

EasyMorph Server Administrator Guide

Version 5.4

Jan 22, 2023

Table of Contents

- TABLE OF CONTENTS..... 1
- PREREQUISITES 3
 - Memory requirements* 3
- INSTALLATION..... 3
 - First login* 4
 - License key* 5
 - System folder* 5
 - The "EasyMorph Server" group*..... 6
- SERVER SERVICE ACCOUNT 6
 - Changing Server service account* 7
- UPDATING FROM PREVIOUS VERSIONS 7
- CONNECTOR REPOSITORY 7
 - Repository encryption* 8
- CONFIGURING SPACES 8
 - The Default space*..... 9
 - Space worker*..... 9
 - Access modes* 10
 - Connector repository access for Desktop users*..... 11
 - Arbitrary code execution* 11
 - Execution of unsigned projects* 11
 - File/folder picker locations*..... 11
- SPACE ACCESS RESTRICTION 12
 - Anonymous* 12
 - Password-protected* 12
 - Windows Authentication (Enterprise edition only)* 12
- ACCESSING THE PUBLIC FOLDER..... 13
 - Web File Manager*..... 13
 - Network Share* 14
 - EasyMorph Server Command*..... 15
 - Third party FTP or SSH server* 15
- LEASING LICENSES TO DESKTOP USERS FROM SERVER..... 15
 - Assigning Dynamic licenses*..... 15
 - Quarantine* 17
 - Oversubscription* 17
- USER LICENSING FOR DATA CATALOG 17
 - Professional users (creators)*..... 18
 - Regular users (consumers)* 18
 - Accessing the Catalog* 18
- JOURNAL 18
 - Failover switching* 19
 - User interface*..... 19

<i>Task journal</i>	20
<i>Journal cleanup</i>	20
WORKERS.....	20
<i>The Default worker</i>	21
<i>Additional workers (Enterprise edition)</i>	21
<i>Run spaces under different Windows accounts</i>	21
<i>Recycling workers</i>	22
<i>Mapped drives</i>	22
TAB PAGES	23
EMAIL NOTIFICATIONS ABOUT FAILED SCHEDULED TASKS	24
<i>Email notifications in spaces</i>	25
FILE LOCATIONS	25
REMOTE ADMINISTRATION	26
SERVER MONITOR	26
HTTPS-ONLY MODE	27
SECURITY CONSIDERATIONS	28
<i>Cloud hosting</i>	28
START/STOP BATCH SCRIPTS	28
LOGGING	28
DATA PERSISTENCE AND LOCALITY.....	29
COMMAND-LINE API CLIENT	29
EASYMORPH SERVER .NET SDK	29
UNINSTALLATION	29
DESKTOP TO SERVER LINK	30
UI CUSTOMIZATION	30
TROUBLESHOOTING	31
<i>Technical support</i>	31

Prerequisites

- 64-bit version of Windows 10 (or above) or Windows Server 2016 (or above)
- .NET 4.7.2 ([link](#))
- MSVC++ 2015 Redistributable Packages ([link](#))
- Tableau drivers require MSVC++ 2013 Redistributable Packages ([link](#))
- The PowerShell action requires PowerShell v3 or above installed ([link](#))
- 200 MB free disk space

Memory requirements

EasyMorph Server is a memory-intensive application because it processes all data in memory. The required amount of RAM greatly depends on data volumes processed by Server workflows. Therefore, estimating exact memory requirements is not so straightforward. Due to aggressive on-the-fly data compression in EasyMorph, the amount of RAM consumed highly depends on data types and cardinality. A very (very!) rough rule of thumb is 4GB plus 1GB per each 1 million rows in the largest dataset to be loaded entirely in a workflow. Add up dataset sizes for simultaneously executed workflows.

It's possible to use EasyMorph Desktop to obtain memory consumption estimates because both EasyMorph Server and EasyMorph Desktop employ exactly the same in-memory engine under the hood. Run actual projects with real data in EasyMorph Desktop first and track memory consumption in Windows Task Manager. Keep in mind that EasyMorph Server typically requires up to 10-20% less memory than Desktop due to server-specific optimizations.

