



# DataMart Client Server Setup Guide

Version 0.1

## AUDIENCE

This guide is intended for a user who is familiar with the setup of Microsoft Internet Information Services (IIS), and Microsoft SQL Server. The configuration of the DataMart Client Server (DMCS) will be the responsibility of the end user administrator. The administrator will be responsible for the configuration of the DMCS instance within their own network. Maintenance and availability will be the providence of the end user administrator.

This guide is intended to provide guidance for the configuration of the DMCS instance.

## MINIMUM SYSTEM REQUIREMENTS

- Microsoft Windows 8.1 or Microsoft Windows Server 2012 R2
- Microsoft SQL Server 2014
- ASP.NET Core 3.1 Runtime Hosting Bundle
  - <https://dotnet.microsoft.com/download/dotnet/3.1>
- Internet Information Services (IIS)

## CONFIGURATION

### File/Directory Setup

- Inside of the deployment package the root folder for the website is “DMCS”. This folder should be placed in the desired IIS website root folder.
- If upgrading the DMCS application, all of the contents of the existing DMCS except the appsettings.json file should be deleted before being replaced by the new application files. I.E. do not just extract the new application package over the old one – replace the files.
- A folder should be chosen to act as the cache for files uploaded and downloaded by the application. Local or internal network locations are valid.

### Database Setup

- Installation and configuration of the database server is the responsibility of the administrator configuration the application.
- An empty database should be created – naming of the database does not have a required format.
- The method of accessing the database is up to the discretion of the administrator so long as it can be expressing in a common connection string format.
- Note: the identity used by the application to access the database must have enough permission to allow it to read, write, update, delete, and modify tables and columns.

### Internet Information Services Setup

- Installation and configuration of the IIS instance is the responsibility of the administrator configuration the application.
- The DMCS application requires the ASP.NET Core Module be installed. The module should be installed after the installation of IIS but prior to creating the DMCS website.
  - After installing the module the server will need to be restarted or the following commands executed from an elevated command prompt:
    - “net stop was /y”
    - “net start w3svc”
- Create the website for the DMCS application; provide a site name and set the physical path to point to the “DMCS” folder from the installation package. Configure the desired bindings, and transport.
- Confirm the process model identity (the identity the site is running under) has proper permissions. The identity will need read/write permissions to the cache folder, and the website root folder.

## DMCS Configuration

Set the following configuration settings, all other settings have default values:

- ConnectionStrings: DBContextConnection
- PopMedNet: NetworkName and ApiServiceURL
- Settings: CacheFolder

ConnectionStrings		
DBContextConnection	Connection string for the database. Example: Server=localhost;Database={database name};Integrated Security=SSPI;MultipleActiveResultSets=True;  Server=192.168.0.1:1452;Database={database name};User ID={username};Password:{password};MultipleActiveResultSets =True;	
PopMedNet		
NetworkName	The name of the network the application is connected to. Displayed as the name of the application.	
ApiServiceURL	The qualified url to the PMN API. This is the same value as used in the DMC.	
ServiceUserCredentials	Service user account credentials, used to authenticate to the PMN API when a specific user account is not available/applicable.	
	UserName	The username of the identity the DMCS application will use to authenticate to the PMN API as. This is a service user account, do not change unless instructed to.
	EncryptedPassword	The password of the service user account.

Settings	
DMCSIdentifier	A unique identifier for the DMCS instance. If empty the application will automatically generate an identifier. It is recommended to let the application generate the value. If the administrator wishes to generate a specific identifier it must be a valid GUID in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx.
CacheFolder	The full path to the cache folder. The folder must be accessible for read and write operations by the DMCS application. Network paths to file shares are valid.
CacheFolderTimer	The interval for how often the caching service should check for expired cache items in minutes.
Hash	The salt hash used for encrypting cached items.
Key	The encryption key used for encrypting cached items.
SyncServiceInterval	<p>The time interval between synchronizations with the PMN API. Default is 1 minutes.</p> <p>Format: [days -optional with period delimiter]hours:minutes:seconds d.hh:mm:ss</p>
Application	
LockoutTime	* Not currently implemented.
LockoutCount	* Not currently implemented.
SessionDurationMinutes	The duration of the user session in whole minutes. Will logout a user if there has been no activity within the duration.
SessionWarningMinutes	The duration prior to session ending that a warning should be shown to the user. The warning dialog will provide an opportunity for the user to refresh their session.
Serilog	

Logging configuration settings, not recommended to change. Logging is configured by default to store in the DMCS database, any configuration in this section is additional and overrides. Refer to Serilog documentation for setting values.

See: [Serilog — simple .NET logging with fully-structured events](#)

AllowedHosts

A comma delimited list of hostnames allowed to access the application. Default is “\*” which allows for all non-empty hostnames. Not recommended to change.

See: [HostFilteringOptions.AllowedHosts Property \(Microsoft.AspNetCore.HostFiltering\) | Microsoft Docs](#)