Access and Hardware Specifications

Document version: 1.9.2

Document Properties

Client Name	[Client Organization Name]
Client Addressee	[First Name] [Last Name]
Sent By	[First Name] [Last Name]
Sent Date	[dd/mm/yyyy]
Document Version	[x.x]

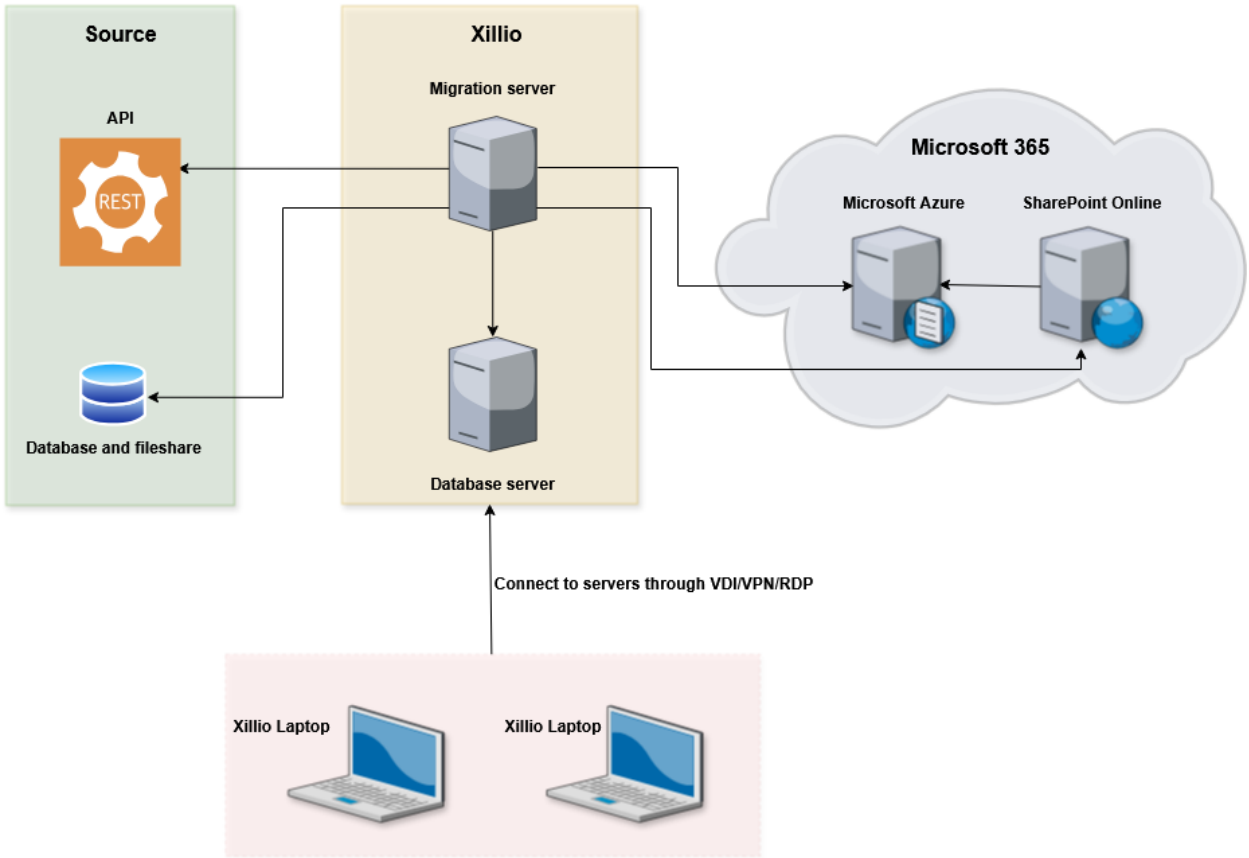
Table of Contents

Introduction

This document describes the activities and specifications of hardware and software needed to arrive at a working setup for the migration of data and content from the source environment to the Microsoft SharePoint Online tenant (hosted in the Microsoft Azure / MS 365 cloud).

Infrastructure

Xillio consultants perform their migration work on two servers which should be located within the client its network environment. The migration server should be able to connect to the source system to retrieve all the metadata and files, and it should be able to connect to the Microsoft 365 servers to perform the actual migration to SharePoint Online. Connections to the migration and database servers are made from laptops where the Xillio consultants are working on. The laptops will be provided by Xillio or by the client and the connection to these servers can be made through a VDI, VPN, RDP or any other gateway mechanism that has been set up. The diagram below depicts the described infrastructure.