What would happen if the Server runs out of memory? The system would become unstable and would behave unpredictably. In the best case, depending on system settings Windows will try to allocate more memory by swapping parts of RAM to disk. This will drastically slow down project execution, delay scheduled tasks and possibly break schedule frequency, and can even make the Server unresponsive for a period of time. In the worst case, project execution will fail producing an "Out of memory" error.

When processing large amounts of data, consider partitioning and processing your data chunk by chunk using iterations.

Note that memory is only consumed when a task is running. As soon as a task is finished all the memory used by the task is freed up. When idle, the memory footprint of the Server is insignificant (a few tens MBs) and constant.

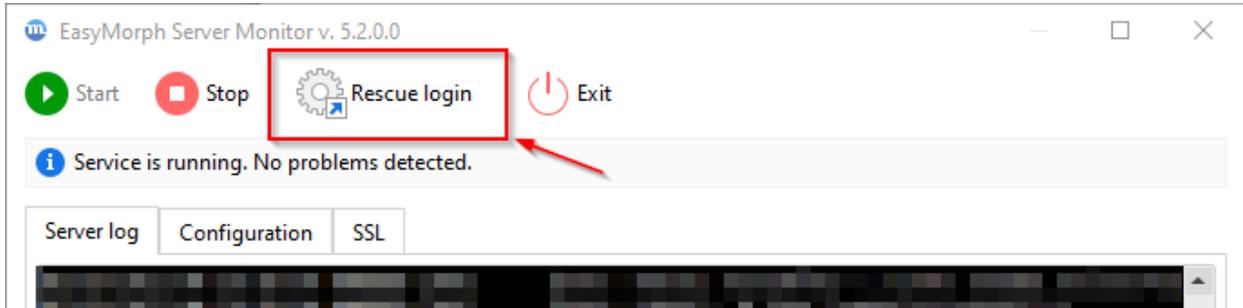
It's recommended to have a reserve of memory to avoid running out of memory. To help detect possible memory deficit, EasyMorph Server logs warnings into the Server log when available RAM falls below 20%. Also, the tab "Task" of the Server's web-console and the administrative tabs display a live indicator of available memory.

Installation

Run the installer under a Windows administrator account and follow instructions.

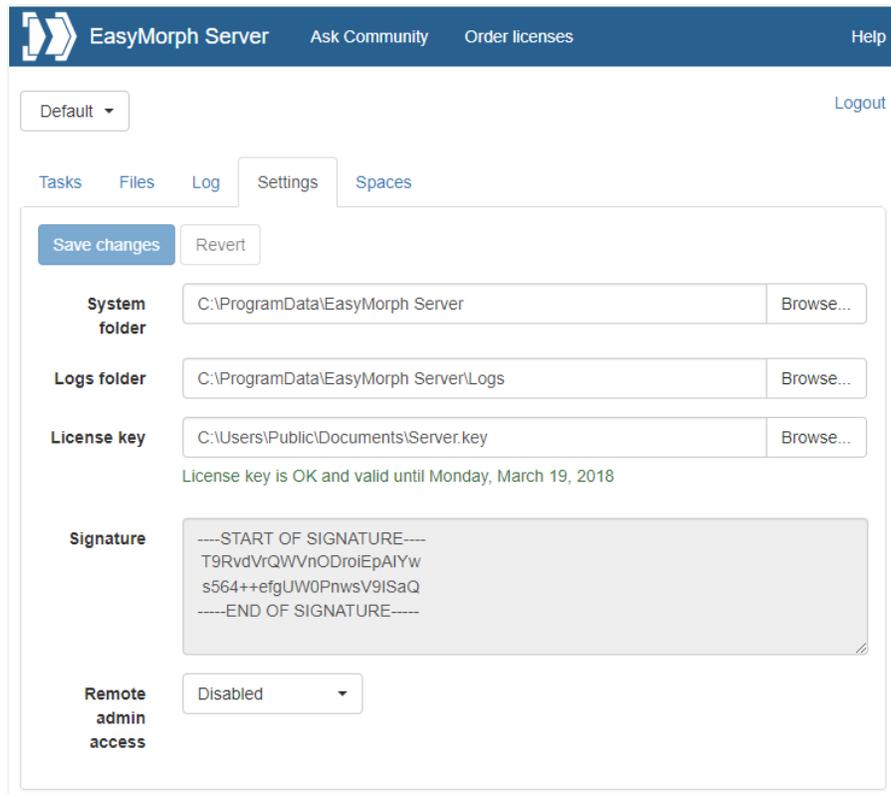
First login

After successful installation, EasyMorph Server starts automatically. Also, the Server Monitor, a Server configuration utility described in detail further in this guide, is launched simultaneously.



