One Identity Manager Data Governance Edition 8.1

Release Notes

February 2019

These release notes provide information about the One Identity Manager Data Governance Edition 8.1 release.

About this release

One Identity Manager Data Governance Edition enables security administrators and business owners to manage user access to unstructured data on files/folders/shares for Windows Server, NAS devices and SharePoint. It leverages the One Identity Manager platform for providing integrated self-service request portal, segregation of duties policies, attestation and re-certification workflows.

Using Data Governance Edition, IT Administrators are provided with management capabilities that enable them to see who is using data in the organization and how access should be modified to best fit the business. Specifically, they can:

- Examine a file system, SharePoint farm or other supported platforms to see what users and groups have access to it, and modify the access if required.
- Examine a user or group to ensure they have the correct data access.
- Investigate access for a user in a particular role within your organization to help grant the same access to a new hire.
- Evaluate a group's access before deleting it.
- Compare account access and simulate the addition and removal of users or groups from groups.
- Calculate perceived owners to identify potential business owners for data within your environment.

- Place data under governance and leverage the self-service requests, attestations, policies, and reports that help you to ensure your data is in compliance.

Through workflows that cross both the Manager and the Web Portal, users can:

- Manage access to and governance of Windows Server, NAS devices, SharePoint resources, and certain Cloud resources.
- Perform access modeling to compare user accounts/groups to identify the impact of adding/removing users to/from groups and identify why employees in the same department have different access rights.
- View how access was achieved, who requested it, who approved or denied it. This information is useful to verify during the attestation process.
- Define access policies including Separation of Duties to assist in fulfilling security and compliance requirements around data protection.
- Manage access as a business owner, an administrator or a security officer through dashboards and views.
- Review user and resource activity to identify patterns of usage, spot atypical behavior, and determine business owners to ensure that users have only the access to what they absolutely need, and nothing more.
- Use an access request workflow which allows business owners to grant or deny resource access and recommend a group for fulfillment from the list of best fit groups suggested by the system – thereby improving efficiency and reducing IT burden.
- Identify data without owners, suggest potential business owners, and allow compliance teams to schedule a process for business owners to verify and attest to employee access as well as enable the immediate remediation.
- Access pre-defined reports to help you identify, summarize, and analyze resource and account access and activity throughout your organization.

Data Governance Edition 8.1 is a minor release that provides compatibility with One Identity Manager 8.1. There are no enhancements or new features in this version of Data Governance Edition. See Resolved issues for a list of fixes included in this release.

Deprecated features

The following is a list of features that are no longer supported in Data Governance Edition 8.1.

- Oracle Database support: One Identity Manager no longer supports Oracle Database systems for hosting the One Identity Manager database. Therefore, the following settings and parameters are no longer supported in Data Governance Edition and should not be used:
  - ActivityCompression utility parameter: - DatabasePlatformOracle <string>
  - ActivityDeletion utility parameter: -DatabasePlatformOracle <string>

- Data Governance service configuration file setting: OracleBulkImportBatchSize
- Data Governance service registry settings:
  - Q1IMDBPlatformOracle
  - QDGDBPlatformOracle
- PowerShell command parameters:
  - -IdentityManagerIsOracle (Initialize-QDataGovernanceServer)
  - -ActivityDatabaseIsOracle (Initialize-QDataGovernanceActivity)

Resolved issues

The following is a list of issues addressed in this release.

NOTE: This release contains all resolved issues since the general release of One Identity Manager Data Governance Edition 8.0.2.

Table 1: Resolved issues

Resolved Issue	Issue ID
Fixed empty remote deployment agent drop-down list when running under non-US operating system culture settings.	776305 796562
Fixed include deviations feature for SharePoint.	794156
Fixed missing display names for SharePoint child deviations and updated display names for SharePoint Resource Access report.	794157 794158
Fixed SharePoint "Security Change" events.	794159
Re-enabled cloud managed host types: SharePoint Online and OneDrive for Business.	794160
Fixed circular group expansion in web portal Access Analysis view.	794329
Removed cloud login screen from displaying when switching host types for non-cloud hosts.	796558

Known issues

The following is a list of issues, including those attributed to third-party products, known to exist at the time of release.

