opentext™

OpenText
Core Data Discovery & Risk Insights

Application Version 24.4.0

Processing Agent Version 24.4.100

Support Matrix

Legal notices

OpenText Core Data Discovery & Risk InsightsSupport Matrix

Application version:24.4.0

Processing Agent version:24.4.100

Publication date: November 2024

About OpenText Core Data Discovery & Risk Insights

OpenText Core Data Discovery & Risk Insights lets you find, protect, and secure sensitive and high-value data within on-premises and cloud data platforms across your enterprise. Identify, collect, and organize content to ensure discovery of sensitive data. Configure how structured and unstructured sources and datasets are processed and categorized with Connect. Analyze your data under management with Analyze. Organize, review, and take action on documents and unstructured data items with Manage.

Support matrix

The following hardware, software, and application requirements are supported with this version of OpenText Core Data Discovery & Risk Insights.

Web browsers and plug-ins

OpenText Core Data Discovery & Risk Insights is supported on the following browsers.

- Google Chrome 129 or later
- Firefox 131 or later
- Microsoft Edge 129 or later

OpenText Core Data Discovery & Risk Insights is best viewed at the following screen resolution:

- 1366 x 768 or greater resolution.

Data Resources

The following resources are supported for data processing by the on-premises agent.

- OpenText Content Manager 10.1.x or 23.4.x

  > **IMPORTANT:** Only Microsoft SQL Server Unicode RDB datasets are supported at this time.

- File system CIFS/ SMBv2 shares
  - Must comply with SMBv2 protocol for share name restrictions.
- Microsoft Exchange Server 2016 fully updated and patched, 2019 fully updated and patched, and Office 365
- SharePoint 2016, fully updated and patched, and Office 365
  - For SharePoint 2016, Site Collections, Web Applications, and OneDrive are supported.
  - For Office 365 SharePoint, Site Collections and OneDrive are supported.
- Google Workspace's Drive (personal Google Drives are not supported)
- Documentum 24.3.x or later
- Extended ECM 24.3.x or later
- Structured data platforms
  - *Platforms supported by the built-in structured data processor*
    - Oracle
      - Oracle 19c, Oracle 21c

- IBM Db2

  - Db2 11.5.x

- SQL Server

  - SQL Server 2019, SQL Server 2022

- PostgreSQL

  - PostgreSQL 12.x, PostgreSQL 13.x, PostgreSQL 14.x, PostgreSQL 15.x, PostgreSQL 16.x

- MySQL

  - MySQL 8.x

- Sybase

  - Sybase 16.0

- *Platforms supported by connection to Structured Data Manager*

  > **NOTE:** For supported versions, see the *Structured Data Manager Certification Matrix*.

  - Oracle

  - IBM Db2

  - SQL Server

  - PostgreSQL

  - MySQL

  - JDBC

  - Sybase

Processing agent host

Review the agent host requirements.

> **CAUTION:** Install the processing agent on a dedicated VM machine with connectivity to your data resources. Do not install the processing agent on a machine that you will be processing data from.

On-premises agent host requirements

The server that will host the on-premises processing agent must meet the following requirements.

Resources

The host server for the agent requires the following resources. The agent should be installed on a dedicated drive. If you will be processing large container files, start with the recommended values.

Resource	Minimum (AWS c5.xlarge equivalent)	Recommended (AWS c5.2xlarge equivalent)
CPUs	4	8
RAM	8GB	16GB
Free space	85GB	200GB

If more than 4 CPUs are available, increase the number of threads available to the Connector Framework Server service.

To increase the threads available to the Connector Framework Server service

1. Open `<agentInstallDir>\CFS\cfs.cfg`. By default, the agent install directory is `C:\Program Files\OpenText\Core Data Discovery & Risk Insights\Agent\`.

2. Under the `[ImportService]` section, locate the `ThreadCount` setting.

3. Change the default setting value of `3` to be roughly two-thirds the number of the cores available.

   For example, if you have 8 cores, set the `ThreadCount` value to **6**.

4. Save the `cfs.cfg` file.

5. Restart the Connector Framework Server service.

Operating System

Ensure that you are running a supported operating system with all currently "critical" and "important" updates installed from update.microsoft.com.

- Windows Server 2016 from English Installation Media (Standard, Datacenter)

  The "Server with Desktop Experience" installation option is required. Additional language packs may be added after OS installation.

- Windows Server 2019 from English Installation Media (Standard, Datacenter)

  The "Server with Desktop Experience" installation option is required. Additional language packs may be added after OS installation.

- Windows Server 2022 from English Installation Media (Standard, Datacenter)

  The "Server with Desktop Experience" installation option is required. Additional language packs may be added after OS installation.

Agent host ports in use

The processing agent uses the following ports on the agent host server. Ensure these ports are available.

