



Production Environments – Preparation Sheet (Content Server to SPO)

To ensure migration readiness is achieved, Gimmel recommends the following action items are prepared in advance.

PRODUCTION ENVIRONMENTS	
Destination SharePoint Online environment <ul style="list-style-type: none"> Available as a destination migration repository 	SharePoint Tenant Url:
Azure Storage <ul style="list-style-type: none"> Adequate blob storage capacity <ul style="list-style-type: none"> Minimum: Standard performance, Read-access geo-redundant storage (RA-GRS), Storage (general purpose v1) Tenant geo location – same as SPO if possible Network speed: recommended upload speed > 200 Mbps to ensure optimal migration performance <ul style="list-style-type: none"> Azure ExpressRoute Circuit is nice to have, or a fast connection 	Azure Storage Account Name: Azure Storage Account Key:
Network Drive Storage or local disk <ul style="list-style-type: none"> High speed storage and appropriate capacity located within same network / data center as Content Server (ex. 1 TB) For temporary Azure package preparation 	Storage Path:
Source Content Server environment <ul style="list-style-type: none"> Enterprise Content Web Services Enabled Records Management Web Services Enabled (optional) See Content Server Requirements checklist for additional requirements (If you require assistance with configuration of CWS please contact us and we can assist you with the configuration.)	Content Server URL: Enterprise Content Web Services Path: Records Management Web Services Path:
Windows Server environment – if deploying Legacy Link Redirector <ul style="list-style-type: none"> Windows Server box (ex. Windows Server 2008 R2 and up), IIS 7.0+ AD Login account with adequate local privileges 	Server Name:
SQL Server Database <ul style="list-style-type: none"> The database is used for storing migration profiles Provide SQL Server Account (Windows or SQL) credentials Enable mixed mode authentication See SQL Server Database Requirements checklist for additional requirements A highly available, stable and performant database is required for use. We recommend the database is provisioned in the same data center where your Content Server and Migration VMs are located. A reliable and performant database server is required to ensure optimal migration speeds are achieved.	Account Name: Password: Server Name, Database Name and Port:

ACCOUNTS (REQUIRED)	
<p>Content Server migration service account (ex. CSMigrationAccount)</p> <ul style="list-style-type: none"> • With appropriate read access to Content Server source Collections • We strongly recommend granting the service account System Admin privileges in Content Server to ensure all content is read accessible 	<p>Service Account Name:</p>
<p>At least one O365 service account(s) for migrations. You can use an existing AD Account from Azure or create a new cloud managed service account for migration purposes (ex. SPMigrationAccount).</p> <ul style="list-style-type: none"> • We recommend you create a cloud managed service account (ex. SPMigrations@yourdomain.onmicrosoft.com) • This account must have login enabled and be specified as a Site Collection Administrator for the migration destination Site Collections <p>Authentication Mechanisms:</p> <ul style="list-style-type: none"> • MAPIT supports 2 modes of authentication – Legacy Authentication and Modern Authentication in O365 using Application ID Delegation <p>Legacy Authentication:</p> <ul style="list-style-type: none"> • This mode does not support using multi-factor authentication in O365, as such you must disable MFA for this account • If you have Azure conditional access policies enabled, you will need to whitelist the newly created account (no blocking legacy authentication) <p>Modern Authentication</p> <ul style="list-style-type: none"> • You must have your O365 Global Administrator grant a one-time authorization from within MAPIT to Gimmel’s Application ID access to your O365 SharePoint Online environment on your behalf to run migrations in delegated mode 	<p>Service Account Name 1:</p> <p>Password:</p> <p>Service Account Name 2:</p> <p>Password:</p> <div data-bbox="1047 1050 1112 1123" style="text-align: center;">  </div> <p>The recommended login mechanism recommended by Microsoft is to use Modern Authentication with App ID. This will allow you to achieve fastest migration speeds versus the old mechanism. If you use the Legacy Authentication mechanism your migrations will be significantly slower.</p>
<p>AD Login account – for network drive access</p> <ul style="list-style-type: none"> • With full read/write access • For migration access purposes 	<p>AD Account Name:</p>
<p>AD Login account – for Content Server</p> <ul style="list-style-type: none"> • With System Admin level privilege to the Content Server test environment <ul style="list-style-type: none"> • To enable access for analysis, validation, and config if required • For Content Server validation purposes 	<p>Same as above</p>
<p>AD Login account – for SharePoint Online</p> <ul style="list-style-type: none"> • Site Collection Administrator level permissions to SharePoint environment <ul style="list-style-type: none"> • For required analysis, validation, and configuration access • SP Global Admin and Content Type Hub access is nice to have • For SharePoint Online validation and configuration purposes 	<p>Same as above</p>