Please note that with this setup ALL data will remain within the client its environment and will not be copied to any laptop.

Servers

To perform all the migration activities Xillio needs 2 servers (either physical servers or virtual machines) within the client its network. The first server runs our migration tooling and is used to perform the actual migration (called migration server). The second server is the database server running both MongoDB and the insights tooling.

The minimum system requirements for each of these 2 servers:

- Windows server 2019 or higher
- 32GB of RAM
- Intel Xeon E3 1270 V6 or equivalent (Xeon Quadcore, 8 threads / virtual processors).

For storage we require different configuration depending on the server:

- Migration server:
  - 100GB SSD on a separate partition (for OS)
  - 500GB SSD on a separate partition (for software and import packages)
- Database server:
  - 100GB SSD on a separate partition (for OS)
  - 2TB SSD on a separate partition (for the database for migrations up to 1 TB)

Xillio needs 2 accounts with local administrator permissions on all servers to be able to install and configure the required software. When providing local administrator permissions is not possible, Xillio can provide installation packages.

If the Xillio Link Redirector is part of the implementation, we recommend two separate servers. One that will host the Link Redirector, and one for the database. The database server from the migration can be repurposed for this use-case as the Link Redirector can also work with MongoDB. The server which will host the Link Redirector has the following minimum system requirements:

- RAM: 4GB
- CPU: 2 core @ 2.4Ghz
- Disk Space: 40GB
- OS: Windows Server / Linux / MacOS

For more information about these system requirements please refer to the documentation. It should be noted that these requirements may be subject to change, as additional business rules and requirements are set during the initiation. For example, in a scenario where there is a high volume of business critical network traffic flowing through the Link Redirector, an additional server might be required to share the network load. More information can be found in the documentation about Load Balancing.

Security

The MongoDB instance should be password-protected and it is strongly recommended to limit access to the migration servers only by setting up a firewall rule for TCP ports: 27017, 27018, 27019 and 27020. Furthermore, please make sure the Xill4 application is not accessible from the outside.

Backups

Throughout the duration of the project the data on partitioned drives of the server needs to be backed up on a regular interval. Preferably this is done daily.

Whitelisting

For the Xillio tooling the cryptolens.io platform is used to validate the Xillio licenses. For the Xillio application to work these Cryptolens IP addresses need to be whitelisted on port 443 on the migration server:

- 23.102.21.212
- 20.82.170.150

The database server should be accessible from the migration server on TCP ports:

- 27017, 27018, 27019 and 27020 (Mongo)
- 9200 (Elasticsearch database)
- 5601 (Kibana dashboards)

For VPN access Xillio's IP address will have to be whitelisted: 84.243.234.102 /24.

Network and Internet

In the migration the metadata and documents will have to be retrieved and uploaded to Azure. The available network bandwidth will have an impact on the duration of the migration. Xillio recommends having a minimum of 800 Mbps bandwidth available.

Furthermore, Xillio requires (limited) internet access to be able to access the source and target system, and to be able to share reports and migration design documents. These reports are generated and used by the migration software throughout the project. Usually, Microsoft Teams is used for this purpose, but other content sharing platforms like Box.com is also an option.

Lastly, Xillio regularly makes backups of the project code. For this purpose, we require access to github.com.

Updates, Restarts, and Scanning

Typically, the migration activities last several days and interruptions could disrupt the migration. Therefore, Xillio requests the following changes to be made to the servers:

- Exclude all servers from restart/update schedules. Xillio understands that updates sometimes need to be made. Please inform Xillio up-front in case any update or restart must be made so it can be scheduled in the migration activities.
- Disable on-access (virus) scanning of Mongo database data folders. The Xillio tooling makes intensive use of the Mongo database and scanning might decrease the performance of the migration activities. Other changes to the virus scanner are not necessary.

Access Requirements for Source Systems

Xillio requires access to both the front-end and back-end of the source systems. Front-end access is required to validate the extracted data. Possible back-ends Xillio needs to connect to depending on the source system:

- Database (Local DB access, Windows authentication is **NOT** supported)
- Network drive and / or cloud location where the files are stored
- API, e.g., REST or SOAP

For front-end and API access the created account should have sufficient permissions to view and read all the content that needs to be migrated.