Ports	Location	Usage
7957	available on agent host; does not need to be open for communication outside this box	processing agent
7432	available on agent host; does not need to be open for communication outside this box	PostgreSQL; will bind to the local loopback addresses of 127.0.0.1 (IPv4) and ::1 (IPv6)
7500, 7502	available on agent host; does not need to be open for communication outside this box	CFS (Connector Framework Server)
9312	network needs to be open from the agent host to the OpenText Core Data Discovery & Risk Insights service (gateway).	gateway for the processing agent

General

The following requirements must be met for the server hosting the processing agent. Applications listed must exist on the host server prior to installing the agent.

- If processing file system documents from a host machine that has long paths enabled, long paths must also be enabled on the agent host.

- Ensure the public certificate presented by the external proxy is trustable by agent hosts. Depending on the certificate presented, this may include importing a private certificate authority (CA) certificate to the local Windows certificate store.

  > **IMPORTANT:** If a private CA is used, ensure the private CA's certificate is removed if the agent is uninstalled.

- Ensure the Windows server is permitted to communicate through TLS 1.2 or 1.3, using a current "safe" cipher suite to ports 9000-9999. The OpenText Core Data Discovery & Risk Insights back office components (commonly in the cloud) implement and require an Intermediate TLS security level (https://wiki.mozilla.org/Security/Server_Side_TLS).

> **IMPORTANT:** By default, most supported Windows server operating systems are pre-configured to allow communication with the back office and to dataset targets enforcing TLS 1.2 communication using a reduced safe set of ciphers (EX2019, O365, SPO). Ensure this connectivity is communicating with functional targets by using a web browser that utilizes Windows Schannel (Internet Explorer) or via the Invoke-WebRequest PowerShell cmdlet.

It is possible to harden encryption in Windows server to restrict the native Schannel encryption component, used by the processing agent services, to specific operating modes and particular cipher suites (https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings). The following are the minimum required values.

- TLS 1.2 (Client): Enabled
- Windows 2016/2019/2022 required cipher suites
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- Ensure earlier versions of SSL and TLS in Windows Schannel are disabled and that .NET applications (particularly 4.x) use the system's Windows Schannel configuration. See https://docs.microsoft.com/en-us/officeonlineserver/enable-tls-1-1-and-tls-1-2-support-in-office-online-server#enable-strong-cryptography-in-net-framework-45-or-higher.

- Ensure that the user you run the installation as has administrative rights on each server. You cannot perform the installation unless you have administrative rights to perform the required tasks.

- If the agent will connect using a proxy, ensure the user you are logged in as has internet access on the host machine. Details for connecting using a proxy are detailed in the appropriate procedures for installing and configuring the agent.

- If using Media Server for optical character recognition (OCR), OpenText Core Data Discovery & Risk Insights processing agents and any Media Server host machines they interact with must be within the same network and can not have a proxy between them.

- If you will be sending copies of masked data items to a target location, ensure the most recent version of a 64-bit Chromium-based browser (such as Microsoft Edge, Google Chrome, or Chromium) is installed on the agent host machine.

- Microsoft Outlook 2019 x64 to process PST files located on file systems.

  > **IMPORTANT:** The default installation for Outlook 2019 is x32. Ensure you have the x64 version installed.

- SMTP (currently optional)

- Visual C++ 2019 runtime, updated to the most current version

- .NET 8

- If processing structured data from Db2 databases, ensure the following are in place.

- ○ Visual C++ 2013 Redistributable, updated to the most current version

- ○ Additional drivers to support processing from Db2 databases are needed on the agent host machine.

    1. Download the driver package for your operating system from your Db2 web console.

    2. Unpack the driver package.

    3. Copy `IBM.data.Db2.dll` and the entire `\clidriver` directory from the unpacked driver package and place in the `\Agent\StructuredDataProcessor` directory of the OpenText Core Data Discovery & Risk Insights application installation path. By default, the application installation path is `C:\Program Files\OpenText\Core Data Discovery & Risk Insights\Agent\StructuredDataProcessor`.

Integrated resources

The following third-party applications are supported by OpenText Core Data Discovery & Risk Insights.

- Microsoft Purview Information Protection (MPIP) for file protection in Connect and Manage.

  > **IMPORTANT:** OpenText Core Data Discovery & Risk Insights supports the version of MPIP available at the time of this release.
  >
  > In OpenText Core Data Discovery & Risk Insights, this file protection type is referred to as "Microsoft data protection".

- OpenText Media Server 12.11 for optical character recognition (OCR).

  OpenText Core Data Discovery & Risk Insights processing agents and any Media Server host machines they interact with must be within the same network and can not have a proxy between them.

The following third-party applications are required for specific OpenText Core Data Discovery & Risk Insights features.

- Microsoft Excel on the local machine where OpenText Core Data Discovery & Risk Insights is being accessed with a browser. This is required to support uploading term lists using a CSV file.