Screenshot 1: The "Rescue login" button in Server Monitor.

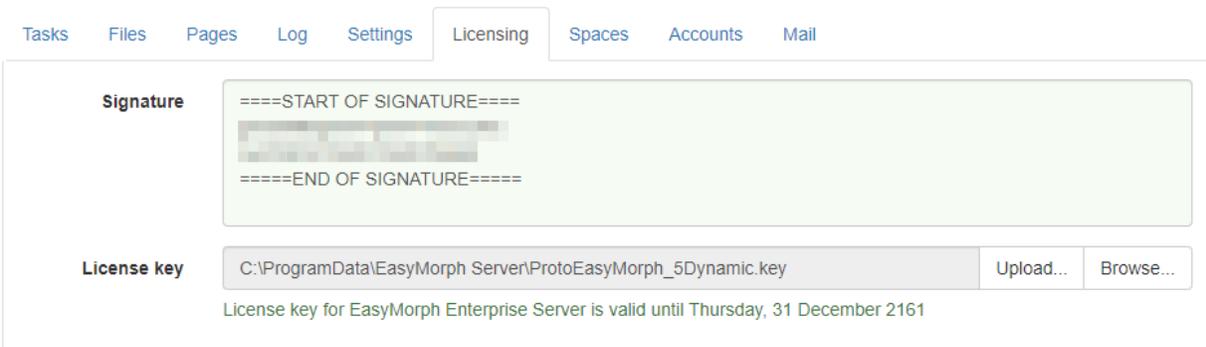
Press the "Rescue login" button on the toolbar of Server Monitor. This will open your web browser with the following URL: <http://localhost:6330/settings/edit>. The "rescue login" allows accessing Server as administrator (from the local group "Administrators") without a password on the computer where EasyMorph Server is installed. You can later configure remote administration and a password in Server settings and log in as administrator using a web-browser.



Screenshot 2: Server Settings page

License key

Send the digital signature from the Licensing tab (see "Screenshot 3: Installation signature in the Licensing page." below) to sales@easymorph.com to request a license key for the Server, if you don't have it yet. After applying a valid license key the Server is ready to use. Note that the key should be placed into a folder that is accessible by the Server service account. For that, permit the Windows account group "EasyMorph Server" to access the folder with the license key.



Screenshot 3: Installation signature in the Licensing page.

A license key may have a mix of Server and Desktop signatures. The contents of the key can be seen in the license certificate (a PDF file) that comes with the license key. One key can be used for Server and Desktops.

Note that when computer name or domain name changes the Server signature also changes. Therefore if you migrate your Server to a different machine, contact sales@easymorph.com in order to transfer your license to another computer.

Note that Desktop user licenses can also be administered from the Server's web-console. See chapter "Leasing licenses to Desktop users from Server" below.

System folder

The system folder contains internal Server files required for Server operation. Note that the system folder doesn't contain user workflows or data – they are located in the Public folder specified in the space settings. It is recommended to not change the path of the System folder. However, if you need the system folder to be in another location, use a local drive. Using network drives (mapped or not) is not recommended because network drives don't provide the necessary file consistency guarantee¹ for the SQLite database that is used internally in EasyMorph.

Note that the System folder and all the files and subfolders in it must allow full access for the "EasyMorph Server" Windows account group. The group is created by the EasyMorph installer automatically.

¹ See <https://www.sqlite.org/draft/useovernet.html>.

