types of managed hosts).</p> <p>The server deploys the agents in a staggered manner.</p> <p>All hosts must be in managed domains.</p> <p>For more information on adding or configuring managed hosts, see Adding</p>

Deployment method	Description	Notes/Where to find additional information
Windows PowerShell	<p>Use the following PowerShell cmdlets in the OneIdentity.DataGovernance snap-in to deploy and configure managed hosts:</p> <ul style="list-style-type: none"> • Add-QManagedHostByAccountName: To add a managed host to your deployment and configure its settings. • Set-QManagedHostProperties: To change the properties of a managed host. • Set-QAgentConfiguration: To set the managed paths to be scanned. 	<p>and configuring managed hosts.</p> <p>These PowerShell cmdlets do not support adding Cloud managed hosts or setting managed paths for Cloud managed hosts.</p> <p>For more detailed information on using Windows PowerShell to manage your agent deployment, see the <i>One Identity Manager Data Governance Edition Technical Insight Guide</i>.</p>

Adding and configuring managed hosts

Different types of managed hosts behave differently. The following sections provide the steps to configure each type of managed host.

You can add the following host computers as a managed host to your Data Governance Edition deployment:

- Local Windows computer. For more information, see [Adding a local managed host \(Windows computer\)](#) on page 68.
- Windows Cluster/Remote Windows computer. For more information, see [Adding a Windows cluster / Windows computer as a remote managed host](#) on page 71.
- Generic resource (that is, a Server Message Block (SMB) share running on any Active Directory joined computer). For more information, see [Adding a generic managed host](#) on page 73.
- Distributed File System (DFS) root. For more information, see [Adding a Distributed File System \(DFS\) root managed host](#) on page 77.
- SharePoint farm. For more information, see [Adding a SharePoint farm managed host](#) on page 78.
- EMC storage device with CIFS file system protocol enabled. For more information, see [Adding an EMC CIFS device as a managed host](#) on page 86.
- NetApp 7-Mode filer with CIFS file system protocol enabled. For more information, see [Adding a NetApp CIFS device as a managed host](#) on page 82.

- NetApp Cluster-Mode filer with CIFS file system protocol enabled. For more information, see [Adding a NetApp CIFS device as a managed host](#) on page 82.
- EMC Isilon storage device with NFS system protocol enabled. For more information, see [Adding an NFS managed host](#) on page 89.
- NetApp 7-Mode filer with NFS file system protocol enabled. For more information, see [Adding an NFS managed host](#) on page 89.
- NetApp Cluster-Mode filer with NFS file system protocol enabled. For more information, see [Adding an NFS managed host](#) on page 89.
- SharePoint Online resources. For more information, see [Adding a cloud managed host](#) on page 93.
- OneDrive for Business resources. For more information, see [Adding a cloud managed host](#) on page 93.

Adding a local managed host (Windows computer)

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a local managed host to a Windows computer

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **Windows Computer**.
3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This is a read-only field displaying the name of the host computer selected on the **Managed hosts** view.
 - b. **Host Type:** Select **Local Windows Computer**.

- c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

- d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.
5. By default, local agents scan all local fixed volumes (NTFS devices) on the host computer. To limit the amount of security data being scanned, use the **Managed Paths** page to specify the root of an NTFS directory to be scanned. Once you configure one or more managed paths, only those paths are scanned.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, select the check box to the left of the directories to be scanned.

NOTE: For local managed hosts, the **Agent Selection** field at the bottom of this dialog is pre-populated with the name of the selected target machine.

- d. Click **OK**.

For more information, see [Managed paths page](#) on page 106.

6. By default, local agents begin scanning immediately once deployed. Use the **Security Scanning** page to define a different scanning schedule for the agent.

For example, to delay the scan to run during off peak hours:

- a. Open the **Security Scanning** page.
- b. Clear the **Immediately scan on agent restart or when managed paths change** check box.
- c. Use the **Scan start time** control to specify the desired time to perform the full scan.

NOTE: The **Scan start time** is local agent time.

Review the options at the bottom of the page to determine if the default security scanning behavior needs to be modified:

- **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.
- **Collect activity for real-time security updates:** Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

For more information, see [Security Scanning page](#) on page 107.

7. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

- a. Open the **Resource Activity** page.
- b. Select the **Collect and aggregate events** option.
- c. Select the type of events to be collected:
 - Security change
 - Create
 - Delete
 - Rename
 - Write
 - Read (disabled by default)
- d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
 - 5 minutes
 - 1 hour
 - 8 hours (default)
 - 1 day
- e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

NOTE: By default, the Data Governance agent excludes the run as account (LOCAL SYSTEM) from activity collection and aggregation.

For more information, see [Resource activity page](#) on page 110.

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy a Data Governance Edition agent on the local computer.

By default, the security scan begins immediately upon agent deployment. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a Windows cluster / Windows computer as a remote managed host

You can add Windows servers and Windows clusters as managed hosts, with remote agents. However, you cannot collect resource activity for these types of remote managed hosts.

NOTE: Only Windows failover cluster configurations are supported.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a Windows cluster or Windows computer managed host with a remote agent

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **Windows Computer**.
3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This is a read-only field displaying the name of the host computer selected on the **Managed hosts** view.
 - b. **Host Type:** Select **Windows Cluster / Remote Windows Computer**.
 - c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
 - d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target computer.
- c. **Select the service account:** Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click the **Add** button to add the agent to the agents list.

TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

For more information, see [Agents page](#) on page 105.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** tab to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the check boxes at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.
 - **Collect activity for real-time security updates:** Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

For more information, see [Security Scanning page](#) on page 107.

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a generic managed host

You can remotely scan managed hosts (other than those on the supported list) by adding a “generic” managed host. This type of managed host supports scheduled scans only and does not support real-time security updates or resource activity collection.

NOTE: These hosts must be accessible through Windows shares. To determine if a host can be scanned for security information, you can use the Filesystem Statistics Utility (QAM.Server.FileSystemStatistics.exe) that is included with a Data Governance Edition installation. It scans a file system, enumerates its contents, and provides statistics on the files and folders contained on the specified data roots.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a generic managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.

NOTE: If you do not see the host you want to manage listed, edit the Data Governance service configuration file (DataGovernanceEdition.Service.exe.config)

as follows:

- Locate the customHostParameters section.

```
<customHostParameters>
  <additionalOperatingSystems>
    <!--<operatingSystem value="MyOperatingSystem"/>-->
  </additionalOperatingSystems>
</customHostParameters>
```

- Remove the commented operatingSystem line and replace it with a line that specifies the operating system value for the host you want to manage. That is, the string found in the ADSMachine.OperatingSystem field. For example, if the host you want to manage has the operating system field "MyOS", edit this setting as follows:

```
<customHostParameters>
  <additionalOperatingSystems>
    <operatingSystem value="MyOS"/>
  </additionalOperatingSystems>
</customHostParameters>
```

This will include all machines that contain the string "MyOS" in its operating system field.

- If you want to specify an exact match, include the isExact parameter as follows:

```
<customHostParameters>
  <additionalOperatingSystems>
    <operatingSystem value="MyOS" isExact="true"/>
  </additionalOperatingSystems>
</customHostParameters>
```

All of the hosts found using this filter will now appear in the Managed Host view as **Unknown** host type.

2. In the Managed hosts view (right pane), select a host with the status of **Not Managed** and a host type of **Unknown**.
3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set**

button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:

- a. **Managed Host:** This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.
- b. **Host Type:** Select **Generic Host Type**.
- c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example C:\Mypath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance Server installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

If there is an existing agent, you cannot install another agent with a different installation directory. All agents must be installed in the same directory.

- d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target computer.
- c. **Select the service account:** Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click the **Add** button to add the agent to the agents list.

TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

For more information, see [Agents page](#) on page 105.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths, including those that are excluded, appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the check boxes at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.

For more information, see [Security Scanning page](#) on page 107.

8. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a Distributed File System (DFS) root managed host

Adding a DFS root enables you to view and manage the access on resources that are physically distributed throughout your network.

TIP: As of Data Governance Edition version 7.0.1, you can perform additional managed host tasks against DFS links, such as:

- Target existing reports, including the Resource Access and Resource Activity reports
- Calculate perceived owners
- Place a DFS link under governance; adding the DFS link to the **Governed data** view and making the usual menu options available
- Publish a DFS link to the IT Shop; making it available to others through a resource access request

Once added, the Data Governance server periodically synchronizes the DFS structure into the One Identity Manager database making the DFS path available within the **Resource browser**. You are able to quickly see where all the data has been replicated throughout your network.

This information is also available within the resource access, resource activity, and account activity reports if the underlying resource is being scanned on another activity enabled host.

NOTE: In order for a DFS link, target share path or folder to be placed under governance or published to the IT Shop, both the DFS server hosting the DFS namespace and the share server where the DFS link is pointing to must be added as managed hosts. If the required servers (those that contain DFS security details) are not already managed, a message box appears listing the servers that need to be added as managed hosts. Click the **Add managed hosts with default options** button to deploy a local agent to the servers listed in the message box and complete the selected operation. Click **Cancel** to cancel the selected operation and manually add the servers as managed hosts.

NOTE: By default, the Data Governance server synchronizes DFS every 24 hours, you can force an immediate synchronization using Windows PowerShell or you can alter the synchronization interval through a configuration file setting.

To force an immediate DFS synchronization, run the following PowerShell cmdlet:

```
Trigger-QDfsSync [-ManagedHostID] <String> [<CommonParameters>]
```

You must specify the ID (GUID format) of the DFS managed host to be synchronized. To synchronize all of your DFS managed hosts, set the -ManagedHostId to All.

To change the default synchronization interval, add or modify the following setting in DataGovernanceEdition.Service.exe.config file (which is located in the Data Governance server installation directory):

```
<add key="DFSDataSyncInterval" value="1440"/>
```

The value specified is interpreted as minutes. If this value is not present, the default is 24 hours.

To add a DFS root managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. From the **Managed hosts** view (right pane), select **Manage DFS host** from the Tasks view or right-click menu.
3. In the **DFS Managed Host Settings** dialog, select the following information:
 - **DFS Domain:** Select the DFS domain.
 - **DFS Root:** Click the **Select Root** button to display a list of available DFS roots within the selected domain. Select a root from the list and click **OK**.Click **OK** to save your selections and close the dialog.
4. Back in the Manager, click the **Save** toolbar button to add the DFS root managed host.

Adding a SharePoint farm managed host

SharePoint farms are similar to remote managed hosts in that they require an associated service account, even though they are installed locally on a SharePoint server. You have the option of selectively including and excluding objects to be scanned by one or more agent services on the SharePoint server.

NOTE: Before adding a SharePoint managed host, ensure that the following configuration steps have been completed:

- Install a One Identity Manager service (job server) on a dedicated SharePoint Application Server in the SharePoint farms to be monitored. Ensure that the One Identity Manager service account is running as the SharePoint farm account (same account that is used to run the SharePoint timer service).

- On the Data Governance server, run the One Identity Manager Synchronization Editor to set up a synchronization project to load your Active Directory objects into the One Identity Manager database. For more information, see the *One Identity Manager Administration Guide for Connecting to Active Directory*.
- On the SharePoint farm server, run the One Identity Manager Synchronization Editor to set up a synchronization project to load your SharePoint objects into the One Identity Manager database. For more information, see the *One Identity Manager Administration Guide for Connecting to SharePoint*.
- Also, check/configure the master data (task in Manager) for the service account.

Once the SharePoint synchronization project has completed, the **Managed hosts** view is updated to include any SharePoint farms that are available for scanning.

To add a SharePoint farm as a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **SharePoint Farm**.
3. Select **Manage host** from the Tasks view or right-click menu.
The **Managed Host Settings** dialog appears.
4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.
 - b. **Host Type:** This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.
 - c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.
NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
 - d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.
5. Use the **Agents** page to select the service account to be used to access the SharePoint farm and the agent services to be used to scan the SharePoint farm.

To add an agent service:

- a. Open the **Agents** page.
- b. **Agent Service Account:** Select the service account that has the required rights for the selected SharePoint farm.

The service account must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One Identity Manager

service (job server)). The SharePoint farm account also needs to be added to the local Administrators group on the SharePoint server.

- c. Click the **Add** button to add the agent service to the agents list.

Repeat to add additional agent services to be used to scan the selected SharePoint farm.

For more information, see [Agents page](#) on page 105.

6. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.
7. Back on the **Managed hosts** view, select the newly deployed SharePoint managed host, and select the **Edit host settings** task or right-click command.

The **Managed Host Settings** dialog appears allowing you to configure the additional settings required for a SharePoint managed host.

8. Use the **Managed Paths** page to specify the point within your SharePoint farm hierarchy to begin scanning.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of the component within your SharePoint farm hierarchy to be scanned.

NOTE: When using multiple agent services to monitor a SharePoint managed host, select the managed path to be monitored and then select an agent service from the **Agent Selection** drop-down menu. Repeat this process for all of the paths to be monitored. An agent service can monitor multiple paths; however, multiple agent services cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the name of the agent service selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths and assigned agent service are displayed on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

9. By default, SharePoint agents scan daily at 2:00 A.M. Use the **Security Scanning** page to set the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the options at the bottom of the page to modify the default security scanning behavior:

- **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
- **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.

For more information, see [Security Scanning page](#) on page 107.

10. By default resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection and aggregation.

NOTE: To gather and report on resource activity in SharePoint, ensure that SharePoint native auditing is configured for any resources of interest. For more information, see [Configure SharePoint to track resource activity](#) on page 166.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

- a. Open the **Resource Activity** page.
- b. Select the **Collect and aggregate events** option.
- c. Select the type of events to be collected:
 - Security change
 - Create
 - Delete
 - Rename
 - Write
 - Read (disabled by default)
- d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
 - 5 minutes
 - 1 hour
 - 8 hours (default)
 - 1 day
- e. By default, certain well-known accounts are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts to be excluded.

NOTE: The agent service account is not included in this exclusion list by default. You will need to add that manually for SharePoint managed hosts.

For more information, see [Resource activity page](#) on page 110.

11. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the SharePoint resources on the target managed host using the **Resource browser**. Double-click the managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a NetApp CIFS device as a managed host

You can add supported NetApp storage devices as managed hosts, with remote agents. This procedure covers NetApp 7-Mode devices and NetApp Cluster-Mode devices running OnTap with the CIFS file system protocol enabled. See [NetApp managed host deployment](#) before adding a NetApp managed host.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add a NetApp CIFS device as a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **NetApp OnTap 7 Mode CIFS Device** or **NetApp OnTap Cluster Mode CIFS Device**.
3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.
 - b. **Host Type:** This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.

- c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
 - d. **Keyword:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.
5. For NetApp OnTap Cluster Mode CIFS managed hosts, use the **Credentials** page to enter the credentials of a user with access to the target NAS host computer:
- a. **User Name:** Enter the name of a user account with access to the target NAS host computer.

NOTE: The user must have the "ontapi" User Login Method application.
 - b. **Password:** Enter the password associated with the user account entered above.
 - c. **Port:** Enter the destination port to be used for communication between the agent and target NAS host computer. The default value is 443.
 - d. **Host EndPoint:** (Optional) Enter the API endpoint (FQDN, host name or IP address) for the NetApp Cluster Mode connection.

NOTE: The default is to use the FQDN of the targeted host. You would only use this setting if the API connection needs to be specified as something other than the FQDN of the targeted host.
 - e. Click the **Test API Credentials** button to verify valid credentials have been entered.
6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target computer.
- c. **Select the service account:** Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click the **Add** button to add the agent to the agents list.

TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

For more information, see [Agents page](#) on page 105.

7. Use the **Managed Paths** page to specify the roots of the NTFS directory tree to be scanned by the agent.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

8. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the options at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.
 - **Collect activity for real-time security updates:** Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

For more information, see [Security Scanning page](#) on page 107.

9. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

- a. Open the **Resource Activity** page.
- b. Select the **Collect and aggregate events** option.
- c. Select the type of events to be collected:
 - Security change
 - Create
 - Delete
 - Rename
 - Write
 - Read (disabled by default)
- d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
 - 5 minutes
 - 1 hour
 - 8 hours (default)
 - 1 day
- e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

NOTE: By default, the Data Governance agent excludes the domain service account from activity collection and aggregation.

For more information, see [Resource activity page](#) on page 110.

10. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding an EMC CIFS device as a managed host

You can add EMC storage devices as managed hosts, with remote agents. This procedure covers NAS devices running EMC Celerra/VNX or EMC Isilon operating systems with the CIFS file system protocol enabled. See [EMC managed host deployment](#) before adding an EMC managed host.

NOTE: You can configure one target host computer at a time or multiple host computers (of the same type) at once.

To add an EMC CIFS device as a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select a host with the status of **Not Managed** and a host type of **EMC Celerra/VNX Device** or **EMC Isilon Device**.
3. Select **Manage host** from the Tasks view or right-click menu.

NOTE: If you selected multiple host computers with the status of **Not Managed** and of the same host type, use the **Manage multiple hosts** task or right-click menu command. The settings specified on the **Managed Host Settings** dialog will apply to all selected host computers.

The **Managed Host Settings** dialog appears.

NOTE: If you select a host computer on a domain that was not previously identified as a managed domain, the **Domain Credentials** dialog appears. Click the **Set** button to supply the credentials of an Active Directory user with administrative rights on the selected domain. Assigning the credentials for the domain registers the user as a Data Governance Edition service account, links the service account to the domain and adds it to the managed domains list.

Once the domain credentials are set, the **Managed Host Settings** dialog appears.

4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This is a read-only field displaying the name of the host computer selected in the **Managed hosts** view.
 - b. **Host Type:** This is a read-only field displaying the type of host computer selected in the **Managed hosts** view.
 - c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
 - d. **Keyword:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

5. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target computer.
- c. **Select the service account:** Select a service account with sufficient permissions to access the target computer and the agent host.

An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click the **Add** button to add the agent to the agents list.

TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

NOTE: If you are collecting resource activity (**Collect and aggregate events** on the **Resource Activity** page) or real-time security updates (**Collect activity for real-time security updates** on the **Security Scanning** page), you can only specify one agent to scan the EMC storage device.