Table 2: General known issues

Known Issue	Issue ID
Data Governance Edition does not handle computer name changes automatically. If a computer's name is changed after it has been registered as a managed host, some functions will not operate correctly. If a managed host computer is renamed, it must be removed and added again with the new name.	42129

Table 3: Installation and upgrade known issues

Known Issue	Issue ID
If you use the MSIExec.exe command to install the Data Governance server to a non-default location, you will be required to perform future upgrades to the server in the same manner. If the installation path is not specified when the upgrade is performed, the custom installation is removed and the new version is installed to the default location of %ProgramFiles%\One Identity\One Identity Manager Data Governance Edition.	313477
Upgrading the Data Governance server reverts the "run as" of the server service to Local System. The service must be reinstalled running as the previously configured account. To resolve this issue, when installing the new version of the Data Governance server, leave the installer Retry/Cancel dialog open when prompted, run the Service Control Manager, and switch the account on the Data Governance server from local system back to the original service account. Then click Retry in the installer dialog, and the installation should complete successfully.	359129
The Data Governance Configuration wizard is not detecting the existing Resource Activity database name. If you are not using the default name for your Resource Activity database, on an upgrade you must enter the "custom" database name on the Data Governance activity database page of the Data Governance Configuration wizard.	592431
After upgrading the Data Governance service to version 8.0, 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.	

Table 4: Resource activity known issues

Known Issue	Issue ID
If a volume is mounted as a drive letter and as a folder path, and changes are made through the folder path - the Activity reports show the drive letter as the path for activity.	148588
The SharePoint system account will be automatically filtered from resource activity.	320562

Known Issue	Issue ID
When you restart a NetApp filer, the Data Governance agents scanning that filer must also be restarted as they do not automatically register the required FPolicy.	417143
Resource activity collection and real-time security updates are not supported for EMC Isilon NFS managed hosts.	629701
EMC VNX activity collection is not supported for devices with multiple CIFS exposed virtual data movers.	
EMC activity collection requires that EMC CEE 7.1 is installed on the same server as the Data Governance agent.	
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 directly from your EMC device with both Change Auditor and Data Governance Edition.	
When integrating with Change Auditor version 6.9.x, no activity is being reported in Data Governance Edition. There is a Change Auditor 6.9 hotfix now available to fix this integration. Please contact One Identity technical support for the latest Change Auditor hotfix.	

Table 5: SharePoint known issues

Known Issue	Issue ID
The SharePoint account SHAREPOINT\system displays in Account access as NULL SID.	202555
In the Group Memberships tab, the location for SharePoint groups displays the URL instead of the friendly path for the group.	213029
In the Accounts view, renamed SharePoint groups do not show the new name after a rescan.	213906
When creating a new site collection on a farm where the SharePoint Auditing farm solution is enabled, you may see an error indicating that the farm solution is already activated. If this occurs, re-create the site collection.	215381
Exceptions occur during security index scans if web app policy denies rights to a farm account, even if the web app is not a selected security index root.	253558
Once data is placed under governance, a user or group's Limited access permission will be changed to the AllowRead permission.	271856
Retrieval of security for SharePoint hidden lists (such as Converted Forms)	314472

Known Issue	Issue ID
through Data Governance Edition may incorrectly list the security for its parent folder regardless of inheritance.	
For SharePoint 2010 farms, you may need to wait several minutes during agent install before managed paths can be successfully configured.	388288
For SharePoint 2010, initial scans do not occur as expected if there is a delay in setting dataroots for newly deployed managed hosts. **Workaround**: Wait for the scan schedule to lapse or restart the agent.	418369
SharePoint and Windows security scans add nested groups to the security index. The default behavior is to add an entry for every trustee that has been found to be directly ACL'd on a managed host. The SharePoint and Windows security scan behavior does not cause any harm, it is simply inconsistent with the expected behavior.	598090
Running Manage Access on a user/employee with a SharePoint user account type in the Security Index view logs an error: Requested value 'domain\user' was not found. **Workaround**: Run another SharePoint synchronization.	667557
In the web portal, the target accounts picker accessed from the "Edit subscription settings" window for an Account Access report shows the Claims Identity for SharePoint resources instead of the employee name.	675807

Table 6: Object naming known issues

Known Issue	Issue ID
Data Governance Edition may incorrectly represent the names of certain Built-in groups, such as Administrators and Power Users, if these groups have been renamed. NOTE: This does not affect the underlying functionality of Data Governance Edition, just the display names of these groups.	114243

Table 7: Machine local groups known issues

Known Issue	Issue ID
If a machine local user or group is renamed after it has been originally added to the Data Governance index, any subsequent name changes will not be properly reflected in the client.	70422