Please reference Appendix A for access requirements to specific source systems.

Access Requirements for Microsoft 365

Microsoft 365 and Azure storage accounts

The Xillio migration software has a built-in encrypted and password protected vault for storing all the required credentials and keys. These secrets are only accessible by migration software and not by any user of the server the software is running on.

For the migration to SharePoint Online Xillio uses several Microsoft APIs, i.e. the Microsoft Graph API and the Microsoft Migration API. To use these APIs and correctly prepare all the data to be migrated, Xillio needs several accounts:

- SharePoint Online Administrator account
- Azure app registration (Microsoft Graph + SharePoint permissions)
- Azure storage account

Xillio can aid with setting up all the accounts if needed. Connectivity can be checked by using the Connectivity Checker app found here: https://xillio.community/products.

SharePoint Online Administrator Account

Xillio needs a SharePoint Online (Microsoft) account with site collection administrator rights limited to the sites and/or site collections where the content will be migrated to. If relevant, this account will need access to both test / acceptance and production tenant(s).

If required, add this dedicated Xillio account to an appropriate security role that allows Xillio to interact with the system Front-End (SharePoint, MS Teams).

Azure app registration

An Azure app will need to be created with Graph API and SharePoint permissions.

Graph API Permissions

The Microsoft **Graph API** is used to retrieve metadata of the sites that will have to be migrated to, i.e., identifiers of libraries and the available content types.

To connect to the Graph API an application needs to be registered in the Azure portal. For more information see https://docs.microsoft.com/en-us/graph/auth.

The following Microsoft Graph API **Application Permissions** are required:

- Sites.Selected for specific sites or Sites.Read.All for the entire tenant
  Used to get the content types, fields, sites, libraries, folders of a site, and to import the content to Microsoft 365
- User.Read.All
  Used to set creator and modifier on SharePoint objects
- Group.Read.All
  Used to set groups on SharePoint objects
- TermStore.Read.All
  Used to set terms on managed metadata fields on SharePoint objects

Note: When limited site access is given with the Sites.Selected permission, an administrator must grant FullControl access to the required sites. For example, this PnP PowerShell command can be used: https://pnp.github.io/powershell/cmdlets/Grant-PnPAzureADAppSitePermission.html. Refer to Xillio's documentation to view another example: SharePoint Online (OneDrive, Teams) target connector | Xill4, under the chapter "SharePoint API".

For more information see https://devblogs.microsoft.com/microsoft365dev/updates-on-controlling-app-specific-access-on-specific-sharepoint-sites-sites-selected

Furthermore, a **self-signed certificate** will be provided by Xillio which is to be registered in the Azure application. The `Thumbprint` value of the registered certificate is needed by Xillio.

Xillio requires the following information of the App Registration:

- Client Id
- Client Secret
- Tenant Id
- Thumbprint (generated by uploading the self-signed certificate to the App Registration)

SharePoint API Permissions

The Microsoft **SharePoint API** is used to import the content to SharePoint Online. In order to connect to the SharePoint API, the previously registered Azure application needs to be given an additional SharePoint API permission using the Application permissions tab.

- Sites.Selected for specific sites or Sites.FullControl.All for the entire tenant
  Used to import the content to SharePoint

> **Note:** When limited site access is given with the Sites.Selected permission, an administrator must grant FullControl access to the required sites. For example, this PnP PowerShell command can be used: https://pnp.github.io/powershell/cmdlets/Grant-PnPAzureADAppSitePermission.html. For more information see https://devblogs.microsoft.com/microsoft365dev/updates-on-controlling-app-specific-access-on-specific-sharepoint-sites-sites-selected

Azure Storage Account

The Microsoft Migration API pulls data from an Azure storage container and migrates it to the appropriate SharePoint Online sites by triggering the matching message queue. For this reason, Xillio requires an Azure storage account name and key. The connection string can be retrieved from the Azure portal (Storage account -> Access keys -> key1).

Syntax of the Azure connection string:

```
DefaultEndpointsProtocol=[http|https];AccountName=myAccountName;AccountKey=myAccountKey
```

The account needs to be able to create blobs and queues. If the Azure firewall is enabled within the storage account, the Microsoft and SharePoint IP addresses need to be whitelisted. These IP addresses will have to be retrieved from the queue and blob logs once the migration solution is in place and tested.