For more information, see [Agents page](#) on page 105.

6. Use the **Managed Paths** page to specify the roots of the NTFS directory trees to be scanned by the agent.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of a directory to add it to the managed paths list.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

7. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** page to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the options at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.
 - **Collect activity for real-time security updates:** Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

NOTE: If you enable **Collect activity for real-time security updates**, ensure your EMC device is configured for auditing. For more information, see [EMC managed host deployment](#) on page 162.

For more information, see [Security Scanning page](#) on page 107.

8. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

To configure resource activity collection and aggregation:

- a. Open the **Resource Activity** page.
- b. Select the **Collect and aggregate events** option.
- c. Select the type of events to be collected:
 - Security change
 - Create
 - Delete
 - Rename
 - Write
 - Read (disabled by default)

- d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
 - 5 minutes
 - 1 hour
 - 8 hours (default)
 - 1 day
- e. By default, certain well-known system accounts, file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the accounts and objects to be excluded.

NOTE: By default, the Data Governance agent excludes the domain service account from activity collection and aggregation.

Click the **View/Update cepp.conf** button to check the status or modify the cepp.conf file. Selecting this button displays a **Logon Credentials** dialog allowing you to enter the IP address or hostname and credentials of the EMC Celerra/VNX control station and select the data mover that holds the managed paths to be scanned.

- Once the cepp.conf is retrieved and displayed, you can edit the Proposed cepp.conf file (lower pane). Select the **Update File** button to save your edits, which will be sent to the EMC device.

NOTE: The cepp service will be stopped and restarted for the selected data mover to apply the new cepp.conf file.

- Use the **Check Status** button to check the status of the current cepp.conf file.

For more information, see [Resource activity page](#) on page 110.

9. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding an NFS managed host

Data Governance Edition supports the scanning of NAS devices with NFS file system protocol enabled, including NetApp 7-Mode, NetApp Cluster and EMC Isilon devices.

NOTE: Before adding an NFS managed host, ensure the following configuration steps have been completed:

- During the One Identity Manager installation process and Data Governance configuration process, add the optional Unix module.
- During the One Identity Manager Data Governance Edition installation process, ensure the One Identity Manager service (job server) is configured properly and that the UNIX connector server function is selected.
- Run the One Identity Manager Synchronization Editor to set up a synchronization project to load your UNIX objects into the One Identity Manager database.

For EMC Isilon NFS managed hosts:

- On the Data Governance server and all agent servers, you must have a Trusted Root Certificate Authority certificate to validate the Isilon server's HTTP certificate. See the EMC Isilon Web Administration Guide for details.
- The service account for an agent managing EMC Isilon storage devices, must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).

For NetApp 7-Mode NFS managed hosts (does NOT apply to Cluster Mode devices):

- The service account for an agent managing NetApp 7-Mode filers must be a member of the local Administrators group on the NetApp filer in order to create FPolicy. This account must also have permissions to access folders being scanned.
- Monitoring real-time security updates and collecting resource activity requires FPolicy; and in order to use FPolicy, the CIFS file system protocol must be enabled for NetApp 7-Mode devices.

Adding a NFS managed host

1. In the **Navigation** view, select **Data Governance | Managed hosts**.
2. From the **Managed hosts** view, select **Manage NFS host** from the Tasks view or right-click menu.

The **Managed Host Settings** dialog appears.

3. At the top of the dialog, specify the following information:
 - a. **Managed Host:** Enter the IP address or the fully qualified domain name of the NFS host computer to be managed.
 - b. **Host Type:** Select **NetApp Cluster NFS Device**, **NetApp 7-Mode NFS Device**, or **EMC Isilon NFS Device**.
 - c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).
 - d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.

4. Open the **NIS Host** page to specify the NIS server whose users and groups have been synchronized with One Identity Manager.
5. Open the **Credentials** page and enter the credentials of a user with access to the target NAS host computer:
 - a. **User Name:** Enter the name of a user account with access to the target NAS host computer.
 - b. **Password:** Enter the password associated with the user account entered above.
 - c. **Port:** Enter the destination port to be used for communication between the agent and target NAS host computer.
 - NetApp filers: The default value is 443.
 - EMC devices: The default value is 8080.

Click the **Test API Credentials** button to verify valid credentials have been entered.

For more information, see [Credentials page](#) on page 103.

6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target computer.
- c. **Select the service account:** Select a service account with sufficient permissions on the selected agent host.

Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click **Add** to add the agent to the agents list.

TIP: For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the **Edit host settings** task after the managed host is deployed.

For more information, see [Agents page](#) on page 105.

7. Use the **Managed Paths** page to specify the directories to be scanned by the agent to create and maintain the security index.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, select the check box to the left of the directories to be scanned.

NOTE: When using multiple agents to monitor a remote managed host, select the managed path to be monitored and then select an agent from the **Agent Selection** drop-down menu. Repeat this process for all paths to be monitored. An agent can monitor multiple paths; however, multiple agents cannot monitor the same managed paths. The **Scanning Agent** field in the Managed Paths Selection grid displays the agent selected to scan the different paths.

- d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

8. By default, remote agents scan daily at 2:00 A.M. Use the **Security Scanning** tab to change the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Review the options at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Collect activity for real-time security updates:** Select this check box to watch for changes to the structure and security of the file system on the target managed host and apply them to the scanned data.

NOTE: Collecting real-time security updates is not available for EMC Isilon NFS devices.

NOTE: For NetApp 7-Mode managed hosts, real-time security updates and resource activity collection requires FPolicy. In order to use FPolicy, CIFS file system protocol must be enabled.

For more information, see [Security Scanning page](#) on page 107.

9. By default, resource activity is not collected. Use the **Resource Activity** page to enable and configure resource activity collection on the target host.

IMPORTANT: Collecting resource activity on your managed hosts impacts network usage and increases the load on the database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation window is important to limit some of this load. Carefully plan out which resources you want to collect activity on and enable resource activity collection only on those resources.

NOTE: Collecting resource activity is not available for EMC Isilon NFS devices.

To enable and configure resource activity collection and aggregation:

- a. Open the **Resource Activity** page.
- b. Select the **Collect and aggregate events** option.
- c. Select the type of events to be collected:
 - Security change
 - Create
 - Delete
 - Rename
 - Write
 - Read (disabled by default)
- d. Use the **Aggregation** control to set the time frame to be used to consolidate similar events. Valid aggregation intervals are:
 - 5 minutes
 - 1 hour
 - 8 hours (default)
 - 1 day
- e. By default, certain file extensions and folders are excluded from the resource activity collection. To modify the exclusion list, click the **Resource Activity Exclusions** button to specify the objects to be excluded.

For more information, see [Resource activity page](#) on page 110.

10. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections and deploy the managed host.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the folders and shares on the target managed host using the **Resource browser**. Double-click a managed host in the **Managed hosts** view to display the **Resource browser**.

Adding a cloud managed host

Data Governance Edition supports the scanning of folders hosted on SharePoint Online and OneDrive for Business.

NOTE: Before adding a cloud managed host, One Identity Manager must be configured to use Azure Active Directory and SharePoint Online. See the following One Identity Manager documents for instructions on configuring and synchronizing the data from these target systems with the One Identity Manager Service:

- *One Identity Manager Administration Guide for Connecting to Azure Active Directory*
- *One Identity Manager Administration Guide for Connecting to SharePoint Online*

These One Identity Manager documents can be found on the One Identity support site:
<https://support.oneidentity.com/identity-manager/technical-documents>

To add a cloud managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view, select **Manage Cloud host** from the Tasks view or right-click menu.

You are redirected to Microsoft to sign in to your account and grant access to Office 365 data.

3. On Microsoft's **Sign in to your account** dialog, enter the administrator account login credentials to be used to authenticate with the Data Governance Edition API cloud proxy.

NOTE: Data Governance Edition only supports one Office 365 domain per cloud provider at this time. That is, you can deploy only one managed host for the SharePoint Online administrator account and one managed host for the OneDrive for Business administrator account. Data Governance Edition does not currently block you from deploying a second SharePoint Online or OneDrive for Business managed host; however, it will not work.

NOTE: You must use a separate administrator account for this purpose. This administrator account must be, or have equal access as, a SharePoint Online Administrator. Each site will be modified to list this account as a Site Collection Administrator for the site. This provides the account with access to the site's contents.

- a. **Email, phone, or Skype:** Enter the email address of the administrator account to be used to grant access to your Office 365 domain. For example: Administrator@MyDomain.onmicrosoft.com.

Click **Next**.

- b. **Password:** Enter the password associated with the specified email.

Click **Sign In**.

After successfully signing in, the **Managed Host Settings** dialog appears allowing you to configure your cloud managed host.

4. At the top of the **Managed Host Settings** dialog, specify the following information:
 - a. **Managed Host:** This field will remain blank.
 - b. **Host Type:** Select the type of cloud provider: **SharePoint Online** or **OneDrive for Business**.
 - c. **Agent Install Path:** (Optional) Use this field to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.

NOTE: By default, this field displays **Use default install directory** and the agent is installed in the Data Governance agent services installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).

- d. **Keywords:** (Optional) Enter a keyword which can be displayed and used to group managed hosts in the **Managed hosts** view.
5. The **Cloud Provider** page displays a green check mark and message indicating you are authenticated with your Office 365 domain. If you do not see this green check mark and authentication message, use the **Re-authenticate** button to authenticate with the cloud API proxy.
6. Use the **Agents** page to select the remote agent and service account to be used to scan the target host.

NOTE: You can only specify one agent to scan a cloud host.

To add a remote agent:

- a. Open the **Agents** page.
- b. **Select the agent:** Select the agent host computer to be used to scan the target managed host.
- c. **Select the service account:** Select a service account with sufficient permissions on the selected agent host.

Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see [Readying a service account and domains for deployment](#) on page 60.

- d. Click **Add** to add the agent to the agents list.

For more information, see [Agents page](#) on page 105.

7. Use the **Managed Paths** page to specify the folders under the Documents site to be scanned by the agent to create and maintain the security index.

NOTE: OneDrive for Business support is limited to the Documents folder for the Administrator account. Therefore, all managed paths are selected within the scope of the Administrator's Documents folder.

For SharePoint Online, a site is available for managing, only if it can be navigated on the SharePoint Online website.

To add managed paths:

- a. Open the **Managed Paths** page.
- b. Click the **Add** button.
- c. In the **Managed Paths Picker** dialog, click the check box to the left of the folders to be scanned.

TIP: A check box appears to the left of the folders that can be selected. Click the expansion box to the left of a container to expand it and navigate to the folders available for scanning.

- d. Click **OK** to save your selections and close the dialog.

The selected paths appear on the **Managed Paths** page.

For more information, see [Managed paths page](#) on page 106.

8. By default, remote agents scan cloud-based managed hosts daily at 2:00 A.M. Use the **Security Scanning** page to set the time and frequency with which the agent scans the target computer.

To modify the scanning schedule and settings:

- a. Open the **Security Scanning** page.
- b. Use the controls in the **Scanning Schedule** pane to define the time and frequency of the agent scans.
- c. Use the options at the bottom of the page to modify the default security scanning behavior:
 - **Immediately scan on agent restart or when managed paths change:** Select this check box to perform a full scan whenever the agent restarts or there are changes made to the managed paths.
 - **Ignore all files and only store folder security data:** Clear this check box if you want to include file security data in the security index.

For more information, see [Security Scanning page](#) on page 107.

9. Click the **OK** button at the bottom of the **Managed Host Settings** dialog to save your selections.

Scanning of the specified managed paths begins on the configured schedule. Once the managed host is successfully added (Status is **Managed**), you are able to see and manage security information for the resources on the target managed host using the **Resource browser**. Double-click the managed host in the **Managed hosts** view to display the **Resource browser**.

Managed host configuration settings

Managed hosts must be properly configured for security scanning (and resource activity collection, if applicable) to begin. An agent must be configured to communicate with the server and gather resource information. Until this is completed, no security information will be stored or indexed for this computer. Agents are configured when you add or edit a managed host.

- Real-time security updates in the context of Data Governance Edition refers to the monitoring of changes to the file system caused by create, delete, and rename operations, as well as DACL, SACL and Owner changes, in order to maintain the security index. These real-time security updates are not monitored by default, but can be configured on the **Security Scanning** page of the **Managed Host Settings** dialog.

NOTE: Enabling real-time security updates for NAS devices requires additional configuration on the NAS device itself. For more information, see [EMC managed host deployment](#) on page 162 and [NetApp managed host deployment](#) on page 156.

- When enabled, resource activity is collected in real time, compressed, and then stored in the Data Governance Resource Activity database. Historical activity data

can then be used to calculate a resource's perceived owner and to generate activity-related reports. Use the **Resource Activity** page of the **Managed Host Settings** dialog to enable and configure resource activity collection and aggregation.

- Managed paths will be scanned for security access information and if enabled, for collecting resource activity.

The available configuration settings vary depending on the type of managed host, as shown in the following table. Yes indicates that the settings can be configured.

Table 16: Configurable managed host settings

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
Local Windows Computer	Yes Not collected by default.	Yes Not monitored by default.	Yes By default, scanning starts immediately once an agent is deployed.	Yes By default, all NTFS drives are scanned if no managed paths are specified.	No service account is required as the agent runs as the Local System.
Windows Cluster / Remote Windows Computer	N/A	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with Local Administrator rights on the managed host. The agent scanning the host runs under the service account.
NetApp 7-Mode and Cluster-Mode CIFS Devices NetApp 7-Mode and Cluster Mode NFS Devices	Yes Not collected by default. Requires FPolicy	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must be a member of the local Administrators group on the NetApp 7-Mode filer in order to create FPolicy. This account must also have permissions to

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
					access folders being scanned.
EMC CIFS Devices	Yes Not collected by default.	Yes Not monitored by default.	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with required permissions. The agent scanning the host runs under the service account. The service account for an agent managing EMC Isilon storage devices, must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).
EMC Isilon NFS Devices	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must have "run as root" permissions on the Isilon SMB share to be managed (that is, selected as a managed path).
SharePoint Farm	Yes Not collected by default.	N/A	Yes Scanning starts on a configured schedule. By default, every day of	Yes Managed paths must be defined for scanning to occur.	Requires a service account; must be the SharePoint farm account (same account that is used to run the

Managed host type	Resource activity	Real-time security updates	Security scanning	Managed paths	Service accounts
			the week at 2:00 A.M.		SharePoint timer service and the One Identity Manager service (job server)); must be a member of the administrators group on SharePoint server. The agent scanning the host runs under the service account.
Cloud (for example, SharePoint Online)	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account which becomes the agent run as account. This account is not used to connect to the Cloud provider.
Generic	N/A	N/A	Yes Scanning starts on a configured schedule. By default, every day of the week at 2:00 A.M.	Yes Managed paths must be defined for scanning to occur.	Requires a service account with required permissions. The agent scanning the host runs under the service account.
Distributed File System	Yes Not collected by default.	N/A	N/A	N/A	N/A

Managed host settings dialog

The **Managed Host Settings** dialog allows you to define the configuration settings for new managed hosts. This dialog appears when you select one of the following tasks from the **Managed hosts** view:

- Manage host
- Manage multiple hosts
- Manage NFS host
- Manage Cloud host
- Edit host settings

This dialog contains the following controls.

Table 17: Managed Host Settings dialog: Controls

Control	Description
Managed Host	<p>Specifies the managed host to be added.</p> <ul style="list-style-type: none">• For local managed hosts, this is a read-only field that displays the name of the host computer selected in the Managed hosts view.• For remote managed hosts, including supported EMC and NetApp storage devices with CIFS file system protocol enabled, this is a read-only field that displays the name of the host computer selected in the Managed hosts view.• For cloud managed hosts, this field is blank when using the Manage Cloud host task. However, it displays the <i><DomainName>.onmicrosoft.com</i> host name when using the Edit host settings task.• If multiple hosts are selected, <Multiple Managed Hosts> appears in this field.• For NFS managed hosts, enter the IP address or fully qualified domain name of the NFS host computer to be managed.
Host Type	<p>Select the type of managed host to be added to the Data Governance Edition deployment.</p> <p>When using the Manage host or Manage multiple hosts task, the options available depend on the host computer selected in the Managed hosts view. Valid managed host types include:</p> <ul style="list-style-type: none">• EMC Celerra/VNX Device• EMC Isilon Device• Generic Host Type

Control	Description
	<ul style="list-style-type: none"> Local Windows Computer NetApp OnTap Cluster Mode CIFS Device NetApp OnTap 7-Mode CIFS Device SharePoint Farm Windows Cluster/Remote Windows Computer <p>When using the Manage NFS host task, you must select one of the following host types:</p> <ul style="list-style-type: none"> EMC Isilon NFS Device NetApp Cluster NFS Device NetApp 7-Mode NFS Device <p>When using the Manage Cloud host task, you must select one of the following host types:</p> <ul style="list-style-type: none"> SharePoint Online OneDrive for Business <p>When using the Edit host settings task, this is a read-only field that specifies the type of host.</p>
Agent Install Path	<p>By default, the agent will be installed in the Data Governance Server installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services).</p> <p>When you deploy an individual agent, you can use this field to specify an alternate agent installation. To specify an alternate installation directory, enter a local path (for example C:\Mypath) that does not exceed 512 characters.</p> <p>NOTE: If there is an existing agent on the machine, you cannot install another agent with a different installation directory. All agents must be installed in the same directory.</p> <p>NOTE: If required, use the Customize default host settings task to define an alternate default installation directory for deploying new agents. When you opt to set the installation directory for an individual agent using the Agent Install Path field on the Managed Host Settings dialog, it will take precedence over the default agent installation location defined on the Customize default host settings dialog.</p>
Keywords	(Optional) Enter a keyword which can then be displayed and used to group your managed hosts on the Managed hosts view.
NIS Host	Use the NIS Host page to select the Network Information Systems (NIS) server whose users and groups have been synchronized with One

Control	Description
	<p>Identity Manager.</p> <p> NOTE: This page only applies to NFS managed hosts.</p> <p>For more information, see NIS Host page on page 103.</p>
Credentials page	<p>Use the Credentials page to provide user credentials that can establish a connection with the NAS device.</p> <ul style="list-style-type: none"> • For NetApp hosts, the user must have the "ontapi" User Login Method application. • For EMC hosts, this account must have the "Platform API" privileges applied. <p> NOTE: This page only applies to NFS managed hosts and NetApp OnTap Cluster Mode CIFS managed hosts.</p> <p>For more information, see Credentials page on page 103.</p>
Cloud Provider	<p>The Cloud Provider page indicates if you are successfully authenticated with the Data Governance Edition API cloud proxy and can also be used to re-authenticate to the cloud proxy.</p> <p> NOTE: This page only applies to Cloud managed hosts.</p> <p>For more information, see Cloud Provider page on page 104.</p>
Agents page	<p>Use the Agents page to configure the agents to be used to monitor a remote managed host or SharePoint managed host.</p> <p> NOTE: This page only applies to remote managed hosts and SharePoint managed hosts.</p> <p>For more information, see Agents page on page 105.</p>
Managed Paths page	<p>Use the Managed Paths page to define the paths to be managed by Data Governance Edition. These managed paths will be scanned for security access information and if enabled, for collecting resource activity.</p> <p>Click the Add button to display the Managed Paths Picker dialog, where you can then navigate to and select the paths to be scanned.</p> <p>For more information, see Managed paths page on page 106.</p>
Security Scanning page	<p>Use the Security Scanning page to set the schedule and settings for scanning agents for changes to the structure and security of the file system.</p> <p>For more information, see Security Scanning page on page 107.</p>
Resource activity page	<p>Use the Resource Activity page to configure the collection and aggregation of resource activity for the target managed host.</p> <p> NOTE: Not available for Windows Cluster/Remote Windows</p>

Control	Description
	<p>Computer, Generic, or Cloud managed hosts.</p> <p>For more information, see Resource activity page on page 110.</p>
OK	Click the OK button to save your selections and close the dialog.
Cancel	Click the Cancel button to close the dialog without saving your selections.