The "EasyMorph Server" group

The Server installer automatically creates the Windows account group "EasyMorph Server". The group contains² the Service account. The group simplifies folder access management, for instance, when the Server service account needs to be changed. By default, the system folder, the log folder, and the Public folder of the Default space also allow full access to the group "EasyMorph Server". If you need the Server service account to access some other folder, allow the "EasyMorph Server" group to that folder, instead of allowing the Service account explicitly.

Installing EasyMorph Server on a machine that serves as Windows Domain Controller is not recommended, but still possible. In this case, the Server installer will fail to add the Server service account (explained below) to the group due to Windows-specific restrictions on Domain Controllers. You will have to manually create or ensure that the access group "EasyMorph Server" (the exact name and case matters) exists already. Create a technical user account to run EM Server service, set the Server service to use this account as Logon account in Windows service settings, and finally, add this technical account to the "EasyMorph Server" group. Failing to do any of these steps could lead to hard-to-diagnose issues (e.g., the Server service having no/partial access to its own configuration files).

Server service account

By default, the Server service is installed under the local Windows account *NT AUTHORITY\LocalService*, not the account under which the installer was run. The *NT AUTHORITY\LocalService* account is a standard account for Windows services. It has fewer privileges than an administrator account. For instance, it can't access the users' Documents folders and other protected locations. If you need the Server to access a particular folder, there are 3 possible solutions:

- make sure that the service account has been given necessary access permissions;
- or, switch the Server service to using a different Windows account that has the necessary permissions;
- or, configure a Server worker to use a Windows account that has necessary permissions in the Server settings, and use the worker for the space which tasks require the permissions. Read more about Server spaces and workers in chapters "Configuring spaces" and "Workers" respectively.

Also, when using "Windows authentication" in the connector properties, keep in mind that the connection will be established using the Windows account specified in the settings of the Server space worker from which the connection is established. Use explicit login/passwords for accessing databases, instead of integrated Windows authentication, if necessary. Alternatively, add the Default worker's Windows account (by default it's *NT AUTHORITY\LocalService*) to database logins.

² The "EasyMorph Server" group was introduced in v5.2 and can be empty if your Server was installed from an earlier version. In this case, just add the current Service account to this group.

Changing Server service account

Generally, it's not recommended to switch the Server service account after the Server was in use. In the Enterprise edition it is possible to configure spaces to use different Windows accounts (see chapter "Workers"). Consider using this capability before changing the service account.

If you still need to switch the Server service to another Windows account:

- 1) Add the new account to the "EasyMorph Server" Windows account group.
- 2) Make sure that the new account can access the Public folder of the Default space or other spaces, if necessary.
- 3) Stop the service.
- 4) Change the "Log On" account setting in the EasyMorph Server service properties in Windows Services panel to use the new account.
- 5) Start the Service.
- 6) Remove the old account from the "EasyMorph Server group".

Updating from previous versions

To update from a previous version:

- 1) Stop the EasyMorph Server service
- 2) If the service is installed under a different account than LocalService then write down that account and make sure you know its password.
- 3) Check the Release Notes if it contains a clear demand for uninstalling the previous version before installing the new one. If it does not (which is typical) then skip to the next step. If it does, uninstall EasyMorph Server. Do not uninstall the previous version unless it explicitly requested in the Release Notes.
- 4) Install the new version. In the installer choose "Use existing configuration" (selected by default).
- 5) The Server service will be installed under the default account (LocalService). If your EasyMorph Server previously used a non-default account, change the "Log On" account in the EasyMorph Server service properties in Windows Services panel.
- 6) Start the Server service using either the Server Monitor (see "Server Monitor"), or the Windows Services panel.

Connector repository

EasyMorph has a repository of pre-configured connectors that are used by EasyMorph workflows (including those executed by EasyMorph Desktops) to access database servers, email servers, and various external services and applications. The repository is technically a SQLite database file. Note that the repository doesn't store the actual data from external systems. It only stores the connector settings (e.g. connection strings).

The initial EasyMorph Server installation comes with an empty connector repository in the Default space. You can see the path to the repository in the space settings page. To add, edit, and delete connectors in the repository use the Connector Manager of EasyMorph Desktop.

A new space by default points to the repository of the Default space. During space creation you can choose to create a new repository for the new space, or point it to another repository, if necessary.