It is also possible to let Microsoft provision the Azure storage containers. In this case an Azure storage account is not required. However, this is not recommended because it decreases the performance of migration.

Access requirements for Xillio Link Redirector

For a successful implementation of the Xillio Link Redirector, access to the DNS settings is a must. It is not mandatory that one of Xillio's employees has free access to these settings, as this can be done in cooperation with another internal administrator.

Secondly, some organizations use internal reverse-proxies to manage domain names and traffic within the network. If this is applicable in the current project, access to these settings is also required. As with the DNS settings, this can be done together with an admin.

List of Installable Xillio Software

Below is a list of software Xillio can (install and) use during the project for each server.

Note: Depending on the project scope, the installation and use of certain software(s) may not be required.

Migration server

Group	Application name	Application link	Description
Migration software			
	Xillio migration tooling	https://docs.xill.io/xill4	Migration engine to perform the ETL activities
	PowerShell 7, modules	https://learn.microsoft.com/en-us/powershell/module/	Interact with the SharePoint and Azure environments. Installed modules: az, PnP, Mdbc
Database software			

	MongoDB compass	https://www.mongodb.com/products/tools/compass	Mongo database browsing tool
	SQL developer	https://www.oracle.com/database/sqldeveloper/	For browsing source system databases
	SQLiteStudio	https://sqlitestudio.pl/	For browsing sqlite databases
Utilities			
	Notepad++	https://notepad-plus-plus.org	Text editor
	7-zip	https://www.7-zip.org/	File archiver to zip and unzip
	Microsoft Edge or Google Chrome	https://www.microsoft.com/edge https://www.google.com/chrome	Browser to view data in insights, share reports and view data in the source system front-end
	LibreOffice	https://www.libreoffice.org/	Used for Excel reports
	Visual Studio Code	https://code.visualstudio.com	With PowerShell module installed. Used for running PowerShells cripts

Database Server

Group	Application name	Application link	Description
Database software			
	MongoDB 8.x or higher	https://www.mongodb.com/	Database engine used by our migration

			engine. All metadata is stored here
	MongoDB compass	https://www.mongodb.com/products/tools/compass	Mongo database browsing tool
Insights software			
	Elasticsearch	https://www.elastic.co/	Database used by Insights to store and retrieve all the metadata and analytics
	Kibana	https://www.elastic.co/kibana/	Insights dashboards for analyzing the content to be migrated
Utilities			
	Notepad++	https://notepad-plus-plus.org	Text editor
	7-zip	https://www.7-zip.org/	File archiver to zip and unzip
	Microsoft Edge or Google Chrome	https://www.microsoft.com/edge https://www.google.com/chrome	Browser to view data in insights, share reports and view data in the source system front-end
	LibreOffice	https://www.libreoffice.org/	Used for Excel reports

Checklist

This checklist can be used by the client and consultant to confirm that all requirements are met.

- ☐ Connecting to customer network environment:
  - ☐ Connection security
    - ☐ VPN software for Xillio laptop
    - ☐ Site-to-site VPN from Xillio office to client environment
    - ☐ Xillio Office IP in client Firewall whitelist and port forward
    - ☐ Other
  - ☐ Remote Access Software
    - ☐ Remote Desktop Connection
      - Resources Xillio client side
        - ♦ Drive redirection is not allowed.
        - ♦ Clipboard is allowed.
    - ☐ TeamViewer
    - ☐ VNC
    - ☐ Other
- ☐ Connect to each server (migration and insights)
  - ☐ Confirm hardware specifications are met
  - ☐ Confirm local administrator access and/or confirm availability of required software
  - ☐ Confirm (limited) internet access
  - ☐ Confirm required network bandwidth
- ☐ Migration server
  - ☐ Confirm access to the source system front-end
  - ☐ Confirm access to the source system back-end(s)
  - ☐ Confirm access to the SharePoint Online sites by using the Connectivity Checker app (https://xillio.community/products)

After installation of the software the following needs to be checked for each type of server:

Migration Server:

- ☐ Confirm access to the Xillio migration tool (by default running on http://localhost:8000)
- ☐ Confirm access to the Mongo database (by default running on Mongo DB server IP address port 27017)
- ☐ Confirm access to the Insights dashboard (by default running on http://localhost:5601)