NIS Host page

Select a Network Information Service (NIS) server whose users and groups have been synchronized with One Identity Manager.

NOTE: This page only applies to NFS managed hosts.

Table 18: NIS Host page: Controls and settings

Control/setting	Description
NIS Host	<p>Select the NIS server to be managed.</p> <p>The NIS servers previously synchronized with One Identity Manager (UNIX synchronization project) are listed in the drop-down menu.</p>

Credentials page

Provide the credentials of a user which can establish a connection to the NAS storage device.

- For NetApp devices, this user account must have the 'ontapi' User Login Method application.
- For EMC Isilon devices, this user account must be assigned the 'Platform API' privilege.

NOTE: This page only applies to NFS managed hosts and NetApp OnTap Cluster Mode CIFS managed hosts.

Table 19: Credentials page: Controls and settings

Control/setting	Description
User Name	Enter the name of a user account with access to the target NAS storage device.
Password	Enter the password associated with the specified user account.
Port	Enter the destination port to be used for communication between

Control/setting	Description
	<p>the agent and target NAS storage device.</p> <ul style="list-style-type: none"> • NetApp filers: The default value is 443. • EMC devices: The default value is 8080.
Host EndPoint	<p>Optionally, enter the API endpoint for the NetApp Cluster Mode connection. This could be an FQDN, host name or IP address.</p> <p>The default is to use the FQDN of the targeted host. You would only use this setting if the API connection needs to be specified as something other than the FQDN of the targeted host.</p> <p> NOTE: Only applies to NetApp Cluster Mode devices.</p>
Test API Credentials	Click this button to verify that the credentials entered are valid.

Cloud Provider page

The **Cloud Provider** page appears when managing a cloud resource. This page indicates if you are successfully authenticated with the Data Governance Edition API cloud proxy. You can also use this page to re-authenticate to the API cloud proxy. This API cloud proxy provides a consistent method for Data Governance Edition to interface with different cloud providers. When valid login credentials are provided, the system issues an access token which is used during the current and subsequent sessions to access resources hosted by the specified cloud provider.

| **NOTE:** This page only applies to Cloud managed hosts.

Clicking the **Re-authenticate** button redirects you to Microsoft to sign in to your account and grant access to Office 365 data.

On Microsoft's **Sign in to your account** dialog, enter the following information:

1. **Email, phone, or Skype:** Enter the email address of the administrator account to be used to authenticate with the cloud proxy.

For example: Administrator@MyDomain.onmicrosoft.com

| **NOTE:** You must create a separate administrator account for this purpose. This administrator account must be, or have equal access as, a SharePoint Online Administrator. Each site will be modified to list this account as a Site Collection Administrator for the site. This provides the account with access to the site's contents.

For SharePoint Online, create a separate Global Administrator account.

Click **Next**.

2. **Password:** Enter the password associated with the specified email account.

Click **Sign in**.

Once signed in, Data Governance Edition will have access to the specified resources for all users in your organization; no other user will be prompted to enter credentials.

Agents page

Use the **Agents** page of the **Managed Hosts Settings** dialog to configure the agents to be used to monitor remote managed hosts and SharePoint farms. Once an agent is deployed, use the **Agents** view to check its status and performance metrics.

NOTE: For EMC managed hosts, if you are collecting resource activity (**Collect and aggregate events** on the **Resource Activity** page) or real-time security updates (**Collect activity for real-time security updates** on the **Security Scanning** page), you can only specify one agent to scan the EMC storage device.

NOTE: You can only specify one agent to scan a cloud host.

Table 20: Agents page: Remote managed hosts

Control/setting	Description
Select the agent	Select the agent host computer to be used to monitor the target computer.
Select the service account	Select the service account with sufficient permissions to access both the target computer and the agent host. An agent requires a service account that has the rights to read security information on the remote host. Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 60.
Add	After selecting the agent and service account, click the Add button to add it to the Agent list.
Remove	Select an agent from the Agents list and click the Remove button to remove it from the Agent list. Removing the selected agent also removes the configured managed paths for the agent.
Agent list	Displays the agents selected to monitor the target computer. For remote managed hosts, add only one remote agent during the host's initial deployment. You can add additional remote agents later using the Edit host settings task after the managed host is deployed.

Table 21: Agents page: SharePoint farm managed hosts

Control/setting	Description
Agent Service Account	<p>Select the service account with sufficient permissions to access the SharePoint farm.</p> <p>The service account must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One Identity Manager service (job server)). The SharePoint farm account also needs to be added to the local Administrators group on the SharePoint server.</p> <p>Only previously configured service accounts that are registered with Data Governance Edition are available for selection. For more information, see Readying a service account and domains for deployment on page 60.</p>
Add	<p>After selecting the service account, click the Add button to add an agent service to the Agent list.</p> <p>Repeat to add additional agent services to be used to scan the target SharePoint farm.</p>
Remove	<p>Select an agent service from the Agent list and click the Remove button to remove it from the Agent list.</p> <p>Removing the selected agent service also removes the configured managed paths for the agent service.</p>
Agent list	<p>Displays the agent services selected to monitor the target SharePoint farm.</p>

Managed paths page

Managed paths determine the unstructured data for which a security index is maintained. A managed path is the root of an NTFS directory tree to be scanned by an agent, or a point in your SharePoint farm hierarchy below which everything is scanned. The agent monitors the specified managed paths for changes to security settings to maintain the security index. In addition, if resource activity collection is enabled, the agent collects resource activity for resources within these same managed paths.

Use the **Managed Paths** page on the **Managed Host Settings** dialog to specify the paths to be monitored and scanned for the target managed host.

NOTE: For all managed host types, when placing a resource under governance, the resource must be a managed path or a folder or share under a managed path.

- For remote managed hosts and SharePoint managed hosts, if you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. If the managed host has more than one agent assigned, you are prompted to select the agent to which the managed path is added.

- For local managed hosts, if you are scanning managed paths (that is, there are paths in the managed paths list), and you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. However, if you are scanning the entire server (that is, the managed paths list is empty) and you place a resource under governance, no changes are made to the managed paths list and you continue to scan the entire server.

Table 22: Managed paths page: Controls and settings

Control/setting	Description
Managed paths list	<p>Displays the managed paths to be monitored by the agent.</p> <ul style="list-style-type: none"> • For local managed hosts, when this list is empty, all NTFS drives are scanned and monitored (default scan behavior). When paths are added to this list, only the specified paths are scanned and monitored. • For remote managed hosts and SharePoint managed hosts, you must specify the paths to be managed in order for scanning to occur. So if this list is empty, no scanning will occur for the target managed host.
Add	<p>Use the Add button to define the paths to be monitored. Clicking the Add button displays the Managed Paths Picker dialog allowing you to select the paths to be managed and the agent to be used to scan the selected managed paths. In the Managed Paths Picker dialog, click the check box to the left of a path to add it to the managed paths list and use the Agent Selection drop-down menu to specify the agent to be used to scan the different managed paths.</p> <p>Multiple agents cannot scan the same managed paths on a remote managed host or SharePoint managed host.</p>
Remove	<p>Use the Remove button to remove a path from the managed paths list. Select the path to be removed and click the Remove button.</p>

Security Scanning page

Use the **Security Scanning** page on the **Managed Host Settings** dialog to define when an agent is to perform the initial security scan and when to watch for changes to the structure and security of the file system. Where possible, schedule the scan to low peak hours to avoid heavy network traffic.

The default behavior for security scanning is different depending on the type of agent deployed:

- Local agents: By default, local agents begin scanning immediately when the agent is deployed. Subsequent scans occur on the configured schedule, which is daily at 2:00 A.M. by default.

- Remote agents: Remote agents scan the target computer on a configured schedule. By default, scans are daily starting at 2:00 A.M.
- SharePoint farm agents: SharePoint farm agents scan the target computer on a configured schedule. By default, scans are daily starting at 2:00 A.M.

You can modify the scan schedule and define the time and frequency with which the agent scans the target computer using the options available on the **Security Scanning** page. In addition to defining the security scan schedule, you can specify whether to ignore files and only store folder security data, as well as continuously monitor the file system and apply real-time updates to scanned security data.

NOTE: The schedule times for security scanning are based on the agent's local time.

Table 23: Security scanning page: Controls and settings

Control/setting	Description
Scanning Schedule	<p>Use the options in the Scanning Schedule pane to define the frequency at which the agent performs a full security scan on the target managed host.</p> <p>For remote managed hosts and SharePoint managed hosts, managed paths must be defined for scanning to occur. For more information, see Managed paths page on page 106.</p>
Scan start time	<p>Specifies the local time of day, with respect to the machine on which the agent is running, when the security scan is to start. The default start time is 2:00:00 AM. To change this time, use the arrow controls to specify a new time.</p> <p>When the Immediately scan on agent restart or when managed paths change option is selected, the scan start time is ignore for the initial scan.</p>
Run Daily	<p>Select this option to scan the target computer on a daily schedule. Use the days of the week check boxes to define when the scan will occur during the week and the Scan start time field to specify the time the daily scan is to begin.</p> <ul style="list-style-type: none"> • Days of the week: Specifies the days of the week to be included/excluded from the daily run. All days of the week are selected by default. Click the corresponding day check box to clear the check box and exclude that day from the daily schedule. <p>For all agents, this option is selected by default along with a scan start time of 2:00 A.M. However, since local agents also have the Immediately scan on agent restart or when managed paths change option selected by default, the initial scan starts immediately when a local agent is deployed. This daily schedule is then used for subsequent scans by the agent. For remote and SharePoint agents, this daily schedule is used for the initial and subsequent scans.</p>

Control/setting	Description
Run on an interval	<p>Select this option to scan the target computer on an hourly interval instead of a daily schedule. Selecting this option enables the Every control to specify the interval to be used.</p> <ul style="list-style-type: none"> • Every: Specifies the hour interval to be used. Every 4 hours is specified by default. Click the arrow controls to select a different hour interval. <p>When using the Run on an interval option, it is possible to select 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 is skipped and the next scan starts as normal.</p>
Run once	<p>Select this option to schedule a single security scan of the agent.</p> <p>When the Run once option is selected, the Collect activity for real-time security updates option is automatically selected. This is to ensure that changes to the structure and security of the file system on the target managed host are applied to the scanned data.</p>
Immediately scan on agent restart or when managed paths change	<p>Select the Immediately scan on agent restart or when managed paths change option if you want the agent to scan immediately when it is added, when the agent is restarted and when any managed paths are changed.</p> <p>For local agents, this option is selected by default. To delay the initial scan and use a configured scan time, clear this check box and use the options in the Scanning Schedule pane to define when to start the agent scan.</p>
Ignore all files and only store folder security data	<p>The Ignore all files and only store folder security data indicates whether the agent is to capture file security data for the target managed host during an agent scan. When this option is cleared, the agent will include file security data in the agent scan.</p> <p>For all supported managed host types, this option is selected by default, indicating that only folder security data is to be scanned.</p> <p> NOTE: This option is not available for NFS host types.</p>
Collect activity for real-time security updates	<p>Select the Collect activity for real-time security updates option to have the agent watch for changes to the structure and security of the file system on the target managed host (that is, monitor create, delete, and rename operations, as well as DACL, SACL, and Owner changes). This results in a more up-to-date security index.</p> <p>When the Run once option is selected, this option is automatically selected to ensure that change to the structure and security of the</p>

Control/setting	Description
	<p>files system on the target host are applied to the scanned data.</p> <p>NOTE: When using Change Auditor to collect resource activity, it is not recommended to enable the Collect activity for real-time security updates on EMC or NetApp managed hosts. The agents managing these host types should be configured to scan on a schedule and not run once. The performance gain in using Change Auditor's event collection will be lost if the Data Governance agent is also collecting activity from these storage devices for security updates.</p> <p>NOTE: This option is not available for Generic, SharePoint Farm, SharePoint Online or OneDrive for Business host types.</p> <p>NOTE: When changing this setting, the agent starts watching for changes during and following the next scheduled full scan.</p>

Resource activity page

You can collect resource activity on local managed Windows servers, SharePoint farms, and supported NetApp and EMC managed hosts. Resource activity collection is not supported for Windows Cluster/Remote Windows Computer, Generic, or Cloud managed hosts.

NOTE: Limitations with collecting resource activity on EMC storage devices:

- EMC activity collection requires that EMC CEE 7.1 is installed on the same server as the Data Governance agent.
- EMC VNX activity collection by Data Governance agents is not supported for storage devices with multiple CIFS exposed virtual data movers.
- Resource activity collection and real-time security updates are not supported for EMC Isilon NFS managed hosts.
- If Change Auditor is configured to collect activity from your EMC device via the Quest Shared EMC Connector, and you would like activity collection/aggregation in Data Governance Edition, you **MUST** configure Data Governance Edition to collect activity directly from Change Auditor. You will not be able to collect activity from your EMC device with both Change Auditor and Data Governance Edition.

When enabled, you can configure to collect data on identities, reads, writes, creates, deletes, renames, and security changes on securable objects. Resource activity summary information is used to calculate ownership and for generating activity-related reports, including the Resource activity, Account activity, Interesting resources without an owner, Data owner vs. perceived owner, and Perceived owners for data under governance reports.

IMPORTANT: By default, the collection of resource activity is disabled. You can enable it when you configure your managed hosts. However, collecting resource activity on your managed hosts impacts network usage and increases load on the Resource Activity database server and Data Governance server, especially when collecting activity on large busy servers. Configuring the proper exclusions and aggregation is important to limit

some of this load. You should carefully plan out which servers you want to collect activity on and enable it only on those machines.

If you are collecting resource activity, it is recommended that you set up a scheduled execution of the activity database compression utility. This utility compresses the activity in your database that is older than a certain age and optionally purges entries that are even older. This is essential in ensuring your database remains manageable. For more information on the activity database compression utility, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

NOTE: Data Governance Edition may report certain operations in unexpected ways. For example, in some instances a file rename operation may be represented as a delete and a create. This is normal behavior and depends on the system, or in some cases, the applications being used to interact with the resources.

NOTE: The time stamps for resource activity are based on the agent local time.

The **Resource Activity** page on the **Managed Host Settings** dialog contains the following information and options to configure the collection and aggregation of resource activity.