EasyMorph Server uses the same repository format as EasyMorph Desktop. Therefore if a repository was created with EasyMorph Desktop it can be uploaded to Server and used by Server.

From a security standpoint, it is recommended to use Server-hosted repositories on Desktops. In this case, the repository file is not accessible directly from Desktop. Instead, the Server provides connectors to Desktops on demand. Connectors in a Server-hosted repository can be edited from Desktop. For more details read the chapter "Connector repository access for Desktop users" below.

Important! Do not share the same repository file between Server and Desktops via a shared network folder. The Server coordinates access permissions and resolves access conflicts. However, if the repository file is accessed as a file directly by some Desktop, this may interfere with Server operation and cause a database file lock.

Repository encryption

Since repositories can contain connectors to sensitive data and the connector settings can include credentials and API keys, all repositories are encrypted using a 2048 bit encryption algorithm.

For better protection, it's possible to configure read and write passwords for repositories.

The read password is required for retrieving connectors from a repository and is configured in space settings. Desktop users don't need to provide a read password to access connectors in a Server-hosted repository.

The write password, when set, must be provided by users when they need to create a new connector, or update/delete an existing connector from EasyMorph Desktop.

Configuring spaces

The purpose of Server spaces to separate and manage access to tasks and files for different user groups. Each space is independent from other spaces, and has individually configured:

- Tasks
- Custom API endpoints
- Public folder (accessible through a web-browser or by other means, e.g. API)
- Server worker (its Windows account is used to run tasks and access files in the space)
- Connector repository and its availability to Desktop users
- Root folder for Pages (if Pages are enabled)

- User access list (for spaces with Windows Authentication)
- Space security settings
- File/folder picker locations
- Email notifications about failed tasks

The tasks of a space are stored as XML files in subfolders in the system folder defined on the Server settings page. Each subfolder corresponds to a space.

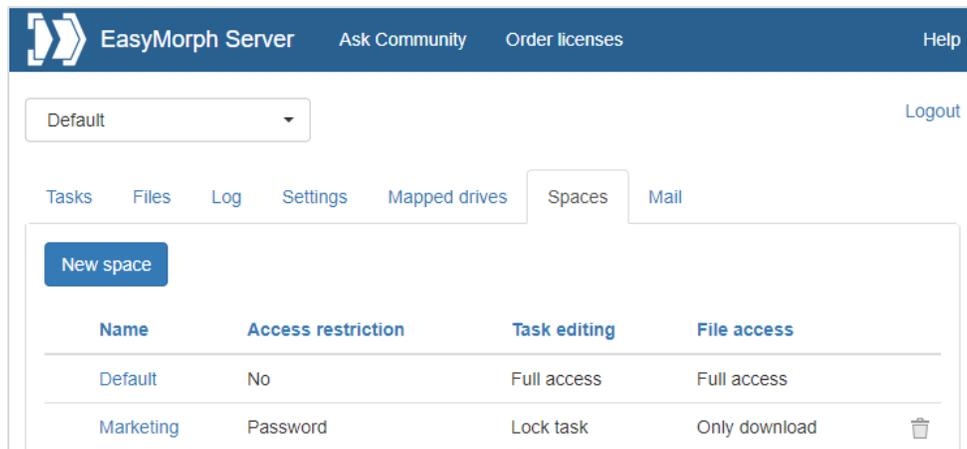
The API endpoints of a space are stored as XML files in the public folder, in the subfolder named ".endpoints".

Two spaces can point to the same public folder, or have nested public folders (i.e. the public folder of one space is a subfolder of the public folder of another space).

Two spaces can refer to the same repository file. It is recommended to keep the repository file outside of the public folder in order to restrict user access to it.

Spaces can't share the same list of tasks or list of users.

Spaces are managed in the tab called "Spaces" visible only to a Server administrator.



Screenshot 4: Spaces.

The Default space

The Default space is created automatically during the initial Server installation. It must not be removed or renamed. If the Default space is missing then it will be created automatically again.

Note that if an API command omits space name, it is implicitly assumed that it's related to the Default space.