Table 8: Agent known issues

Known Issue	Issue ID
Network configuration changes may not be reflected in the agent connection information. If the network configuration of a managed host changes such that outgoing connections become blocked, the agent on that computer may be incorrectly reported as operating in Active mode. Additionally, queries against this agent may not be processed. To resolve this situation, restart the agent to renegotiate the connection.	45912
If you attempt to export an agent log from a client, ensure the agent state is set to OK. If the state is not set to OK, the process will fail. **Workaround**: Go to the agent installation directory, right-click the DataGovernance.Agent.exe.dlog file for the agent in question, and choose **Copy**.	178061

Table 9: Managed paths (formerly referred to as Security index roots) known issues

Known Issue	Issue ID
When deploying remote agents, it is sometimes possible to select roots that the specified service account cannot access. Ensure that the service account being selected for agent deployment can read the target.	110236
C$ and ETC$ are not valid as managed paths for NetApp filers.	177265

Table 10: Security modifications known issues

Known Issue	Issue ID
Removal of inherited and explicit entries in the security editor should be performed as two separate operations. When removing permissions in the security editor, if both explicit and inherited permissions are present in the selection, you will be prompted to confirm how to remove the inherited permissions. If the **Copy from Parent** option is selected, the permissions originally selected for removal will not be removed. A subsequent removal of the explicit permissions will properly remove the rights.	99724
Do not manipulate security on the computer's recycle bin as this can cause consistency issues with the content of the recycle bin itself.	105477
Adding machine local objects to a folder ACL on a NetApp filer using the Data Governance security editor is not supported. When navigating to a folder using a share path through the Resource browser or security editor, attempting to add a machine local ACE from the filer on the folder ACL will fail.	154142

Known Issue	Issue ID
You may receive an error when editing security, through the Manage Access view, for renamed resource on devices with a configured scanning schedule. It is recommended to use the Resource browser to complete this action.	215371

Table 11: Reporting known issues

Known Issue	Issue ID
Local reads of .txt files using notepad – no read event appears on activity reports. Account Activity and Resource Activity reports include events as they are conveyed by the system where the activity occurred. In some instances, certain applications do not report events as they may be expected by the user. This is the expected behavior of the application and Data Governance Edition, in most cases, is limited by what is reported by the operating system.	149909
If agents are not in an OK or Data available state, data from these agents will not be included in reports.	369565
Data Owners vs. Perceived Owners report in web portal does not allow you to select the root folder of a DFS link, therefore, the report can not be generated for that folder. **Workaround**: Select the root folder using the Grid view instead of the Tree view in the web portal.	648054

Table 12: Group membership known issues

Known Issue	Issue ID
Domain Built-in groups may not show access points on any managed host when selected from the tree view in the detailed Accounts view. To see this information, you must select the Built-in Group and run a Manage Access query that will return information on the Built-in group.	155748

Table 13: Built-in users known issues

Known Issue	Issue ID
Only well-known accounts (such as Everyone and Authenticated Users) are returned when the Built-in filter is selected. Other Built-ins, such as administrators and users, are returned as groups.	109347

Table 14: NetApp managed host known issues

Known Issue	Issue ID
Cloning an account on a NetApp managed host is not supported.	208968
Adding rights to a folder on a NetApp managed host is not supported.	208975
If you wish to collect security changes from your NetApp filer using Change Auditor, and you are also using Data Governance Edition to collect activity, you must disable cifs_setattr on the Data Governance FPolicy. In addition, you should not select to collect real-time security updates in Data Governance Edition. NetApp will not send the security change to more than one FPolicy.	262027

Table 15: Shared managed resource process known issues

Known Issue	Issue ID
Configuration in a cross domain/forest scenario: In order to create the shared folder, the service account for the One Identity Manager job service requires extended permissions on the managed host server in the other domain/forest where the share root resides. That is, this service account requires permissions to create the share and add the groups to the share.	520543

Table 16: Governed data attestation known issues

Known Issue	Issue ID
The Governed Data: Resource security deviation attestation shows no selected objects. That is, in the Manager when you select **Change master data | Run attestation cases for single objects** for a governed resource that has security deviations from its parent folder, the expected objects are not listed on the Run attestation cases for single objects dialog.	647709

Table 17: Cloud managed host known issues

Known Issue	Issue ID
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.	
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.	