Table 24: Managed host settings: Resource Activity page

Field	Description
No activity (scheduled security scans only)	<p>Use this option if you do not want to collect resource activity for the target managed host.</p> <p>NOTE: For all types of managed hosts, this option is selected by default indicating that resource activity is not being collected for the target managed host.</p>
Collect and aggregate events	<p>Select this option to collect resource activity for the target managed host. When this option is selected, you can configure the events to be collected and the aggregation interval to be used to compress the activity data.</p> <p>NOTE: For SharePoint farm managed hosts, native SharePoint auditing must be enabled in order to collect resource activity.</p> <p>NOTE: For NetApp managed hosts, the FPolicy settings control the activity sent to the agent, unless resource activity is being collected directly from Change Auditor. For more information, see FPolicy deployment on page 157.</p> <p>NOTE: For EMC Celerra/VNX devices, you must configure the cepp.conf. For more information, see Creating the cepp.conf file (Celerra or VNX devices) on page 163.</p> <p>NOTE: For EMC Isilon CIFS devices, you must enable auditing. For more information, see Enabling system configuration auditing (Isilon devices) on page 164.</p> <p>NOTE: When using Change Auditor to collect resource activity, this option is selected by default. For more information, see Configuring Change Auditor to collect resource activity on page 157.</p>

Field	Description
	55 .
Events	<p>Select or clear the check boxes to specify the type of events to be included in the resource activity collection process:</p> <ul style="list-style-type: none"> • Security change • Create • Delete • Rename • Write • Read (Disabled by default) <p>NOTE: When resource activity collection is enabled, read operations are not collected by default. Care should be taken when enabling read operations because they may cause performance issues.</p>
Aggregation	<p>Select how often you would like to aggregate the data. Valid aggregation intervals are:</p> <ul style="list-style-type: none"> • 5 minutes • 1 hours • 8 hours (default) • 1 day <p>All activity is aggregated within the set time frame, which is 8 hours by default. For example, if a user reads a file ten times within the time frame, it appears as a single line item with a count of 10.</p> <p>The aggregation interval should be chosen carefully. A shorter interval gives more granular information about activities but can cause the size of the database to use up all the disk space on the server.</p> <p>NOTE: When using Change Auditor to collect resource activity, the aggregation setting is not available. Change Auditor is configured to collect events every 15 minutes on all managed hosts. For more information, see Configuring Change Auditor to collect resource activity on page 55.</p>
Resource Activity Exclusions	<p>Click this button to specify the accounts, file extensions, and folders to be excluded from the resource activity collection process. By focusing on the objects in whose activity you are interested, you can reduce network traffic.</p> <p>Certain well known system accounts, file extensions, and folders are excluded by default, such as:</p>

Field	Description
	<ul style="list-style-type: none"> Accounts: Local Service, Network Service, Null SID, System <p>The Accounts tab is not available for NFS managed hosts.</p> <ul style="list-style-type: none"> File Extensions: Database files, Disc Image files, Email files, Executable files, Explorer Metadata files, Log files, Shortcut files, Temporary files, and Virtual machine files Folders: %SystemRoot%, %ProgramFiles%, %ProgramFiles (x86)% <p>By default, the Data Governance agent excludes the run as account (local managed hosts) and the domain service account (remote managed hosts) from activity collection and aggregation regardless if the service account is specified in the Resource Activity Exclusions list. The service account for SharePoint farm managed hosts are not excluded by default; you will need to add the SharePoint service account manually for SharePoint farm managed hosts.</p> <p>To see the full list, click the Resource Activity Exclusions button.</p> <ul style="list-style-type: none"> If the list is empty on the Resource activity exclusions dialog, click Default to populate the exclusions list with default values. To add an object to the exclusion list, click Add and specify the account, file extension or folder. <p>NOTE: When using Change Auditor to collect resource activity, the Resource Activity Exclusions feature is not available. For more information, see Configuring Change Auditor to collect resource activity on page 55.</p>
View/Update cepp.conf	<p>For EMC Celerra/VNX hosts, this button allows you to view or update the cepp.conf file for the selected data mover.</p> <p>Clicking this button displays a Logon Credentials dialog allowing you to enter the EMC Celerra/VNX control station credentials and to select the data mover to be scanned.</p> <ul style="list-style-type: none"> Control Station: Enter the IP address or host name of the EMC Celerra/VNX control station. User: Enter the user name of an account with administrative rights on the specified control station. Password: Enter the password associated with the user account entered. <p>The client attempts to connect and loads the list of available data movers on the specified device.</p> <ul style="list-style-type: none"> Data Mover: Select the data mover that holds the managed paths you wish to monitor and will also be associated with

Field	Description
	resource activity collection.
	<p>The client then retrieves and displays the cepp.conf file from the selected data mover. You can edit the Proposed cepp.conf file (lower pane) as needed. To save your edits, select Update File. The client then sends the Proposed cepp.conf file to the EMC device. It will stop and start the cepp service for the selected data mover to apply the new cepp.conf file.</p> <p>Click the Check Status button to retrieve the same information you would get if you ran "server_cepp server_2-pool-info" on the EMC device.</p>

Editing managed host settings

You can edit the managed host settings for one or more managed hosts of the same host type. For more information on the configuration options available, see [Managed host configuration settings](#) on page 96. You can also use the **Edit host settings** task to add, remove or change the agents used to scan a remote managed host. For more information, see [Removing agents](#) on page 124.

To edit a managed host's configuration settings

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select the required managed host with a status of **Managed**.
3. Select **Edit host settings** in the Tasks view or right-click menu.

The **Managed Host Settings** dialog appears, displaying the pages that contain settings that can be edited based on the type of host selected in the Managed hosts view.

- Use the **Managed Paths** page to change the paths to be scanned and monitored.
 - Use the **Security Scanning** page to change the scanning schedule and scan settings.
 - Use the **Resource Activity** page to change the resource activity collection and aggregation settings.
4. After making the required changes, click **OK** to save your selections and close the dialog.

The agent will scan using the new settings at the next scheduled scan time. However, if you modified the managed paths being scanned and the **Immediately scan on agent restart or when managed paths change** option is selected on the **Security Scanning** page, the agent initiates a scan immediately.

To edit multiple managed hosts

NOTE: When multiple managed hosts are selected, keep in mind that the settings are overwritten for all selected managed hosts and only the settings that are appropriate for the selected managed host type are applied. Because of this, you may notice that not all the same pages are displayed when multiple managed hosts are selected for editing (for example, the **Managed Paths** page is not displayed).

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select multiple managed hosts with the same host type in the **Managed hosts** view.
3. Select **Edit host properties** in the Tasks view or right-click menu.

The **Managed Host Settings** dialog appears, displaying the pages that contain settings that can be edited based on the type of host selected in the Managed hosts view.

- Use the **Security Scanning** page to change the scanning schedule and scan settings.
- Use the **Resource Activity** page to change the resource activity collection and aggregation settings.

The options displayed are the factory default values regardless of the current values of the selected managed hosts.

4. Select the **Apply these settings to all selected managed hosts** check box and make the required changes, which will be applied to all selected managed hosts.
5. Click **OK** to save your selections and close the dialog.

The agent will scan using the new settings at the next scheduled scan time.

Customizing default host settings

Defining default host settings for each type of managed host is now available through the Manager. Using the **Customize default host settings** task in the Manager, you can define the default scanning schedule and settings and the default resource activity collection and aggregation settings for the selected managed host type. Once customized default settings are defined, they are used when adding new managed hosts to the Data Governance Edition deployment.

NOTE: Currently managed hosts are not affected by the default host setting changes made on this dialog; only those added in the future use the settings defined here.

To customize default host settings

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select the **Customize default host settings** from the Tasks view or right-click menu.

The **Customize default host settings** dialog appears.

3. At the top of the dialog, specify the following information:
 - a. **Host Type:** Select the host type from the drop-down menu:
 - Local Windows Computer
 - Windows Cluster/Remote Windows Computer
 - Generic Host Type
 - SharePoint Farm
 - EMC Celerra/VNX Device
 - EMC Isilon Device
 - NetApp OnTap 7-Mode CIFS Device
 - NetApp OnTap Cluster Mode CIFS Device
 - NetApp Cluster NFS Device
 - EMC Isilon NFS Device
 - NetApp 7-Mode NFS Device
 - SharePoint Online
 - OneDrive for Business
 - b. **Agent Install Path:** Use this field if you want to specify an alternate installation location. This must be a local path (for example, C:\MyPath) and cannot exceed 512 characters.
 - c. **Keywords:** Use this field if you want to specify a keyword to be assigned to newly managed hosts, which can be used for sorting and grouping on the **Managed hosts** view.
4. Use the **Security Scanning** page to define the default scanning schedule and settings. For more information, see [Security Scanning page](#) on page 107.
5. Use the **Resource Activity** page to define the resource activity collection and aggregation settings. For more information, see [Resource activity page](#) on page 110.

NOTE: Resource activity collection is not available for the following host types:

 - Windows Cluster/Remote Windows Computer
 - Generic Host Type
 - EMC Isilon NFS Device
 - SharePoint Online
 - OneDrive for Business
6. Repeat steps 3 - 5 for any additional host types that require custom default settings.
7. If necessary, click the **Restore Factory Defaults** button to reset all changed settings back to the factory defaults.

NOTE: Clicking the **Restore Factory Defaults** button resets all custom default settings back to the factory default settings for all managed host types.
8. Click **OK** to save your selections and close the dialog.

All managed hosts of the selected host type that are added in the future will use these customized default settings.

Deployment management

You should regularly check the status of your managed hosts to ensure that the system is working properly. You can see the state of your deployment through the **Managed hosts** view and **Agents** view.

- [Verifying managed host system status](#)
- [Determining the state of the data](#)
- [Checking the agent status](#)
- [Viewing agent errors](#)
- [Restarting agents](#)
- [Remove managed hosts \(and associated agents\)](#)
- [Removing agents](#)

Verifying managed host system status

When you first deploy a managed host it takes a few minutes for the agent to start collecting data. As the status changes, a regular refresh allows you to see the changes. You can also use this status to track the progress whenever you add or remove an agent.

A managed host's status is displayed on the **Managed hosts** view.

Table 25: Managed host status

Status	Description
Agent Issue	One or more agents for this managed host are in an error state. The Status Detail column on the Agents view may contain additional information to identify the problem. NOTE: For remote managed hosts, if there is an issue with any of its agents, you see a status of "Agent Issue."
Agent Out of Disk Space	An agent for this managed host is out of free disk space. For more information, see Checking the agent status on page 120.
Agent Registration Failed	An error occurred while an agent was attempting to register with the server.
Agent Unregistered	An agent for this managed host has unregistered.

Status	Description
	Ensure that the agent service is running, and that the computer hosting the agent is online.
Agent Update Required	An unsupported agent version has attempted to register with the server. The agents on the managed host must be upgraded.
Deleting	The managed host is being deleted.
Deleting And Uninstalling	The managed host is being deleted and all agents associated with this managed host are being removed.
Deploying Agent	An agent for this managed host is being installed.
Install Failed	An automatic agent install has failed. The Status Detail column on the Agents view may contain additional information regarding the failure.
Installing agents failed	You are attempting to install an agent on a server that already has an agent on it, and that agent belongs to another Data Governance Edition deployment. The Status Detail column on the Agents view may contain additional information, including the name of the deployment that is already using this agent.
Managed	All agents associated with this managed host are working properly.
No communication from agent	The lease for an agent on this managed host has expired. A communications issue has occurred between the agent and the server, or the agent is no longer running. Ensure that the agent can communicate with the server.
No agents for host	There are no agents associated with this managed host. Deploy an agent for this host in order to maintain a security index and track resource activity.
Not Managed	The host computer is not being managed by Data Governance Edition. That is, no managed host has been configured for the host computer.
Resolved	The managed host's information has been resolved, but it has not yet been configured for management. This is a temporary state.
Resolving Agents	The server is resolving an agent computer for this managed host.
Un-deploying Agents	An agent for this managed host is being uninstalled.
Uninstalling agents failed	An automatic uninstall of an agent failed. The Status Detail

Status	Description
	column on the Agents view may contain more information regarding the failure.
Unknown	An error occurred while retrieving this managed host's agent status.
Unknown host type	A host computer with an unknown host type was found.
Unresolvable	The managed host computer has failed to be resolved.
Unresolved	The managed host computer has not yet been resolved.
Upgrading agent	The agent is being upgraded to the latest version.
Waiting for Agent Connection	<p>The managed host has been configured and is waiting for an agent to register.</p> <p>If a managed host stays in this state for a long time, it could indicate a communications issue between the agent and the server.</p>

Determining the state of the data

For each managed host, use the **Managed hosts** view to determine the state of the data. Errors should be addressed immediately, in order to ensure accurate data from the managed host being scanned. The following table outlines the different states your data can have.

Table 26: Data states

State	Description
A scanning error has occurred	There has been an error with one of the scanners. Data is incomplete, so you should determine what the issue is. Ensure that the managed host is available on the network, and confirm that the agent's service account has adequate access to the managed host.
Data available	The agent has successfully completed scanning security information for the managed host.
Please use Agents View to see status data for multiple agents	On multi-agent hosts, this message indicates that the status of the data is not available for all of the agents. Open the Agents view to see the status of the data for each individual agent assigned to the selected managed host.
Scanning	The agent is performing a full scan of security information. Queries for information at this time may be incomplete.
No managed paths configured	There are no managed paths specified and therefore scanning cannot be performed on the managed host.

State	Description
Waiting for scanning to start	The agent is ready to scan when the next scheduled scan is triggered.
Waiting for scanning status	The agent is not yet ready to start scanning.

Checking the agent status

For security indexing and resource activity tracking to function as expected, the agent must have a status of **Managed**. You can see the status of an agent in the **Agents** view. Also, if the status of a managed host is anything other than **Managed**, check the host's agents' status to determine where the issue lies.

NOTE: During deployment, the state changes quickly, and a regular refresh allows you to see the changes.

Table 27: Agent states

Agent states	Description
Agent host belongs to another deployment	An agent already resides on this server that belongs to another Data Governance Edition deployment. See the Status Detail column for additional information, including the name of the deployment that is already using this agent.
Agent Out Of Disk Space	<p>The hard disk of the agent's working directory dropped below 2GB.</p> <p>NOTE: This condition causes the agent to shutdown with an error. This is a safeguard to prevent disruption of other services hosted on the computer, allowing you time to add a volume or reallocate space. See Agent Shutdown Because of Error.</p>
Agent Shutdown Because of Error	<p>The agent may shut down with error for the following reasons:</p> <ul style="list-style-type: none"> Agent scanning does not progress after two hours. There is not enough free disk space on the agent (minimum 2GB). See Agent Out Of Disk Space. <p>NOTE: To determine if low space on the host volume was the cause, check the Agent Events view or agent logs.</p> <ul style="list-style-type: none"> An error occurred while the agent attempted to open an NTFS security database to perform a sync.
Agent Update Required	An unsupported agent version has attempted to register with the server.

Agent states	Description
Agent Unregistered	The agent has unregistered.
Configuration Failed	An error has occurred while creating the agent service on the agent host computer.
Configuration in Progress	The agent service is being configured.
Deleting	The agent is being deleted.
Deleting and Uninstalling	The agent software is being uninstalled.
Host Configuration Failed	<p>While preparing for an agent installation, one of the conditions were encountered:</p> <ul style="list-style-type: none"> • The host's data root is invalid. • The host has a NetApp FPolicy configuration error.
Host Domain Not Managed	The host domain is not yet managed in Data Governance Edition.
Install Failed	An error occurred while installing the agent.
Install in Progress	The agent installation is in progress.
No Communication from Agent	The agent has failed to renew its lease. This state is often an indication of an error on the agent computer. Ensure that the agent can communicate with the server.
OK	The agent is working properly. The agent is deployed and has contacted the Data Governance service.
Registration Failed	An error occurred while the agent was attempting to register with the server.
Removal of configuration failed	An error occurred while removing the agent from the agent host computer.
Removal of configuration in progress	The agent service is being removed.
Resolved	The managed host's information has been resolved, but it has not yet been confirmed for management. This is a temporary state.
Uninstall Failed	An error occurred while uninstalling the agent service from the agent host computer.
Uninstall in Progress	The agent is being uninstalled.
Uninstalled	The uninstall has finished. This is a temporary state.

Agent states	Description
Unknown	The current state of the agent is unknown.
Unresolvable	The agent computer cannot be resolved.
Unresolved	The agent computer has not yet been resolved.
Waiting for agent connection	The management server is waiting for the agent to register with the server. NOTE: If an agent remains in this state for a long time, it could indicate a communication issue between the agent and the server.

Viewing agent errors

You can quickly assess your agents for any potential critical issues by reviewing logged error messages using the **Agents** view in the Manager.


NOTE: The **Agent Errors** column in the **Managed hosts** view indicates when an agent associated with a managed host has encountered any errors. However, you can only view an agent's error messages using the Agents view.

To view agent errors

1. In the Navigation view, select **Data Governance | Agents**.
The **Agents** view appears.
2. The **Critical Error** column indicates if there are any error messages logged for an agent.
3. Select the agent from the **Agents** view, and select **View agent errors** in the Task view or right-click menu.

NOTE: The **View agent errors** task is only available for agents that have error messages logged.

4. The event viewer appears.

Click the  **Clear Events** button in the upper left corner to clear the agent errors. Click **Yes** on the confirmation dialog.

Click the close button in the upper right corner to close the event viewer.

NOTE: You can also clear error messages for a specific agent using the **Clear agent errors** task from the Agents view.

Restarting agents

You must restart an agent when a new storage volume is added to the managed host being scanned by the agent.

To restart an agent

1. In the Navigation view, select **Data Governance | Agents**.
2. Select the required agents in the **Agents** view, and select **Restart agent** in the Tasks view or right-click menu.
3. Click **Yes** to confirm.

NOTE: When a Data Governance agent is restarted, it re-creates all information within its local index. The server index is updated when the full scan completes. An agent will immediately start scanning when the service is restarted if the **Immediately scan on agent restart or when managed paths change** option is selected. This option is available at the bottom of the **Security Scanning** page on the **Managed Host Settings** dialog.

To determine whether data in the client is the most current from the agent, ensure that the data state of the managed host being examined is marked as "Data available."

Remove managed hosts (and associated agents)

NOTE: All agents associated with a managed host are uninstalled when you remove a managed host.

Before removing a managed host ensure that the impact of its removal is considered. Any governed data records or activity information associated with resources on that host is removed from the database as well. Use caution when removing the governance on an item, as there may be business reasons for this setting.

It can take a considerable amount of time to remove a managed host with governed resources (for example, one to two hours per million governed resources). The Manager lists the managed host in the "Deleting" state until this process finishes.

To remove a managed host (and its agents)

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select a managed host from the **Managed hosts** view, and select **Remove** in the Tasks view or right-click menu.

NOTE: You can select multiple managed hosts for removal.

The **Remove** task is not available for host computers with a status of **Not Managed**.

3. Click **Remove** to confirm the removal.

If you remove a managed host with governed data, the data is no longer governed. All associated security information and resource activity is also deleted.

Removing agents

All agents associated with a managed host are uninstalled when you remove a managed host. You can, however, remove a remote agent without removing the managed host using the **Edit host settings** task.

NOTE: You must have at least one agent assigned to the managed host in order to complete the edit operation.

To remove a remote agent from a managed host

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view (right pane), select the required managed host with a status of **Managed**.
3. Select **Edit host settings** in the Tasks view or right-click menu.
The **Managed Host Settings** dialog appears.
4. Open the **Agent** page, select the agent to be removed and click **Remove**.
5. Click **OK** to remove the selected agent.

NOTE: Removing the agent will also remove the managed paths associated with that agent. If that is the desired result, select **Yes** on the confirmation dialog.

NOTE: If you remove the last agent in the list, the **OK** button will not be available. You will need to specify at least one agent for the managed host before you can save your changes.

Upgrade Data Governance Edition

One Identity Manager and Data Governance Edition must be running the same version; therefore, a full One Identity Manager Data Governance Edition upgrade is required. Use the new installation and configuration wizards to upgrade from a previous version of One Identity Manager Data Governance Edition.