Database Server:

- ☐ Confirm access to the Mongo database (by default running on localhost port 27017)
- ☐ Confirm access to the Insights dashboard (by default running on http://localhost:5601

Appendix A – Source Systems

Alfresco

Xillio requires read-only access to:

- Front-end
- Database + location of stored files
- REST API

Alfresco Front-end

Xillio needs the following information:

- Username
- Password
- Alfresco URL (e.g., https://alfresco.client.com/share/page)

Alfresco Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

Alfresco Network Drive / Cloud Location

Xillio needs the following information:

- Username
- Password
- Location

Alfresco CMIS and REST API

Xillio needs the following information:

- Username
- Password
- Alfresco CMIS API URL (e.g. https://alfresco.client.com/alfresco/cmisbrowser)
- Alfresco REST API URL (e.g. https://alfresco.client.com/alfresco/api/-default-/public/alfresco/versions/1)

The provided credentials for the front-end can be used for the back end.

Documentum

Xillio requires read-only access to:

- Front-end
- Database + location of stored files
- REST API

Documentum Front-end

Xillio needs the following information:

- Username
- Password
- Documentum URL (https://documentum.client.com/da)

Documentum Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

Documentum Network Drive / Cloud Location

Xillio needs the following information:

- Username
- Password
- Location

Documentum REST API

Xillio needs the following information:

- Username
- Password
- Documentum REST API URL (e.g. https://documentum.client.com/dctm-rest)

The provided credentials for the front-end can be used for the back-end.

FileNet

Xillio requires read-only access to:

- Front-end
- Database + location of stored files
- API

FileNet Front-end

Xillio needs the following information:

- Username
- Password
- FileNet URL (e.g. https://filenet.client.com/acce)

FileNet Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

FileNet Network Drive / Cloud Location

Xillio needs the following information:

- Username
- Password
- Location

FileNet API

Xillio needs the following information:

- Username
- Password
- FileNet API URL (e.g. http://filenet.client.com/wsi/FNCEWS40MTOM)

The provided credentials for the front-end can be used for the API.

HP TRIM

Xillio requires read-only access to:

- Front-end
- Database + location of stored files
- REST API

HP TRIM Front-end

Xillio needs the following information:

- Username
- Password
- HP TRIM URL (e.g., http://hptrim.client.com/HPEContentManager)

HP TRIM Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

HP TRIM Network Drive Location

Xillio needs the following information:

- Username
- Password
- Location

HP TRIM REST API

Xillio needs the following information:

- Username
- Password
- HP TRIM REST API URL (e.g. http://hptrim.client.com/HPECMServiceAPI)

The provided credentials for the front-end can be used for the back end.

Objective

Xillio requires read-only access to:

- Front-end
- Database + location of stored files

Objective Front-end

Xillio needs the following information:

- Username
- Password
- Objective URL or client application

Objective Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

Objective Network Drive Location

Xillio needs the following information:

- Username
- Password
- Location

OnBase

Xillio requires read-only access to:

- Front-end
- Database + location of stored files

OnBase Front-end

Xillio needs the following information:

- Username
- Password
- OnBase URL or client application

OnBase Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

OnBase Network Drive Location

Xillio needs the following information:

- Username
- Password
- Location

OpenText CS

Xillio requires read-only access to:

- Front-end
- Database + location of stored files
- REST API

OpenText CS Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner

OpenText CS Network Drive / Cloud Location

Xillio needs the following information:

- Username
- Password
- Location

OpenText CS Front-end

Xillio needs the following information:

- Username
- Password
- OpenText CS URL (e.g. http://otcs.yourcompany.com/otcs/cs.exe?func=llworkspace)

OpenText CS API

Xillio needs the following information:

- Username
- Password
- OpenText CS REST API URL (e.g. http://otcs.yourcompany.com/otcs/cs.exe)

OpenText eDOCS

Xillio requires read-only access to:

- Front-end
- Database + location of stored files

OpenText eDOCS Front-end

Xillio needs the following information:

- Username
- Password
- OpenText eDOCS URL (e.g. http://edocs.yourcompany.com/eDOCS)

OpenText eDOCS Database

Xillio needs the following information:

- Host name
- Port number
- Username (Local DB user, Windows authentication is **NOT** supported)
- Password
- Database type (e.g., Oracle, MSSQL)
- Database name
- Database owner