Table 18: Identity Manager Application Server known issues

Known Issue	Issue ID
Unable to assign user (Active Directory, UNS, SharePoint) accounts to an employee from Employees view in the Manager client when logged in through the Application Server. **Workaround**: In some situations, using an Application Server connection with the Manager may not function as expected. Switching temporarily to a direct database connection should allow the function to succeed.	678767

Table 19: Third-party known issues

Known Issue	Issue ID
Windows 2008	
Unable to install an agent on a computer running Windows 2008. To resolve this issue, download and install the VeriSign Class 3 Primary CA -G5 certificate in the local certificate store on the required target computers. The download is available here: https://www.symantec.com/page.jsp?id=roots.	352646
Windows Server 2012/2012 R2	
Agents used to scan an EMC or NetApp filer cannot be hosted on Windows Server 2012 or 2012 R2. When the Data Governance server is hosted on Windows 2012/2012 R2, you cannot browse resources or set managed paths for the EMC or NetApp managed host. This is related to a known issue with Windows Server 2012/2012 R2. **Workaround**: Use an alternative supported operating system to host the agent to scan the EMC or NetApp filer or 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` For more details on the known issue, see http://support.microsoft.com/kb/2686098.	272220
Agent cannot access EMC or NetApp shares. After adding an EMC or NetApp host machine to a domain running Windows Server 2012/2012 R2 or Windows 8, a "Windows cannot access <*machine*>" network error appears when attempting to access a share on the NAS device using the file explorer. The root cause is likely due to an incompatibility between your NAS device and SMB 2.0. **Workaround**: Upgrade the FLARE code on your NAS device with support for SMB 2.2. If that is not feasible, disable SMB 2 in Windows Server 2012/2012 R2 or Windows 8.	596797

Known Issue	Issue ID
For more details on the known issue and the proper solution, see http://www.exaltedtechnology.com/windows-8-access-is-denied-to-network-shares-could-be-an-issue-with-smb-2-2-with-emc-cellera-or-nas-device/	
NetApp	
Local user accounts created on a NetApp filer with a password longer than 14 characters, will not be included in the indexed information sent to the Data Governance server.	204302

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 meet. 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 20: Minimum system requirements: Data Governance server

Processor	quad core CPU
Memory	16GB RAM
Free drive space	100GB
Operating system	64-bit Windows operating systems: • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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.
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 21: Minimum system requirements: Database server

Processor	16 physical cores with 2.5GHz+
Memory	32GB RAM minimum NOTE: In addition to One Identity Manager's memory requirements of 16 + GB, Data Governance Edition requires an extra 16GB of RAM.
Hard drive 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	64-bit Windows operating systems: • Note the requirements given by Microsoft for the SQL Server version you are using. NOTE: The 64-bit requirement for Windows Servers is specific to Data Governance Edition. UNIX and Linux operating systems: • Note the requirements given by the operating system manufacturer for SQL Server databases.
Software	Supported SQL Server versions are: • SQL Server 2017 Standard Edition (64-bit) with the latest cumulative update • SQL Server 2016 Standard Edition (64-bit), Service Pack 2 with the latest cumulative update NOTE: SQL Server Enterprise Edition is recommended for performance reasons. SQL Server Management Studio (recommended)

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

Table 22: Database server settings

Property	Value	Comment
Language	English	
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	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. 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.

Property	Value	Comment
SQL Server Agent	Started	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. 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.
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	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 **Simple**, the installation is not started.
Compatibility level	SQL Server 2016 (130)	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 Identi-fiers Enabled	True	The setting is checked by the Configuration

Property	Value	Comment
		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 fro transactions is **AutoCommit**. If transactions are required, they are opened explicitly. 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. The setting is checked by the Configuration Wizard before installing or updating the One Identity Manager database and adjusted for the database if necessary.
Database file and data file group for memory-optimized tables	Required	One Identity Manager uses In-Memory-OLTP (Online Transactional Processing) for memory-optimized data accesses. For the creation of memory-optimized tables, the following prerequisites must be met: • A database file with the **Filestream data** file type must exist. • A memory-optimized data file group must exist. Before installation or update of the One Identity Manager database, the Configuration Wizard checks whether these requirements are fulfilled. 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`).

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 23: 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	Windows operating systems: • Windows Server 2008 • Windows Server 2008 (R2) (32-bit or non-Itanium 64-bit) • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 NOTE: New Dynamic Access Control (DAC) features are not supported. 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". 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.
Software	.NET Framework 4.5 or later .NET Framework 3.5.1 (SharePoint 2010 agents) NOTE: SharePoint 2010 agents require .NET Framework 3.5.1; all other Windows Servers and SharePoint 2013 farms hosting an agent require .NET Framework 4.5 or later.

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 24: 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 25: Supported target systems

Target	Version	Additional notes
Windows Server	The following Windows Server versions are supported for scanning (local or remote managed hosts): • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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.	Resource activity collection is not supported for remotely managed Windows Server hosts.