TIP: When upgrading from version 7.x.x to 8.x, you are only upgrading the One Identity Manager database. During an upgrade, One Identity Manager 8.x creates a new One Identity folder and leaves the old Dell folder. Once One Identity Data Governance Edition 8.x is installed and all of the Data Governance agents have been upgraded, then you can uninstall One Identity 7.x.x, which will remove the old job service and files. Do NOT uninstall One Identity 7.x.x first; this will remove the Data Governance service and local agents before they are updated.

NOTE: Required changes to system connectors or the synchronization engine are made available when you update One Identity Manager. These changes must be applied to existing synchronization projects to prevent target system synchronizations that are already set up from failing..

NOTE: By default, all job servers are automatically updated after the One Identity Manager database is upgraded when you run the Configuration wizard.

NOTE: After the One Identity Manager database is upgraded, the web portal will be automatically updated when it appears to be idle.

If it appears that the web portal did not get updated properly, check the web client log (C:\inetpub\wwwroot\IdentityManager\App_Data\Logs). The web portal upgrade will fail if the auto upgrade flag was manually disabled or if the required domain administrator credentials were not specified.

You can trigger the update of the web portal by accessing the following web site, <Web Portal>/IdentityManager/Monitor#Status and clicking the **Update Now** button.

On an upgrade, do NOT use the same user account for your update account and your application pool account.

For more detailed information on updating the web portal, see the *One Identity Manager Installation Guide*.

NOTE: After the One Identity Manager database is upgraded, the Application Server will be automatically updated when it appears to be idle. However, you can trigger the update by accessing the following web site, <App Server>/AppServer and clicking the **Update**

Immediately button.

On an upgrade, if you enter an optional update account, do NOT use the same account as your application pool account.

For more detailed information on updating the Application Server, see the *One Identity Manager Installation Guide*.

NOTE: If the Application Server or web portal do not upgrade, you can uninstall the existing one and reinstall the Application Server and web portal sites.

Before you upgrade

Note the following information that should be taken into consideration before you begin the upgrade process.

One Identity Manager system requirements

Some of the system requirements for One Identity Manager have changed in version 8.1. Prior to upgrading Data Governance Edition, ensure that the minimum requirements for all of the One Identity Manager components are met. See the *One Identity Manager Installation Guide* for full details on One Identity Manager's system requirements.

Upgrading an existing One Identity Manager installation

Review the *One Identity Manager Release Notes* for important information regarding upgrading an existing One Identity Manager installation to version 8.x. There are some additional steps that are required. For example:

- You need at least one dialog user with administrative permissions that has a password assigned; otherwise, the schema update cannot be completed successfully.
- You must upload and update some DLLs in your 7.x.x installation prior to upgrading to 8.x, otherwise auto-update will not work properly.
- To successfully compile HTML applications with the Configuration wizard, you must download packages from the NPM repository. Ensure that the workstation running the Configuration wizard can establish a connection to the web site registry.npmjs.org.

Alternatively, you can download the packages from a proxy server and make them available manually. For more information, see the knowledge base article: <https://support.oneidentity.com/kb/266000>.

One Identity Manager Database system requirements (SQL Server)

As of version 8.1, the One Identity Manager database must be running a minimum of Microsoft SQL Server 2016 Standard Edition, Service Pack 2 with the latest cumulative update. Earlier versions of SQL server are no longer supported.

TIP: Best practice: Create a copy of the One Identity Manager database before you upgrade.

Prior to running the **Configuration Wizard** (ConfigWizard.exe) to upgrade and configure the One Identity Manager database, set the database compatibility level to 130:

```
ALTER DATABASE <Database name>  
SET COMPATIBILITY_LEVEL=130  
GO
```

One Identity Manager permissions

During the installation or upgrade of the One Identity Manager database, you can specify whether you want to use a more fine-grained set of SQL permissions to access the SQL server. With this more granular permission set, the Configuration wizard creates SQL Server logins and database roles with the necessary permissions for administrative users, configuration users, and end users. For more detailed information about permissions, see the *One Identity Manager Installation Guide*.

If you select to use this more granular permission set, adjust the configuration parameter after updating the One Identity Manager. This affects, for example, the connection data for the database (DialogDatabase), the One Identity Manager Service, the Application Server, the administration and configuration tools, the web applications, the web services, and the connection data in synchronization projects.

Agent system requirements

As of Data Governance Edition version 7.0.2, there are new system requirements for Data Governance agents. Ensure your agents meet the system requirements:

- .NET Framework 4.5 (or later) is required.
- Agents running the Windows Server 2003 R2 operating system are no longer supported.

EMC system requirements

EMC Common Event Enabler (CEE) 7.1 is the minimum version now supported for scanning and resource activity collection.

- If you are using EMC Celerra/VNX devices with multiple CIFS exposed virtual data movers, do not upgrade to Data Governance Edition version 7.0.2 (or later).
- If you are using EMC Isilon devices or EMC Celerra/VNX devices with only physical CIFS exposed data movers, each Data Governance agent managing an EMC device must run on a different host server and point to its own local CEE 7.1. Each managed EMC storage device needs to specify the single CEE server where the Data Governance agent is running.

The Quest Shared EMC Connector server is no longer used as of Data Governance Edition version 7.0.2.

- If Change Auditor is configured to collect activity from your EMC storage device using the Quest Shared EMC Connector, and you would like activity collection or aggregation in Data Governance Edition, you **MUST** configure Data Governance Edition to collect activity directly from Change Auditor. You will not be able to collect activity directly from your EMC device with both Change Auditor and Data Governance Edition.
- If you have EMC managed hosts currently using the Quest Shared EMC Connector server, follow this procedure to ensure this connector service is removed from your Data Governance Edition deployment:
 1. Uninstall EMC CEE framework.
 2. Uninstall Quest Shared EMC Connector service (QCeeService).
 3. Install EMC CEE 7.1 framework on the same server as the Data Governance agent.
 4. Modify the following registry key to ensure "Dell" or "QuestSoftware" is no longer referenced:


```
HKEY_LOCAL_MACHINE\SOFTWARE\EMC\CEE\CEPP\Audit\Configuration
```

 - Enabled: Set to 0
 - Endpoint: Remove "Dell" or "QuestSoftware"

Custom agent registry settings

Legacy Data Governance agent registry settings are no longer available as of Data Governance Edition version 7.0.2. You can use the agent's configuration file to modify agent configurations that are not available in the Manager client. Previously set agent registry settings need to be reviewed and will need to be re-set using the corresponding configuration file setting or Manager setting. For more information on the configuration file settings available, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

Custom Data Governance server configuration settings

TIP: Best practice: Create a copy of the Data Governance server configuration file before you upgrade Data Governance Edition.

The upgrade process preserves any configuration changes previously made to the DataGovernanceEdition.Service.exe.config file (which can be found in the server directory: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server). For more information about the configuration file settings available, see the *One Identity Manager Data Governance Edition Technical Insight Guide*.

NOTE: Upgrades from pre-7.1.2 versions: Changes made to the configuration file will be lost when you upgrade. Refer to the copy you made of the configuration file to make the necessary configuration changes after the upgrade is complete.

Previously governed or published files

Beginning with Data Governance Edition version 7.0.2, you can no longer govern or publish files to the IT Shop. However,

- Previously published (those that are both governed and published) files are still available in the IT Shop.
- Previously governed (but not published) files can be published to the IT Shop.

NFS managed hosts

Beginning with version 7.0.2, Data Governance Edition supports the scanning of NAS devices with NFS file system protocol enabled, including NetApp 7-Mode, NetApp Cluster and EMC Isilon devices. If you want to take advantage of this new feature, be sure to add the UNIX module during the upgrade process. For more information, see [Upgrading One Identity Manager Data Governance Edition](#) on page 129.

If you upgrade to Data Governance Edition version 7.0.2 (or later), but do not add the UNIX module as part of the initial upgrade; but later want NFS support, you must select to upgrade the Data Governance Edition module in addition to adding the UNIX module when running the One Identity Manager Configuration wizard.

Upgrading One Identity Manager Data Governance Edition

In order to take advantage of the enhancements added to Data Governance Edition version 8.2, you must perform a full One Identity Manager Data Governance Edition upgrade, which includes:

- Running the autorun.exe program to deploy the latest version of One Identity Manager Data Governance Edition.
- Running the Configuration wizard to upgrade the One Identity Manager database.
- Running the Data Governance Configuration wizard to upgrade the Data Governance service and connect to an existing (or install a new) Resource Activity database.
- Upgrading the Data Governance agents.

To upgrade One Identity Manager Data Governance Edition

NOTE: These are simplified steps. Refer to the *One Identity Manager Installation Guide* or *One Identity Manager Release Notes* for full upgrade information for One Identity Manager and [Deploying Data Governance service and creating Resource Activity database](#) on page 37 for more information regarding the Data Governance Configuration wizard.

1. Run the JobQueueInfo.exe and wait for the queue to clear.
2. Once the job queue is empty, stop the One Identity Manager service on the server handling queries from the Master SQL Server.
3. Stop the Data Governance service.
4. If you are upgrading the One Identity Manager database, stop any One Identity Manager Application Server that has a database connection open.
5. For SQL server deployments, ensure that the SQL server agent is running.
6. Log in to the server hosting the One Identity Manager workstation tools, run the One Identity Manager autorun.exe program, open the **Installation** page and install **One Identity Manager Data Governance Edition**.
7. During the installation process:
 - a. Accept the license agreement
 - b. Confirm the installation source and destination (Installation folder).
 - c. It is recommended that you select the **Select installation modules from existing database** check box. This automatically selects the proper modules to be enabled during the installation, based on the modules assigned to the system within the existing database.

NOTE: If you have purchased additional One Identity Manager modules (for example, the Business Roles module), select the **Add more modules to the selected Edition** check box. An additional screen appears allowing you to select the additional modules to be installed.

If you want to take advantage of the new NFS managed hosts feature, select the **Unix** module.
 - d. Select the database connection string pertaining to the server/database to be updated.
 - e. Confirm the machine roles (modules) to be installed on the current system.
8. Once the installation has successfully completed, the last screen of the setup wizard prompts you to run some additional tools. Two of these tools are required for a successful upgrade:
 - a. **Configuration Wizard** to upgrade and configure the One Identity Manager database.
 - b. **Data Governance Configuration** to upgrade the Data Governance service and Resource Activity database.
9. Run the **Configuration Wizard** and follow the prompts on the screens:
 - a. Select **Update database** to upgrade the existing One Identity Manager database to the new version.
 - b. Select the database connection string of the One Identity Manager database to be updated.
 - c. Confirm the installation source (Source media) for the upgrade of the database.

- d. Before the update process begins, you must confirm that you have backed up your database.
- e. Ensure that the Data Governance module is selected.

Also, if you want to take advantage of the new NFS managed host feature or have purchased additional One Identity Manager modules, select the **Add new modules** check box to select the modules to be installed. An additional screen appears allowing you to select the modules to be installed.

NOTE: To enable the NFS managed hosts feature, add the **Unix** module.

- f. Resolve any errors listed on the **Database check** page. Click **Redo check** to confirm all errors have been resolved.
- g. On the **Create a new login for administrators** page, specify the SQL Server login to be used for administrative users.

NOTE: This page only appears when updating a One Identity Manager database from versions 7.0, 7.1, or 8.0 to version 8.1.

Select one of the following options:

- **Create new SQL Server logins for the database:** Select this option if you want to use a more granular permission set on the SQL Server. Selecting this option, creates additional SQL Server logins and database roles with the necessary permissions for administrative users, configuration users, and end users.

Enter the login name, password, and password confirmation for the new administrative SQL Server login.

NOTE: You will be prompted for the credentials for the other SQL Server logins (system configuration users and end users) after the database has been migrated.

- **Use the current SQL Server login for the database:** If you select this option, no additional SQL Server logins are created for the database. In this case, you cannot use the more granular permission set at the SQL Server level. The user you specified is used to connect to the database.

NOTE: To change to a more granular permission set at a later date, contact One Identity support. To access the One Identity support portal, go to <https://support.oneidentity.com/identity-manager/>.

- h. When prompted, enter the One Identity Manager system administrator credentials to perform the database upgrade tasks. This can be the credentials for the viadmin account or those of another custom administrative system user account.

NOTE: The **Active Sessions** dialog opens if there are active sessions connected to the database. For SQL server deployments, disconnect all sessions using the database by selecting the session and clicking **Disconnect**.

- i. The database will now recompile and update all the necessary files. In addition, after the database is upgraded all of the job servers, the Application Server,

and the web portal will be automatically updated. Wait for the installation to finish. This can take some time depending on the amount of data and system performance.

- j. The **Create SQL server logins** page appears if you selected **Create new SQL Server logins for the database**. Enter the SQL Server login credentials for the system configuration users and end users.
10. Run the **Data Governance Configuration** wizard and follow the prompts on the screens:
 - a. Enter the SQL Server information for your One Identity Manager database.
 - b. Deploy the service update to your current Data Governance service host, or connect to a previously installed Data Governance service host which has already been manually upgraded.
 - c. Confirm the server's fully qualified domain name (FQDN), port, and Deployment name.
 - d. Specify the account to be used to run the Data Governance service.

NOTE: The **Use LocalSystem account** check box is selected by default indicating the local system account will be used to run the Data Governance service. If you clear this check box and specify a different service account, you must move the Service Principal Name (SPN) from the computer object. For more information, see the post installation step, [Move Service Principal Name in Active Directory](#).
 - e. Wait for the deployment to complete.
 - f. Provide credentials to the Data Governance Resource Activity database.
 - g. Confirm the database name and properties.
11. Manually start the One Identity Manager job service.
12. Open the Manager to upgrade the Data Governance agents. When prompted to perform updates, click **Yes**.

NOTE: After upgrading the Data Governance service to version 8.x, existing agents will initially connect; however, after an agent restart, they will no longer connect, displaying a "Waiting to connect" state, and must be upgraded.

NOTE: An agent upgrade may initiate a re-scan of the managed paths.

NOTE: When you upgrade an agent on a computer that hosts multiple agents (agents on this host are scanning different managed hosts), the agent services will be upgraded for all the managed hosts (not just the one you selected).

In cases where you have many agents scanning a single managed host (all watching different managed paths on the managed host), and you select to upgrade one of the agents through the **Agents** view, all the agents (on all computers scanning that host) will be upgraded.

To upgrade Data Governance agents:

- a. In the Navigation view, select **Data Governance | Agents**.
- b. Right-click the agent and select **Upgrade agent**.

NOTE: The **Upgrade agent** option is only available if a newer agent version is available. If you do not see the upgrade option, you are running the latest version and no upgrade is necessary.

NOTE: You can multi-select agents to upgrade.

See [Post installation configuration](#) for additional configuration that may be required post upgrade.

Applying a hotfix to Data Governance Edition 8.x

NOTE: Beginning with version 7.0.1, the Data Governance Edition module can be updated and released independently of One Identity Manager. Therefore, for this release and all future Data Governance Edition releases (hot fixes or service pack releases), you will receive a new QAM folder that will replace the existing QAM folder installed with One Identity Manager Data Governance Edition 8.0.x (and later).

Before you begin:

- Replace the existing QAM module with the QAM module provided in the hotfix release package. That is, replace the existing local `<OneIM-Build>\Modules\QAM` folder with the latest QAM folder you received.

Once this step has been completed, you will perform the following steps to upgrade the databases and services:

- Run the `autorun.exe` program to deploy the latest version of One Identity Manager Data Governance Edition.
- Run the Configuration wizard to upgrade the One Identity Manager database.
- Run the Data Governance Configuration wizard to upgrade the Data Governance service and Resource Activity database.
- Upgrade the Data Governance agents (optional).

To apply a One Identity Manager Data Governance Edition 8.x hotfix

NOTE: These are simplified steps. Refer to the *One Identity Manager Installation Guide* for full upgrade information for One Identity Manager and [Deploying Data Governance service and creating Resource Activity database](#) on page 37 for more information regarding the Data Governance Configuration wizard.

1. Run the `JobQueueInfo.exe` and wait for the queue to clear.
2. Once the job queue is empty, stop the One Identity Manager service on the server handling queries from the Master SQL Server.
3. Stop the Data Governance service.
4. For SQL server deployments, ensure that the SQL server agent is running.

5. Perform a One Identity Manager and Data Governance Edition upgrade:
 - a. Log in to a server hosting the One Identity Manager administrative components and run the One Identity Manager autorun. From the autorun, open the **Installation** page and install **One Identity Manager Data Governance Edition**.
 - b. Run the Configuration Wizard (ConfigWizard.exe) to upgrade and configure the One Identity Manager database.

NOTE: You will be blocked from continuing if the job queue is not empty. You will be asked to stop the job service and close all open connections to the One Identity Manager database.
 - c. Start the One Identity Manager job service.
 - d. Run the Data Governance Wizard (Data Governance Configuration wizard.exe) to upgrade the Data Governance service and resource activity database.
6. Open the Manager to upgrade the Data Governance agents. If prompted to perform updates, click **Yes**.

Remove Data Governance Edition

Use the following sequence to remove the Data Governance Edition components:

- [Remove managed hosts \(and associated agents\)](#)
- [Remove service account assignments](#)
- [Delete service accounts](#)
- [Uninstall Data Governance service](#)
- [Uninstall Resource Activity database](#)

For information on removing the One Identity Manager components (job service and database), see the One Identity Manager documentation.

Remove managed hosts (and associated agents)

NOTE: All agents associated with a managed host are uninstalled when you remove a managed host.

Before removing a managed host ensure that the impact of its removal is considered. Any governed data records or activity information associated with resources on that host is removed from the database as well. Use caution when removing the governance on an item, as there may be business reasons for this setting.

It can take a considerable amount of time to remove a managed host with governed resources (for example, one to two hours per million governed resources). The Manager lists the managed host in the "Deleting" state until this process finishes.

To remove a managed host (and its agents)

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select a managed host from the **Managed hosts** view, and select **Remove** in the Tasks view or right-click menu.

NOTE: You can select multiple managed hosts for removal.