ACCOUNTS – Optional for use with the Content Server Discovery, Analytics and De-Duplication Tool	
 This tool directly queries the Content Server database to conduct advanced queries and reporting. As such you must provide database credentials with the required minimum read access role to the entire Content Server schema. The User ID specified must have default schema set to the Content Server schema. * If using Oracle please specify TNS name info or file location for Oracle	Database Account Name: Content Server Production Database Connection Details:
MIGRATION CLIENTS	
<p>Client PCs – Migration Clients</p> <ul style="list-style-type: none"> • Recommend 1 - 5 dedicated Client PCs (ex. VMs) depending on number of migration resources and planned migration thread usage • On same internal network as Content Server <ul style="list-style-type: none"> • Same datacenter if applicable • CPU Intel i7 or equivalent • Windows 7 or 10, 64-bit OS • 16+ GB of RAM • Recommend PC with 4-8 processor threads for best performance • Login account with local admin rights for software installs (if possible) <p>Install Gimmel Migration Tools Client/Host PC must be satisfied:</p> <ol style="list-style-type: none"> 1.) Must have .NET Framework 4.7.2 installed on host where the tools will be run 2.) Must be installed on either Win 7 or 10, 64-bit Operating System <p>If using Legacy Authentication mode, you must perform steps 3-5. If using Modern Authentication in O365 mode, you can skip directly to step 6.</p> <ol style="list-style-type: none"> 3.) Install Azure AD PowerShell V2.0 <ul style="list-style-type: none"> • Open Windows PowerShell command prompt as Administrator • Run the following command <ul style="list-style-type: none"> • Install-Module -Name AzureAD -RequiredVersion 2.0.0.115 • Enter 'Y' for Nuget provider is required message • Enter 'A' for Untrust repository (A is Yes for all) 4.) Install SharePoint Online Management Shell 5.) If installing on Windows 7 – please install Windows 6.1-KB file (not required for Win10) 6.) Please confirm pre-requisites are installed prior to installing migration tools <ol style="list-style-type: none"> a. Install Content Server Analytics and Deduplication Tool b. Install Content Server Exporter c. Install MAPIT for O365 <p>* If installing on Windows 7 or Windows Server 2008 R2 – see section 1.2 Client Software Pre-Requisites of the MAPIT for O365 user guide. This will provide the full requirements required to install.</p>	PC Name 1 (required): PC Name 2: PC Name 3: PC Name 4: PC Name 5:
<p>Remote Access</p> <p>If the nature of the engagement requires remote access – please ensure Remote VPN access is also made available.</p>	

Client Resource Availability Assumptions

Client resources should be available to assist as required from a technical perspective for the tool configuration and training phases.

- Client project analyst resource responsibility:
 - Work with internal business and project stakeholders as required
 - Perform testing and validation
 - Provide scope and decision making
- Client Content Server and SharePoint resources:
 - Set up appropriate access to CS and SP (provide account ids and passwords)
 - Help with initial setup. (ie. web service urls)
 - Configure permissions in SharePoint
 - Answer questions about environment and provide architecture diagrams
 - Additional environment investigation, configuration or optimization as required
- From the Database side, we would require resource to create the actual DB and provide credentials
- Link Redirector
 - Someone to assist with the IIS specific configuration from Client perspective