Target	Version	Additional notes
Windows Cluster	The following failover clusters are supported for scanning (remote managed host): • Windows 2008 • Windows 2008 (R2) • Windows 2012 • Windows 2012 (R2) • Windows 2016 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.	Resource activity collection is not supported for Windows clusters.
NetApp CIFS Devices	The following NetApp filer versions (with CIFS file system protocol enabled) are supported for scanning (remote managed host): • 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 NOTE: Both NetApp 7-Mode and Cluster Mode are supported.	Real-time security updates and resource activity collection are not supported on versions of NetApp ONTAP filers earlier than 7.3. NetApp storage devices require additional configuration.

Target	Version	Additional notes
	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.	
NetApp NFS Devices	The following NetApp filer versions (with NFS file system protocol enabled) are supported for scanning (remote managed host): • 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 NOTE: Both NetApp 7-Mode and Cluster Mode are supported. 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.	NFS managed hosts require the UNIX module to be installed during the One Identity Manager installation and configuration process. 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. NetApp storage devices require additional configuration.
EMC CIFS Devices	The following EMC devices are supported for scanning (remote managed host): • EMC Celerra	VNXe is not supported. VNXe does not support CEPA currently and therefore Data Governance Edition will not run successfully in VNXe environments.

Target	Version	Additional notes
	• EMC VNX • EMC Isilon The following EMC Framework versions (with CIFS file system protocol enabled) are supported: • Common Event Enabler (CEE) 7.1 (or higher) 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.	EMC storage devices require additional configuration.
EMC Isilon NFS Devices	The following EMC Isilon devices (with NFS file system protocol enabled) are supported for scanning (remote managed host): • EMC Isilon 7.2 • EMC Isilon 8.0 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.	NFS managed hosts require the UNIX module to be installed during the One Identity Manager installation and configuration process. Resource activity collection is not supported for EMC Isilon NFS managed hosts. EMC storage devices require additional configuration.
SharePoint	The following SharePoint versions are supported for scanning (local managed host): • SharePoint Server 2010 • SharePoint Server 2013 • SharePoint Server 2016 100GB disk space on the	Agent is installed where the One Identity Manager service (job server) is running for the SharePoint farm. We recommend installing the One Identity Manager service on a dedicated SharePoint Application Server in the farm and not on a Web Front server

Target	Version	Additional notes
	SharePoint agent computer for data storage and scan post-processing activities. NOTE: The space required depends the number of sites, lists, and document libraries and the number of unique permissions gathered from the farm. 8GB RAM for the SharePoint agent computer.	which prevents extra load processing on that server. Standalone farms are not supported. Farms configured with only Local Users and Groups are not supported.
Cloud	The following cloud providers running on Office 365 are supported for scanning (remote managed host): • SharePoint Online • OneDrive for Business	Resource activity collection is not supported for Cloud managed hosts. 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.
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 26: Required minimum permissions

Account	Permission
System user (Active Directory account logged on to the computer) AND Manager user (Active	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.

Account	Permission
Directory account running the Manager)	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.
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 agent managing SharePoint farms	Must be the SharePoint farm account (same account that is used to run the SharePoint timer service and the One

Account	Permission
	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.

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 27: 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 computer. Used for communication with Data Governance agents, One Identity Manager clients, One Identity Manager web server, and PowerShell. 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. IMPORTANT: Do NOT use the Designer to change the QAMServer configuration parameters, including the Port parameter.
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.

Product licensing

Use of this software is governed by the Software Transaction Agreement found at www.oneidentity.com/legal/sta.aspx. This software does not require an activation or license key to operate.

Upgrade and installation instructions

NOTE: One Identity Manager and Data Governance Edition must be running the same version. Use the installation and configuration wizards to perform a new install or upgrade from a previous version of Data Governance Edition.

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.

For detailed instructions on installing and configuring One Identity Manager Data Governance Edition see the *One Identity Manager Installation Guide* and the *One Identity Manager Data Governance Edition Deployment Guide*.

Upgrading One Identity Manager Data Governance Edition

In order to take advantage of the enhancements added to Data Governance Edition version 8.1, 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.

See the *Upgrading Data Governance Edition* chapter in the *One Identity Manager Data Governance Edition Deployment Guide* for full instructions on upgrading Data Governance Edition.

More resources

Additional information is available from the following:

- One Identity Manager online product documentation: https://support.oneidentity.com/identity-manager/technical-documents
- Data Governance Edition online product documentation: https://support.oneidentity.com/identity-manager-data-governance-edition/technical-documents
- One Identity community: https://www.quest.com/community/products/one-identity/

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

Legend

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

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

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