The **Remove** task is not available for host computers with a status of **Not Managed**.

3. Click **Remove** to confirm the removal.

If you remove a managed host with governed data, the data is no longer governed. All associated security information and resource activity is also deleted.

Remove service account assignments

Use the Manager to remove all the service account assignments from your managed domains:

1. In the Navigation view, select **Data Governance | Service accounts**.
2. In the **Service Accounts** pane, select the service account.
3. Right-click and select **Tasks | Assign domains**.
4. In the **Remove assignments** pane (top pane), double-click the managed domain to be removed. You can also right-click the managed domain and select **Remove** or **Remove All**.

The managed host now appears in the **Add assignments** pane (lower pane).

5. Click the **Save** toolbar button to save your selection.

Delete service accounts

Use the Manager to delete all registered service accounts:

1. In the Navigation view, select **Data Governance | Service accounts**.
2. In the **Service Accounts** pane, right-click the service account and select **Delete**.
3. Select **Yes** to confirm the deletion.
4. Repeat to remove all service accounts.

Uninstall Data Governance service

Use Add/Remove Programs to uninstall the Data Governance Edition service.

1. From the Start menu, run Programs and Features (**Control Panel | All Control Panel Items | Program and Features**).
2. Locate **One Identity Manager Data Governance Edition Server <version>** in

- the program list, right-click and select **Uninstall**.
3. Click **Yes** on the confirmation dialog.

Uninstall Resource Activity database

Using your preferred database management tool, manually remove the Data Governance Resource Activity database.

Troubleshooting

The following troubleshooting tips are provided to assist you in deploying and configuring Data Governance Edition:

- [Data Governance Edition logs](#)
- [Job queue shows that database needs to be compiled](#)
- [Receiving unauthorized access violations](#)
- [Cannot save the service account](#)
- [Cannot connect to a managed host](#)
- [DNS error when attempting to add a new managed host](#)
- [Agent not connecting to the Data Governance server](#)
- [Data Governance agents cannot access NAS devices via SMB](#)
- [Agent leases expiring](#)
- [Cannot add managed paths to my EMC server](#)
- [No activity data](#)
- [No activity data available for SharePoint 2010 managed host](#)
- [Resource activity is not displaying in the web portal for a business owner](#)
- [Governed resources are missing from the All my resources view in the web portal](#)
- [Not receiving scheduled reports](#)
- [Groups missing from the Group Memberships tree view](#)

Additional troubleshooting tips may be found in the following guides:

- *One Identity Manager Data Governance User Guide*: Troubleshooting tips related to the day-to-day administration of Data Governance Edition
- *One Identity Manager Data Governance IT Shop Resource Access Requests Guide*: Troubleshooting tips related to self-service resource access requests and share creation requests.

Data Governance Edition logs

The first place to look when you run into an issue with Data Governance Edition is the logs. The Data Governance Edition logs available are:

Data Governance configuration wizard log

Log name: Data Governance Configuration Wizard.exe.dlog

The Data Governance configuration wizard log is stored as a Trace log document (.dlog) in the users AppData directory. For example:

C:\Users\MyName.MyDomain\AppData\Local\One Identity\One Identity Manager\Data Governance Configuration Wizard\.

Used for capturing errors encountered while using the Data Governance Configuration wizard to deploy the Data Governance service and create the Resource Activity database.

Data Governance server log

Log name: DataGovernanceEdition. Service.exe.dlog

NOTE: The Data Governance server maintains rolling log files based on settings found in the DataGovernanceEdition.Service.exe.config file, therefore there may be multiple server log files in the Data Governance service installation directory. The first log file is the active log and is being maintained by the server. When this log file reaches a specified size, it is renamed (a number is appended to the name) and a new file is started with the original name.

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the DataGovernanceEdition.Service.exe.config file in the Data Governance service installation directory.
2. Open the configuration file and edit the following setting:

```
<rules>  
    <logger name="*" minlevel="INFO" writeTo="logfile">
```
3. Change INFO to DEBUG to get detailed logging.
4. Save the file.

The server log is stored as a Trace log document (.dlog) in the Data Governance service installation directory. For example: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\.

Used for capturing the following information:

- Data Governance service communication
- Group resolution and group expansion
- Agent lease expiration information
- Points Of Interest (POI) collection information
- Resource activity updates

- Security changes made on a resource from the Manager
- Incoming web service calls related to Data Governance Edition from the One Identity Manager web site

NOTE: In previous versions of Data Governance Edition, individual server log files were generated. Starting with Data Governance Edition version 7.0.2, the logging information from all of these server logs are now available in this single server log file.

Server logs can be viewed as described below:

- In the Manager, use the **Get All Logs** task to export the server log to a specified location. From that location, double-click the log file to view the log in the Log Viewer. For more information, see [Getting server logs](#) on page 143.
- From the Data Governance service machine, double-click the log file or right-click and select **Open** to view the log in the Log Viewer.

Applications and Services event logs

Severity error level events and audit events are written to the Applications and Services event logs on the Data Governance server under the "Data Governance" node.

- Severity error level errors have a "Source" of "Data Governance Edition".
- Audit events contain information on operations run by the server (such as security changes) and have a "Source" of "Data Governance Audit".

Data Governance agent deployment logs

Log name: <Agent name>_Agent.log

The agent deployment logs are stored as text files in the Agent Deployment Logs folder in the Data Governance service installation directory. For example: %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Server\Agent Deployment Logs\.

Used for capturing the agent deployment process for each individual agent. There is a separate agent deployment log for each agent installed in your Data Governance Edition deployment.

Agent deployment logs can be viewed as described below:

- In the Manager, use the **Get All Logs** task to export the agent deployment logs to a specified location. From that location, double-click the log file to view the log. For more information, see [Getting server logs](#) on page 143.
- From the Data Governance service machine, double-click the log file or right-click and select **Open** to view the log.

Data Governance agent logs

Log name: DataGovernance.Agent.exe.dlog

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the agent's dlog.config file on the host computer in the agent installation directory (%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services\<Agent instance directory>\dlog.config).
2. Open the configuration file and edit the following setting:

```
<rules>  
    <logger name="*" minlevel="INFO" writeTo="logfile">
```
3. Change INFO to DEBUG to get detailed logging.
4. Save the file.

No agent restart is required.

An agent log is stored as a Trace log document (.dlog) in a subfolder on the host computer in the agent installation folder. For example:

%ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services\DGE_<DeploymentName>_<HostDnsName>.

Used for logging communications, synchronization processes and data transfers between the Data Governance server and the agent.

Agent logs can be viewed as described below:

- From the Manager, use the **Export agent log** task to export the selected agent log to a specified location. From that location, double-click the log file to view the log in the Log Viewer. For more information, see [Exporting agent log](#) on page 143.
- From the agent machine, double-click the log file or right-click and select **Open** to view the log in the Log Viewer.

Web client logs

The Web client log files are located in the following directory:

C:\inetpub\wwwroot\IdentityManager\App_Data\Logs.

This directory contains a series of log files all named with a time stamp.

Errors encountered with the web client IT Shop are recorded to the web client logs.

The best way to get the proper log is to replicate the issue and take the file with the greatest timestamp.

Job server logs

The default URL for a Job Server log is: <http://JobServerHost:1880/Log>

Often when you have errors with Active Directory synchronization or report execution you can find clues in the One Identity Manager Job Server logs. In addition, errors encountered with the process chains used to process resource access requests in the IT Shop are recorded in the Job Server logs.

With a default configuration, you can browse these logs by launching a web browser and navigating to a specific URL on the computer hosting the Job Server.

Manager client log

Log name: QAM.Client.Log.dlog

If experiencing issues with Data Governance Edition inside the Manager client, enable the Data Governance Edition client side logging to determine if the issue is related to the user interface rather than the Data Governance server.

NOTE: By default, the logging level is set to INFO. To change the logging level to get detailed logging:

1. Locate the Data Governance Edition client log configuration file (%ProgramFiles%\One Identity\One Identity Manager\QAM.Client.Log.config).
2. Open the configuration file and edit the following setting:

```
<rules>  
    <logger name="*" minlevel="INFO" writeTo="logfile">
```

3. Change INFO to DEBUG to get detailed logging.
4. Save the file.

The Manager client log files are located in the user profile directory:

```
C:\Users\<Your User Name>\AppData\Local\One Identity\One Identity  
Manager\Manager
```

NOTE: To enable the latest LogView logging for the Manager client, modify the Manager configuration file (%ProgramFiles%\One Identity\One Identity Manager\Manager.exe.config) as follows:

Comment out the following:

```
<include file="{basedir}/globallog.config" ignoreErrors="true"/>
```

Add the following:

```
<include file="{basedir}/QAM.Client.Log.config" ignoreErrors="true"/>
```

Exporting agent log

From the **Agents** view in the Manager, you can export the agent log for the selected agents to a location of your choosing. The log files are exported through a background operation and will exist once the background operation has completed. The export operation can be viewed in the Background operations view.

To export an agent log

1. In the Navigation view, select **Data Governance | Agents**.
2. In the **Agents** view (right pane), select the required agents.
3. Select **Export agent log** from the Tasks view or right-click menu.
4. In the **Browse for folder** dialog, select the location where the exported logs are to be stored.

A compressed zip file is created in the location specified. Clicking this zip file displays a trace log document for the selected agents.
5. Double-click the .dlog file to display the log viewer to view an agent's log entries.

Getting server logs

From the **Managed hosts** view in the Manager you can export the server logs to a location of your choosing. The log files are exported through a background operation and will exist once the background operation has completed. The export operation can be viewed in the **Background operations** view.

NOTE: Server logs retrieved using the **Get All Logs** task consist of the DataGovernanceEdition.Service.exe.dlog file and associated agent deployment logs.

To get server logs

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. Select **Get All Logs** from the Tasks view or right-click menu.
3. In the **Browse for folder** dialog, select the location where the exported logs are to be stored.

A compressed zip file is created in the specified location. Clicking this zip file displays the Data Governance service log and an Agent Deployment Logs folder, which contains a log file for each agent deployed.
4. Double-click the Data Governance service .dlog file to display the log viewer to view the service's log.
5. Double-click an agent deployment log file to open Notepad to view the agent's deployment log.

Job queue shows that database needs to be compiled

On a new install or upgrade, upon Data Governance server startup, the job queue is placed on hold indicating that the database needs to be compiled.

Probable cause

The \TargetSystem\UNS\CreateNewRoot configuration setting must be enabled in order for a Data Governance Edition install to proceed successfully. If Data Governance Edition finds this setting to be disabled, it will mark it enabled; but the job queue will be placed on hold with a 'waiting for database compile' message.

As of Data Governance Edition 7.1, this configuration setting has been incorporated into the Settings.xml file. This Settings.xml file is distributed with One Identity Manager Data Governance Edition version 7.1 and when it is found to be enabled, the database compile step will proceed as expected as part of the installation process.

Resolution

Locate the Settings.xml file (C:\<Identity Manager Build>\Setup\Editions\DGE\settings.xml) and ensure the following SQL command is present:

```
<Command Type="Sql">  
    update DialogConfigParm  
    set Enabled = 1  
    where FullPath = 'TargetSystem\UNS\CreateNewRoot'  
</Command>
```

If it is not present, append this SQL command to the Settings.xml and run the DBCompiler.exe to remove the job queue hold. There should be no need to run the DBCompiler.exe on the next Data Governance Edition upgrade release.

If it is present, but set to disabled, run the DBCompiler.exe to remove the job queue hold.

Receiving unauthorized access violations

Probable cause

The employee is not configured properly.

Communication with the Data Governance server uses Windows Integrated authentication. Regardless of how you logged in to any client application ("viadmin"), calls to the Data Governance server are authenticated by looking at your interactive Windows login identity and finding an associated Employee record. The server validates the permissions and roles assigned to this Employee record, not the login that you used when connecting to the client application.

Cannot save the service account

Probable cause

You may receive one of the following errors: "Not Authorized to Use this Database" or "Access was denied while attempting to perform the requested operation" if you are logged in to the machine with an Active Directory account that does not have an associated employee and appropriate roles to view and manage hosts. This account is used to contact the Data Governance server.

NOTE: Both the System user (account logged on to the machine) and the Manager user (account running the Manager) must have an associated One Identity Manager Employee and must be assigned the appropriate Data Governance application roles.

Resolution

To associate an account with an employee

1. In the navigation view, select **Active Directory** (ADS button at bottom of navigation view).
2. Select **User accounts**, and select the account that you are currently logged in to the machine as.
3. In the Tasks view, select **Change master data**.
4. On the **General** tab, select an employee to associate with the account.

NOTE: Typically an Active Directory synchronization creates an employee for every Active Directory account and this association is already done.

The following application roles are specifically for Data Governance Edition. They are used with One Identity Manager application roles.

- **Data Governance | Access Managers**

Members of this role can access all information related to Data Governance Edition, and can query information from Data Governance agents. Also, they can modify the security of objects contained on managed hosts.

- **Data Governance | Administrators**

Members of this role can perform all administrative tasks necessary for the management of Data Governance Edition. This includes deploying and configuring

managed hosts, managing data access, editing security, and placing data under governance.

- **Data Governance | Business Owner**

Members of this role can view information on resources they own.

- **Data Governance | Direct Owners**

This role is held by accounts and roles marked as the owners of resources within Data Governance Edition.

| **NOTE:** This role cannot be assigned manually; it is assigned programmatically.

- **Data Governance | Managed Resources**

A default container used for roles automatically generated by Data Governance Edition managed resources. For more information on managed resources, see the *One Identity Manager Data Governance Edition IT Shop Resource Access Requests User Guide*.

- **Data Governance | Operators**

Members of this role have read-only access to the **Managed hosts** view and **Agents** view in the Manager.

- **Identity & Access Governance | Compliance & Security Officer**

Members of this role have a view into all security-related information collected by Data Governance Edition. They are responsible for ensuring security-related compliance regulations are being followed correctly.

To assign application roles

1. In the navigation view, select **Employees | Employees**.
2. In the **Employees** result list, double-click the required employee.
3. In the Task view, select **Assign One Identity Manager application roles**.
4. Apply the required application role, and save your changes. For example:
 - a. Expand **Data Governance** in the Add assignments window to view the application roles available.
 - b. Double-click **Administrators** to assign the **Data Governance | Administrators** role to the selected user account.
 - c. Click the **Save** toolbar button.
5. Restart the Data Governance service to renew the authentication cache. The cache is renewed automatically if you are not using the Manager for 5 minutes.

Cannot connect to a managed host

Probable cause

When trying to connect to a managed host you may receive the following error:
"There was no end-point listening that could accept the message."

This error indicates that there is an issue with the Data Governance service.

Resolution

To resolve this issue, open the Services snap-in and restart the One Identity Manager Data Governance Service, then select the managed host in the Navigation view.

DNS error when attempting to add a new managed host

When attempting to deploy a new managed host, the managed host status is "Unresolvable" and the following errors are logged to the Data Governance Edition Service log:

- ERROR: The domain in which the operation was attempted is not registered as a managed domain.
- ERROR: Expected DNS Host Name <DNS Host Name>. The value in Active Directory is <DNS Host Name in AD>.
- ERROR: Access is denied.

Probable cause

These errors are caused by a mismatch between the DNS name in Active Directory and the "expected" DNS Host Name. That is, when adding a remote agent or saving a local managed host, Data Governance Edition is comparing the following two values to ensure they are the same:

- DNSHostName property in Active Directory, which should be the same value in One Identity Manager after AD synchronization.
- Machine name of the agent device plus DNS name of the domain.

Resolution

To resolve this issue:

1. Have your Active Directory administrator change the DNSHostName value in Active Directory to the correct DNS name.

2. Re-synchronize Active Directory into One Identity Manager.
3. Deploy the managed host.

Agent not connecting to the Data Governance server

Probable cause

- The agent has not been able to find a Service Connection Point that points to a valid server.
- A firewall is active on the agent hosting computer, which is preventing the agent from connecting to the server.
- The proxy settings on the agent computer are preventing it from connecting to the server.

Resolution

- Ensure that the Service Connection Points of the agent computer's managed domain are OK.
- Ensure that the following registry value contains the required Deployment ID:
Registry Key: HKEY_LOCAL_MACHINE\Software\One Identity\Broadway\Agent\Services\communication
Registry Value: deploymentId (REG_SZ)
- Configure the firewall on the agent to allow outgoing traffic on TCP port 8721, and incoming traffic on TCP port 18530. Also, ensure that the Data Governance server firewall has the following exceptions configured: incoming TCP 8721, 8722 and outgoing 18530. If the Managed Host is a SharePoint Farm, HTTP port 3149 must be open for incoming traffic from localhost.
- 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.

Data Governance agents cannot access NAS devices via SMB

After adding an EMC or NetApp host machine to a domain running Windows Server 2012/2012 R2, you may encounter one or both of the following:

1. The Data Governance agent cannot access EMC or NetApp shares. For example, you receive a "Windows Cannot Access" network error when trying to access a share on the NAS device using the file explorer.
2. You cannot browse resources or set security index roots for an EMC or NetApp managed host. That is, after adding an EMC or NetApp managed host, the Data Status gets stuck in a "Waiting for scanning to start" state and an error is recorded in the agent log.

Probable cause

Both of these issues are related to known issues with Windows Server 2012/2012 R2 and Windows 8 clients. That is, Windows Server 2012 and later and Windows 8 and later include a newer version of the Server Message Block (SMB) protocol. These newer versions now ship with SMB 3.0 (originally known as SMB 2.2).

1. The first problem, where the agent cannot access EMC or NetApp shares, is most likely due to an incompatibility between your NAS device and the SMB protocol.
2. The second problem, where the agent cannot scan the NAS device, is due to the "Secure Negotiate" feature that was added to SMB 3.0 for Windows Server 2012 and Windows 8.

Resolution

1. To resolve the problem where the agent cannot access EMC or NetApp shares, upgrade the FLARE code on your NAS device with support for SMB 3.0.

WORKAROUND: If upgrading the FLARE code is not an option, disable SMB 2.0 on the agent machine running Windows Server 2012/2012 R2.

See <http://www.exaltedtechnology.com/windows-8-access-is-denied-to-network-shares-could-be-an-issue-with-smb-2-2-with-emc-celler-a-or-nas-device/> for more information on this known issue and how to disable SMB 2.0.

2. To resolve the problem where the agent cannot scan the NAS device, use an alternate supported operating system to host the agent to scan the EMC or NetApp filer or contact the file server vendor for an update that enables the file server to support Windows Server 2012 and Windows 8 clients.

WORKAROUND: Set "Secure Negotiate" to "enable if needed" using the following PowerShell command on the agent machine running Windows Server 2012/2012 R2:

```
Set-ItemProperty -Path  
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters"  
RequireSecureNegotiate -Value 2 -Force
```

NOTE: Using the "enable if needed" setting means that if the remote client is able to go secure, the Windows Server 2012/2012 R2 will use the secure negotiate feature, but if the remote client cannot go secure (like NetApp and EMC), then it will fallback.

Disabling the secure negotiate feature is NOT recommended by Microsoft.

See <https://support.microsoft.com/en-us/kb/2686098> for more details on this known issue.

Additional information

To determine the SMB version running on your server

1. Access the remote file server and run the following PowerShell command:
Get-SmbConnection
2. Look at the "Dialect" entry to see what version of SMB the client has negotiated with the file server.

For example, if the entry is 3.0, both the client and the server support that version of the SMB protocol.

Agent leases expiring

Probable cause

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

Resolution

- Ensure the One Identity Manager Data Governance Edition Agent service is running on the hosting computer.
- Under normal conditions, agent lease expired messages should resolve themselves; however, it may take the duration of the lease renewal to renew. By default, the lease renewal interval is set to five minutes.

Cannot add managed paths to my EMC server

Probable cause

When adding managed paths for an EMC server, you may receive the following error:
Resource: \\Server_Name\, Error Message: The network path was not found.
NetAPI32 Error: 53.

This error means that Data Governance Edition could not resolve the EMC server or any of the shares of the server.

Resolution

Review and verify that the DNS settings are up-to-date, ensure you can ping the EMC server, ensure that the proper ports are open, etc.

Reboot the server having the problem and try again.

No activity data

When you run a Resource Activity, Account Activity, or Perceived Owner report, you may not immediately see an action in the report that you know you have performed.

Probable cause

- There is lag time between when an action occurs, such as a file read or write, and when the data is sent from the agent to the server. This delay is dependent upon the following:
 - The aggregation setting on the **Resource Activity** page of the **Managed Host Settings** dialog
 - The update schedule. By default, resource activity is synchronized into the One Identity Manager database, once a day, after the first initial synchronization. The initial synchronization happens a few minutes after resource activity collection is enabled. This update schedule is controlled by a Data Governance server configuration setting (PerceivedOwnershipCalcUpdateRefreshIntervalMinutes). See the *One Identity Manager Data Governance Edition Technical Insight Guide* for more information on this configuration file setting.
 - Various internal processes.
- It is possible that you did not have resource activity collection enabled for that managed path during the time span covered in the report.
- If you have enabled resource activity collection, it is possible you have excluded some accounts, files or folders where the activity occurred.
- If Quest Change Auditor is installed and you are collecting resource activity directly from Change Auditor, Change Auditor may not be capturing the events you are expecting.

Resolution

- Verify the managed host type. Resource activity collection is only available for local managed Windows servers, SharePoint farms, and supported NetApp and EMC managed hosts.

- Use the **Edit Host Settings** task from the **Managed hosts** view to verify that the required paths are being managed:
 - Open the **Managed Paths** page of the **Managed Host Settings** dialog. Are the required managed paths listed?
- Use the **Edit Host Settings** task from the **Managed hosts** view to verify that resource activity collection is enabled:
 - Open the **Resource Activity** page of the **Managed Host Settings** dialog.
 - Is the **Collect and aggregate events** option selected?
 - Are the required events selected?
- Verify the accounts, files or folders that are being tracked
 - Click the **Resource Activity Exclusions** button on the **Resource Activity** page of the **Managed Host Settings** dialog.
 - Check each tab to see what objects are being excluded.
- Collaborate with the Change Auditor administrator to determine what data Change Auditor is collecting.

No activity data available for SharePoint 2010 managed host

Probable Cause

For SharePoint 2010 managed hosts, the DataGovernance.SharePointShim.exe process is required and may not be running on the SharePoint server.

NOTE: For multi-agent SharePoint 2010 managed hosts, you will see multiple Shim instances; one for each agent service.

Resolution

Check to ensure that the DataGovernance.SharePointShim.exe process is running on the SharePoint 2010 farm server. If it is not running, start the process or restart the agent.

To start the Shim process

Since multiple Shim instances are displayed for multi-agent SharePoint managed hosts, you must provide the PID of the corresponding Data Governance SharePoint agent as an argument when starting up the Shim process for an agent service.

1. In **Task Manager | Services** tab, locate the PID assigned to the agent service that does not have activity available.
2. At the command prompt, enter the following PowerShell command to start the Shim instance:

C:\Program Files\One Identity\One Identity Manager Data Governance Edition\Agent Services\DataGovernance.SharePointShim.exe <PID>

NOTE: This only applies to SharePoint 2010 because in later releases of SharePoint, this is not a separate process.

Resource activity is not displaying in the web portal for a business owner

Probable cause

Activity for owned data may not display in the web portal if:

- Resource activity collection has not been enabled on the selected managed host.
- Resource activity collection is not supported on the selected managed host (such as, remote managed Windows computers, Windows clusters, Generic or Cloud managed hosts).
- Resource activity collection is enabled, but the data is not included within a specified managed paths.

Resolution

To ensure resource activity is being collected:

1. From the **Managed hosts** view, select the required managed host.
2. Select **Edit host settings** from the Tasks view or right-click menu.
3. In the **Managed Host Settings** dialog, open the **Resource Activity** page.
4. Ensure **Collect and aggregate events** is selected.
5. Also, ensure the appropriate events are selected.
6. Click the **Resource Activity Exclusion** button and review each tab to see what objects are being excluded.

To check what managed paths are selected for activity collection:

1. From the **Managed hosts** view, select the required managed host.
2. Select **Edit host settings** from the Tasks view or right-click menu.
3. In the **Managed Host Settings** dialog, open the **Managed Paths** page.
4. Activity is only being collected for the paths listed on this page.

NOTE: For all managed host types, when placing a resource under governance, the resource must be a managed path or a folder or share under a managed path.

- For remote managed hosts and SharePoint managed hosts, if you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. If the managed host has more than one agent assigned, you are prompted to select the agent to which the managed path is added.
- For local managed hosts, if you are scanning managed paths (that is, there are paths in the managed paths list), and you select to place a resource under governance that is not yet defined as a managed path, the path is automatically added to the managed paths list. However, if you are scanning the entire server (that is, the managed paths list is empty) and you place a resource under governance, no changes are made to the managed paths list and you continue to scan the entire server.

For more information about these pages on the **Managed Host Settings** dialog, see [Managed paths page](#) on page 106 and [Resource activity page](#) on page 110.

Governed resources are missing from the All my resources view in the web portal

Probable cause

Business ownership for governed resources was set programmatically or through the Object Browser.

Resolution

If business ownership for governed resources is set programmatically or through the Object Browser, you must also set the following parameter for these governed resources:

QAMDuG.IsPointOfInterest = true.

NOTE: Business ownership is indicated by setting values for either QAMDuG.UID_PersonResponsible or QAMDuG.UID_AERoleOwner.

Not receiving scheduled reports

Probable cause

The One Identity Manager service (job server) is not configured correctly. If you are having issues with scheduled report execution and are not receiving your reports through email, the first place to check is the Job Server log.

Resolution

Scheduled reports are run by the job server with the SMTP Host server mask. To allow this job server to query the Data Governance server, it must be running as an Active Directory account with an associated One Identity Manager Employee with either the **Data Governance | Administrators** or **Data Governance | Access Managers** application role.

To change the identity the job server runs as, open the Services console on the computer hosting the job server and change the Log On identity. For example, the DGEAdministrator Active Directory account needs to be associated with an Employee record that was granted the **Data Governance | Administrators** role or be a Data Governance service account itself. This new identity allows the job server to authenticate against the Data Governance server and perform the necessary queries required for report execution.

Groups missing from the Group Memberships tree view

To examine group membership in your enterprise, Data Governance Edition requires credentials that allow it to read group memberships in the domains that make up your enterprise structure. These credentials are provided when syncing the domain for Active Directory. For SharePoint group membership, it uses the provided database connection string and reads group information from the SharePoint database. If Data Governance Edition is having trouble resolving group memberships, you will see a link in the lower-left pane (after having selected Manage Access from the client). Clicking this link displays a list of issues that details any problems encountered during group expansion.

Resolution

- Ensure that you have provided credentials with the required access.

NetApp managed host deployment

Understanding the following aspects of the deployment process are key to ensuring a successful deployment of NetApp managed hosts:

- [Permissions required to access NetApp filer](#)
- [Data Governance agent deployment](#)
- [FPolicy deployment](#)
- [Managed host configuration options](#)
- [Performance considerations](#)
- [Compatibility with Change Auditor for NetApp](#)

Permissions required to access NetApp filer

The service account for the remote agent responsible for scanning the NetApp filer must meet the following minimum permissions:

- Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.)
- Must be a member of the local Administrators group on the NetApp filer.
- Must have permissions to access the folders being scanned.

Data Governance agent deployment

NetApp filers are added to a Data Governance Edition deployment as managed hosts with remote agents. When selecting an agent for scanning a NetApp filer, take the following into consideration:

- The remote agent must be hosted on a machine in the same domain as the NetApp filer device.

NOTE: If you host a remote agent in an external domain to monitor a filer, the agent will NOT record the resource activity data.

- There should be a good network connection between the NetApp filer and the monitoring agent servers.
- The machine hosting the agent for NetApp can host agents for other servers, but those servers should be close to the agent host.
- If the NetApp is split up into multiple domains, you must deploy one or more agents for each domain.

FPolicy deployment

FPolicy is required for Data Governance Edition to capture real-time security updates and to collect resource activity. In order to use FPolicy on NetApp 7-Mode managed hosts, CIFS file system protocol must be enabled.

When adding a NetApp 7-Mode managed host, you can use one of the following for FPolicy deployment:

- automatic FPolicy deployment
- use a pre-created FPolicy

However, for NetApp Cluster Mode managed hosts, FPolicy deployment is always automatic.

Using automatic FPolicy deployment for NetApp 7-Mode

When you add a NetApp managed host, an FPolicy is created if either of the following managed host settings are enabled:

- **Collect activity for real-time security updates** on the Security Scanning page
- **Collect and aggregate events** on the Resource Activity page

When you deploy an agent, an empty FPolicy (with no monitored operations) is created by the Data Governance server (performed as the service account for the domain). When the agent starts, it registers with the FPolicy as an FPolicy Server. At the point of registration, the agent will register the operations it will monitor.

NOTE: If another agent is added to the managed host to index a separate root on the NetApp device, a new FPolicy will be created (named after the new agent ID).

The FPolicy:

- is created using the credentials of the domain service account.
- is named after the agent ID (that is, DGE_ <DeploymentName>_<FQDN of managed host>).
- is configured to use the version 2 interface.
- includes cifs_set_attr information, which allows Data Governance Edition to receive notification of security changes.
- sets the cifs_setattr option to on (defaults to off in FPolicy).
- is asynchronous.

NOTE: To view all the existing F Policies on a NetApp device, establish a Telnet or SSH connection to the filer device, log in and type the following at the OnTap command line: "fpolicy".

NOTE: When you remove an agent, the FPolicy is deleted.

Using a pre-created FPolicy on a NetApp 7-Mode filer

Data Governance Edition can be configured to connect to a pre-created FPolicy. The following steps are required to configure Data Governance Edition to use a manually created FPolicy instead of automatic deployment:

- Enable CIFS FPolicy on NetApp filer
- Create FPolicy on the filer
- Configure the Data Governance server and agent

To enable CIFS FPolicy on a NetApp filer

- Run options FPolicy.enable on

To create FPolicy on the filer

- fpolicy create <PolicyName> Screen
- fpolicy enable <PolicyName>

To configure the Data Governance server and agent

1. Configure the Data Governance server to prevent the creation of FPolicy on the required NetApp filer:
 - a. Create the following registry key: "HKEY_LOCAL_MACHINE\SOFTWARE\One Identity\Broadway\Server\ManualFPolicyCreation".
 - b. Add a string value with the fully qualified domain name of the NetApp filer.
2. In the Manager, deploy a NetApp managed host.

NOTE: Ensure that the registry key has been created on the server before deploying the agent.

3. Configure the NetApp agent to use the manually pre-created FPolicy.
 - a. Stop the agent service.
 - b. Locate the following configuration setting in the %Program Files%\One Identity\One Identity Manager Data Governance Edition\Agent Services\DataGovernance.Agent.exe.config file.

```
<"Agent">
  <"Services">
    <"ChangeMonitoring">
      <Setting name="OverrideFPolicyName">
```
 - c. Add a string value with the FPolicy name you want the specified agent to register with.
 - d. Save the configuration file.
 - e. Restart the agent.

FPolicy deployment for NetApp Cluster Mode

FPolicy deployment for NetApp Cluster Mode is always automatic and is done by the agent at run time because of the use of dynamic ports. The FPolicy will be deleted when the agent stops. You cannot specify a pre-created FPolicy.

Managed host configuration options

During the configuration of the managed host:

- Select the required shares (managed paths) to scan.
- (Optional) Select to **Collect activity for real-time security updates**.
- (Optional) Select to **Collect and aggregate resource activity**.

When you add an agent, the managed host properties impact whether FPolicy is deployed, and what properties are set within the FPolicy itself:

- If both **Collect activity for real-time security updates** and **Collect and aggregate activity** are disabled on the managed host, FPolicy will not be created when the agent is deployed.
- If **Collect activity for real-time security updates** or **Collect and aggregate activity** is enabled, FPolicy will be created; however, there will be no registered settings until the agent starts up and receives the updated settings from the Data Governance servers.
- The agent must start its security scan before it registers with FPolicy. This means that managed paths must be set and the agent must hit its configured scanning schedule. (To force this scan, select the **Immediately scan on agent restart or when managed paths change** option and restart the agent.)

Monitored events

The following events are tracked on files and folders, as well as the identities associated with those events, when real-time security updates and/or resource activity collection is enabled:

- File create
- File rename
- File delete
- File write
- File open
- Setattr (Security changes including DACL, and Owner changes)
- Directory rename
- Directory delete
- Directory create

Performance considerations

Enabling FPolicy on NetApp filers may impact system performance. Data Governance Edition uses 'async' mode and does not inspect any file data to try and minimize the performance impact. However, every event does require a round trip network request between the NetApp filer and the Data Governance agent.

Are rescans of all directory structures required to detect change?

To have Data Governance Edition watch for security changes, real-time security updates must be enabled. That is, select the **Collect activity for real-time security updates** option at the bottom of the **Security Scanning** page on the **Managed Hosts Settings** dialog for the target managed host. This will cause the FPolicy to be deployed and the security index to be updated when changes to the structure and security of the file system on the target managed host occur.

Compatibility with Change Auditor for NetApp

If you are using Quest Change Auditor for NetApp to monitor a filer that is also being scanned by Data Governance Edition, you have two options available.

Option 1: Collect activity directly from the Change Auditor database

When Change Auditor is installed, you can configure Data Governance Edition to collect resource activity directly from Change Auditor. When enabled, Change Auditor collects the selected activity events every 15 minutes on all managed hosts. The events received from Change Auditor are harvested by the Data Governance server, aggregated and placed directly into the Data Governance Resource Activity database.

When using Change Auditor to collect resource activity, NetApp managed hosts will not place an FPolicy for Data Governance Edition on the NetApp filer.

In addition, when using Change Auditor to collect resource activity, it is recommended to clear the **Collect activity for real-time security updates** option for NetApp managed hosts. The agents managing these host types should be configured to scan on a schedule and not run once. The performance gain in using Change Auditor's event collection will be lost if the Data Governance agent is also collecting activity from these storage devices for security updates.

For more information on configuring Data Governance Edition to collect resource activity directly from Change Auditor, see [Configuring Change Auditor to collect resource activity](#) on page 55

Option 2: Collect activity using Data Governance Edition

You can use Data Governance Edition to collect resource activity; however, for NetApp 7-Mode managed hosts, you must disable real-time security monitoring. You can disable security monitoring from the Resource Activity tab of the **Managed Host Settings** dialog.

To disable security monitoring

NOTE: This approach has the effect of setting the NetApp FPolicy option `cifs_setattr` to off.

You can verify this by running the following command on the NetApp filer: `>fpolicy options <Agent instance>`

Where `<Agent instance>` is in the following format: `DGE_<DeploymentName>_<FQDN of managed host>`

You will still see `setattr` as a monitored operation in FPolicy.

1. In the Navigation view, select **Data Governance | Managed hosts**.
2. In the **Managed hosts** view, select the required managed host.
3. Select **Edit host settings** in the Tasks view or right-click menu.
4. Open the **Resource Activity** page of the **Managed Hosts Setting** dialog and click the check box to clear the **Security change** event.
5. After making the required change, click **OK** to save your selections and close the dialog.

NOTE: This will need to be completed for every NetApp agent. If it is necessary to disable "Security change" due to compatibility settings with Change Auditor for NetApp, ensure the Resource Activity setting is modified prior to the start of the agent scan.

EMC managed host deployment

EMC storage devices are added to the Data Governance Edition deployment as managed hosts with remote agents. Due to the EMC architecture, you must complete the following procedures when you add an EMC storage device as a managed host.

- [Configuring CEE framework](#)
- [Creating the cepp.conf file \(Celerra or VNX devices\)](#)
- [Enabling system configuration auditing \(Isilon devices\)](#)

Configuring CEE framework

Data Governance Edition 7.0.2 (and higher) requires the EMC Common Event Enabler (CEE) 7.1 (or higher) framework to collect resource activity from an EMC storage device. The Data Governance agent will register with EMC CEE as a VCAPS endpoint. EMC CEE must be installed on the same server as the Data Governance agent. If you are collecting resource activity from the EMC storage device, you can only specify one agent to manage the EMC host.

To configure CEE framework

- Install the EMC CEE framework on one or more Windows servers.

| NOTE: EMC CEE must be installed on the same server as the Data Governance agent.

Next steps:

- For Celerra and VNX storage devices, create and configure the cepp.conf file. For more information, see [Creating the cepp.conf file \(Celerra or VNX devices\)](#) on page 163.
- For Isilon storage devices, enable system configuration auditing. For more information, see [Enabling system configuration auditing \(Isilon devices\)](#) on page 164.

Creating the cepp.conf file (Celerra or VNX devices)

You must create a configuration file (cepp.conf file) before using the CEPA auditing feature to monitor file system activity on EMC Celerra or VNX storage devices. The cepp.conf file contains the information needed to connect Data Movers to the Windows computers where the CEE software is installed. It also defines the type of file system events that Data Governance Edition can collect from the EMC device.

To create and configure cepp.conf file

1. Using an SSH client (such as Putty.exe), connect to Control Station using its IP and port (the default is 22).
2. Login using administrative credentials. The default user name and password on a Celerra system are nasadmin/nasadmin.
3. Copy or create the cepp.conf file.
 - To copy the current configuration file from the Data Mover, run the following command: `server_file movername -get.cepp.conf cepp.conf`
Where: *movername* is the name of your Data Mover. The default name is `server_2`.
 - To create the configuration file, open the VI text editor (or other preferred text editor) by running the following command: `vi cepp.conf`
4. Using the text editor, edit the cepp.conf file and ensure the following configuration parameters are in the file:

```
pool name=poolname servers=server1|server2 postevents=event1|event2|...
```

Where: *poolname* is the name assigned to the set of Windows servers where the Event Enabler software from EMC is installed.

Where: *server1|server2* is the fully-qualified domain name of the Windows computers hosting the Event Enabler (CEE) software from EMC. If you have more than one server, separate them with a vertical bar (|).

Where: *event1|event2|...* are the EMC events to be collected during security scans and activity collection. When specifying multiple events, separate them with a vertical bar (|).

NOTE: Do not register for pre-events or post-err-events in the cepp.conf. These events are ignored by the Data Governance agent and add undue load on the EMC device.

The following table shows events (postevents=) that can be registered in the cepp.conf and their mapping to Data Governance events that can be collected during security scanning and activity tracking.

EMC cepp.conf event	Data Governance Edition event
CreateFile CreateDir	Create
DeleteFile DeleteDir	Delete
RenameDir	Rename
SetAcIFile SetAcIDir	SecurityChange
CloseModified	Write
CloseUnmodified	Read

NOTE: If you configure your EMC managed host to collect real-time security changes and apply them to scanned data, you must include the following events:

...postevents=CreateFile|CreateDir|DeleteFile|DeleteDir|RenameDir|SetAcIFile|SetAcIDir

For performance reasons, you may want to filter out the events that are not required, such as CloseUnmodified which are the "Read" events.

5. Save the file. (Press **Escape** then type :wq)
6. Run the following commands in the SSH client to publish the file to the Data Mover and restart the CEPA facility:

```
server_cepp movername -service -stop
server_file movername -put cepp.conf cepp.conf
server_cepp movername -service -start
```

Where: *movername* is the name of your Data Mover. The default name is server_2.

7. Verify the CEPA status by running the following command:

```
server_cepp movername -service -status
```
8. Verify the pool configuration by running the following command:

```
server_cepp movername -pool -info
```

Enabling system configuration auditing (Isilon devices)

EMC Isilon devices do not use the cepp.conf file; however, you must enable configuration change auditing and protocol access auditing in order for Data Governance Edition to perform security scans and collect resource activity on the EMC storage device.

NOTE: On the Data Governance server and all agent servers, you must have a Trusted Root Certificate Authority certificate to validate the Isilon server's HTTP certificate.

To enable auditing (OneFS web interface)

1. Connect to the OneFS web interface.
2. Select **Cluster Management**.
3. Select **Auditing**.
4. In the **Settings** pane, select the following check boxes:
 - **Enable Configuration Change Auditing**
 - **Enable Protocol Access Auditing**
5. In the **Audited Zones** pane, add the zones to be audited:
 - Click the **Add Zones** button to add a zone.
6. In the **Event Forwarding** pane, enter the following information:
 - **CEE Server URIs**: Enter the uniform resource identifier (URI) for the Windows server hosting the Common Event Enabler (CEE) software.
Use the following format: `http://<FullyQualifiedDomainName>:<Port>/cee`.
For example: `http://server.test.abc.com:12228/cee`
The default CEE HTTP port is 12228.
Click the **Add another input field** to add additional CEE server URIs.
 - **Storage Cluster Name**: Enter the resolved name of the EMC Isilon cluster.
Use the following format: `<ClusterName>.<DomainName>.com`
For example: `Cluster1.test.abc.com`
7. Click **Save Changes**.

SharePoint Farm managed host deployment

SharePoint farms are similar to remote managed hosts in that they require an associated service account, even though they are installed locally on a SharePoint server. In addition, you can configure the level of auditing you want to perform on SharePoint farms.

- [Permissions required to access SharePoint farms](#)
- [Configure SharePoint to track resource activity](#)

Permissions required to access SharePoint farms

SharePoint farms are similar to remote managed hosts in that they require a service account with sufficient permissions to access the data, even though they are installed locally. The service account for the agent managing SharePoint farms, must meet the following minimum permissions:

- Must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One Identity Manager service (job server)).
- Must be a member of the administrators group on the SharePoint server.
- Log On as a Service local user rights on the agent computer. (This is automatically granted when the agent is deployed.)

Configure SharePoint to track resource activity

To gather and report on resource activity in SharePoint, ensure that SharePoint native auditing is properly configured for any resources of interest. You can also optionally install

the SharePoint Auditing Monitor farm solution to obtain activity for events not available in the native SharePoint auditing system.

- [Configure auditing on SharePoint farms](#)
- [Install the QAM.SharePoint.Auditing.Monitor farm solution](#)
- [Map SharePoint events to Data Governance events](#)

Configure auditing on SharePoint farms

You can enable auditing at different levels in the SharePoint farm. It is recommended that you enable auditing at the site collection level to ensure that all events are collected. The methods available for configuring auditing vary depending on the SharePoint edition installed. Sometimes, you can use Central Administration; in all cases you can use Windows PowerShell. It is recommended that you enable all SharePoint native events to ensure maximum coverage for data governance activities, but you may select a smaller set to improve performance if necessary.

Consult your Microsoft documentation for complete information on configuring auditing.

Install the QAM.SharePoint.Auditing.Monitor farm solution

If you install the SharePoint farm solution, you can supplement the events captured by native auditing. Install "QAM.SharePoint.Auditing.Monitor.wsp" from the agent installation folder (by default %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition\Agent Services.) Consult your Microsoft documentation for information on installing a farm solution.

NOTE: You must enable SharePoint native auditing. The farm solution is not a replacement for native auditing, it is an enhancement.

This farm solution captures some events that are unavailable through native SharePoint auditing, specifically:

- Adding a folder
- Adding a library
- Renaming a list or library
- Creating a site

Map SharePoint events to Data Governance events

When you track resource activity using Data Governance Edition, the results appear in views, reports, and dashboards. To simplify things, SharePoint events are grouped for easier reporting. The following table outlines the events you see in your reports, and the corresponding SharePoint events.

Table 28: Mapping Data Governance events to native SharePoint events

Data Governance events	Native SharePoint events
Create	Undelete Item copied Item added
Delete	Item deleted
Rename	Item restored from Recycle Bin
Read	Checkout View
Security Change	Audit mask change Inheritance breakage Inheritance restore Permission level granted Permission level revoked
Write	Item checked in Item moved Item renamed Item updated Version deletion Version restored Item updated Attachment added

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit <https://www.oneidentity.com/company/contact-us.aspx>.

Technical support resources

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

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

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

A

Active Directory permissions 29

Active Directory synchronization project 51

add

 Data Governance Edition to One Identity Manager deployment 45

 managed domain 61

 service account 60

add managed hosts

 cloud 93

 distributed file system (DFS) root 77

 EMC CIFS device 86

 EMC Isilon NFS devices 89

 generic 73

 local Windows computer 68

 NetApp CIFS device 82

 NetApp NFS devices 89

 remote Windows computer 71

 SharePoint farm 78

 Windows cluster 71

Agent leases expiring 150

agent not connecting to the Data Governance server 148

agent service 11

Applications and service event logs 140

apply hotfix 133

AppServer

 Active Directory account 28

 auto-update 125

 modify appliance pool identity 57

architecture 9

assign employee to cloud account 53

assign employee to UNIX account 52

B

before you upgrade 126

C

cannot add managed paths to EMC server 150

cannot connect to a managed host 147

cannot save service account 145

CEE framework 162

cepp.conf file 163

Change Auditor

 compatibility with NetApp managed hosts 160

 configure to collect resource activity 55

check agent status 120

Cloud

 add managed host 93

 assign employee to cloud account 53

 cloud providers supported for scanning 26

 configurable managed host settings 99

 specify administrator account login credentials 104

collect resource activity 110

configurable managed host settings 96

custom agent registry settings upgrade considerations 128

- custom configuration settings upgrade considerations 128
- customize default host settings 115

D

Data Governance agent

- deployment
 - best practices 63
 - methods 65
 - pre-flight check 65
- deployment logs 140
- difference between local and remote agents 62
- errors 122
- lease information 64
- leases expiring 150
- logs 140
- NetApp filers 156
- overview 62
- remove with managed hosts 123, 135
- remove without removing managed host 124
- restart 123
- service 11
- states 120
- system requirements 21
- upgrade considerations 127

- Data Governance agents cannot access NAS devices via SMB 148

- Data Governance Configuration wizard 36-37

- log 139

Data Governance Edition

- agent service 11
- architecture 9

- components 9
- connector flag 51
- installation 32
- key processes 8
- logs 139
- minimum permissions 26
- overview 7
- ports 30
- service 11
- upgrade 125

Data Governance server

- log 139
- system requirements 15

Data Governance service

- deploying multiple services 41
- deployment methods 36
- deployment pre-flight check 35
- deployment procedure 37
- uninstall 136

- data states 119

Database server

- system requirements 16

- default host settings 115

- delete service accounts 136

deployment

- best practices for deploying agents 63

methods

- Data Governance agent 65
- Data Governance service 36
- Resource Activity database 36

- overview 13

pre-flight check

- Data Governance agent 65
- Data Governance service 35

- procedure
 - Data Governance service 37
 - multiple Data Governance services 41
 - Resource Activity database 37
- requirements
 - Data Governance agent 21
 - Data Governance server 15
 - Database server 16
 - Resource Activity database server 22
- determine state of data 119
- DFS root
 - add managed host 77
 - configurable managed host settings 99
 - versions supported for scanning 26

E

- edit
 - managed host settings 114
 - service account 60
- EMC
 - configure CEE framework 162
 - create cepp.conf file 163
 - limitations with collecting resource activity 110
 - upgrade considerations 127
- EMC CIFS devices
 - add managed hosts 86
 - configurable managed host settings 98
 - versions supported for scanning 24
- EMC Isilon
 - enable system configuration auditing 164

- service account 28
- EMC Isilon NFS devices
 - add managed host 89
 - configurable managed host settings 98
 - specify NIS server 103
 - versions supported for scanning 25
- error
 - Access was denied while attempting to perform the requested operation error 145
 - Not authorized to use this database 145
 - There was no end-point listening that could accept the message 147
 - Windows cannot access 148
- export
 - agent log 143

F

- FPolicy deployment 157

G

- generic managed host
 - add 73
 - configurable settings 99
- get server logs 143
- groups missing from Group Membership tree view 155

H

- hotfix, apply 133
- how does Data Governance Edition work 9

I

- install
 - post installation configuration 49
- install Data Governance Edition 32

J

- job queue shows that database needs to be compiled 144
- job server
 - account used for scheduling reports 28
 - Data Governance connector flag 51
 - logs 141

L

- local agent 62
- local Windows computer
 - add managed host 68
 - configurable managed host settings 97
 - service account 27
- logs
 - applications and service event 140
 - Data Governance agent 140
 - Data Governance agent deployment 140
 - Data Governance configuration wizard 139
 - Data Governance server 139
 - export agent log 143
 - get server logs 143
 - job server 141
 - Manager client 142
 - web client 141

M

- managed domain
 - add 61
 - authentication overview 59
 - service account 27
- Managed host settings dialog 100
 - Agents page 105
 - Cloud Provider page 104
 - Credentials page 103
 - edit settings 114
 - Managed paths page 106
 - NIS Host page 103
 - Resource activity page 110
 - Security Scanning page 107
- managed hosts
 - configuration settings 96
 - configure agents 105
 - configure resource activity collection settings 110
 - customize default host settings 115
 - define when to perform security scan 107
 - edit settings 114
 - NetApp configuration options 159
 - overview 62
 - remove 123, 135
 - specify managed paths 106
 - system status 117
- managed paths 106
 - cannot add managed paths to EMC server 150
- Manager
 - client log 142
 - user permissions 27

- map SharePoint events to Data Governance events 168
- modify application pool identity 57
- move SPN in Active Directory 49
- multiple Data Governance services deployment 41

N

NetApp

- compatibility with Change Auditor for NetApp 160
- Data Governance agent deployment 156
- FPolicy deployment 157
- managed host configuration options 159
- performance considerations 160
- permissions required to access NetApp filer 156
- service account 28

NetApp CIFS devices

- add managed host 82
- configurable managed hosts settings 97
- versions supported for scanning 23

NetApp NFS devices

- add managed host 89
- configurable managed host settings 97
- specify NIS sever 103
- versions supported for scanning 24

network communications

- ports 30

NFS Export resource 52

NFS managed hosts

- upgrade considerations 129

NIS server 103

- no activity data 151

- no activity data available for SharePoint 2010 managed host 152

- no communication from agent state 64

- not receiving scheduled reports 154

O

One Identity Manager

- Application Server 57
- database configuration 53
- database encryption 58
- service 12
 - account 28
 - Data Governance connector flag 51
- service account 27
- synchronization projects 51

One Identity Manager Database system requirements

- upgrade considerations 126

OneFS web interface 164

P

permissions 26

- granting Active Directory permissions 29
- granting SQL Server permissions 28
- NetApp filer requirements 156
- SharePoint farms 166

ports 30

post installation configuration 49

- assign employee to cloud account 53
- assign employee to UNIX account 52
- configure Change Auditor to collect resource activity 55

- Data Governance Edition
 - components 50
 - move SPN in Active Directory 49
 - One Identity Manager Appliance Server 57
 - One Identity Manager database configuration 53
 - One Identity Manager database encryption 58
 - One Identity Manager service
 - Data Governance connection flag 51
 - One identity Manager synchronization projects 51
 - previously governed or published files
 - upgrade considerations 129
- R**
- receiving unauthorized access violations 144
 - remote agent 62
 - remote Windows computer
 - add managed host 71
 - configurable managed host settings 97
 - service account 27
 - remove
 - agents 124
 - managed hosts 123, 135
 - sequence to remove components 135
 - service account assignments 136
 - service accounts 136
 - resource activity collection 110
 - configure SharePoint to track resource activity 166
 - Resource Activity database
 - deployment methods 36
 - deployment procedure 37
 - system requirements 22
 - uninstall 137
 - resource activity not displaying in web portal for business owner 153
 - restart agents 123
- S**
- security scanning 107
 - service account
 - add 60
 - authentication overview 59
 - delete 136
 - edit 60
 - EMC Isilon managed hosts 28
 - local Windows managed hosts 27
 - managed domain 27
 - NetApp managed hosts 28
 - remote Windows managed hosts 27
 - remove assignments 136
 - SharePoint managed hosts 27
 - SQL account for One Identity Manager database 27
 - SQL account for Resource Activity database 27
 - services
 - Data Governance agent 11
 - Data Governance Edition service 11
 - One Identity Manager 12
 - SharePoint
 - add a managed host 78
 - configurable managed host settings 98
 - configure SharePoint to track resource activity 166
 - map events to Data Governance

- events 168
- no activity data available for
SharePoint 2010 managed
host 152
- permissions required to access
SharePoint farms 166
- service account 27
- versions supported for scanning 25
- SharePoint synchronization project 51
- SQL Server permissions 28
- SQL service account
 - Data Governance Resource Activity
database 27
- system requirements
 - Data Governance agent 21
 - Data Governance server 15
 - Database server 16
 - ports 30
 - Resource Activity database server 22
- System user permissions 26
- systems that can be scanned 22

T

- target systems that can be scanned 22
- troubleshooting
 - agent leases expiring 150
 - agent not connecting to the Data
Governance server 148
 - cannot add managed paths to EMC
server 150
 - cannot connect to a managed
host 147
 - cannot save service account 145
 - Data Governance agents cannot
access NAS devices via
SMB 148
 - groups missing from Group Member-

- ships tree view 155
- job queue shows that database needs
to be compiled 144
- no activity data 151
- no activity data available for
SharePoint 2010 managed
host 152
- not receiving scheduled reports 154
- receiving unauthorized access viola-
tions 144
- resource activity not displaying in
web portal for business
owner 153

U

- unauthorized access violations 144
- uninstall
 - Data Governance service 136
 - Resource Activity database 137
- UNIX object synchronization project 51
- update
 - One Identity Manager to add Data
Governance Edition 45
- upgrade
 - agent system requirements 127
 - apply hotfix 133
 - before you upgrade 126
 - custom agent registry settings 128
 - custom configuration settings 128
 - Data Governance Edition 125
 - EMC system requirements 127
 - NFS managed hosts 129
 - One Identity Manager Database
system requirements 126
 - previously governed or published
files 129
 - procedure 129

V

verify managed host system status 117

view

agent errors 122

W

web client logs 141

web portal

auto-update 125

Windows cluster

add a remote managed host 71

configurable managed host
settings 97

versions supported for scanning 22

Windows installer 36

Windows Server

versions supported for scanning 22