Space worker

By default, a space runs tasks and accesses files under the Windows account that is used to run the Server service (see "Server service account" above). It's called the Default worker.

In the Enterprise Edition it is possible to create workers that use another Windows accounts and assign them to spaces. Such spaces will run tasks and access files using worker's Windows account instead of the Default account. For more information read "Workers" below.

Access modes

Spaces allow limiting access to tasks using one of the 4 modes:

- Disabled – tasks are entirely disabled and not available in this particular space.
- Lock task – a user can only trigger tasks, but not create or edit them.
- Lock project – a user can edit task schedule, task parameters, but not create tasks, or change the project in a task.
- Full access – no restrictions, the only mode where new tasks can be created.

Accessing API endpoints has 3 modes:

- Disabled (in the space settings) – API endpoints are not available in this space
- Full access
- Read-only access – API endpoint configurations can't be modified

Accessing files in the public folder (and its subfolders) of a space via EasyMorph Server (or its API) can also be done in different modes:

- Disabled – files are entirely disabled and not available in this particular space.
- Download only – files can only be downloaded, but not uploaded or deleted (basically the read-only mode).
- Upload only – files can be uploaded or deleted, but not downloaded.
- Full access – no restrictions.

Note that these file access modes do not change folder permissions of the Windows account used by the space. If the Windows account has full access to the public folder, setting "File access mode" to "Disabled" won't prevent other applications (e.g. executed by a task in this or another space) from accessing files in the public folder.

A combination of a task access mode with one of the file access modes allows flexibly configuring spaces for different types of users and use cases. For instance:

Use case	Task access mode	File access mode
External data suppliers that are required to only provide files with source data.	Disabled	Upload only
Marketing analysts that upload files, trigger pre-configured tasks, and collect results.	Lock task	Full access
Sales department employees that need to generate a report on demand. They run a pre-configured task and provide their employee ID as a task parameter.	Lock project	Download only
Power users that use a dedicated server to perform ad hoc heavy data transformations.	Full access	Full access

Table 1: Examples of use cases for spaces.

Connector repository access for Desktop users

Users of EasyMorph Desktop can access the space's connector repository right from their Desktops. To use the space's repository, Desktop users should configure the Server Link in their EasyMorph Desktops and then switch to using Server Link in the Connector Manager. Note that when a Desktop user uses a Server-hosted connector, the connection is established from the user's computer, not from the Server. No data is transmitted between Server and Desktop when a Server-hosted connector is being used on a Desktop.

The setting modes:

- Disabled – Desktop users can't access and Server-hosted repositories at all
- Read-only – Desktop users can access and use Server-hosted repositories, but not create, or edit, or delete them
- Full access – Desktop users can access, use, create, edit, and delete Server-hosted connectors

It is also possible to disable/enable copying connectors to Clipboard for Desktop users that use a Server-hosted repository.

Arbitrary code execution

Workflows in EasyMorph projects can have actions that can execute an arbitrary code (e.g. a script or an application), specifically, the "Run program", "Iterate program", "PowerShell", and "SSH Command" actions. Under certain conditions this can be undesirable from a security standpoint, especially when projects are executed under the built-in Default worker (that can access system files of Server). The "Arbitrary code execution" setting can be used to disable execution of such actions in projects.

Execution of unsigned projects

Projects edited in EasyMorph Desktop are digitally signed. If a project is modified outside of EasyMorph, its digital signature becomes invalid. When EasyMorph Server executes a project, it verifies signature validity and disables project execution if the project was modified by a 3rd party outside of EasyMorph and its signature became invalid. Project signing provides an additional layer of security.

File/folder picker locations

The "Locations" tab in the space settings allows specifying drives that are shown in the file/folder picker dialog. The dialog is invoked when a task parameter is specified, and the corresponding project parameter has type "File path" or "Folder path".

Note that the locations only specify which drives are shown in the file/folder picker dialog. They do not restrict physical access to disk drives for particular space, and can't be used to restrict access to local and mapped drives.

Space access restriction

A space can use one of the three possible authentication modes:

- Anonymous
- Password-protected
- Windows Authentication (uses Active Directory for user authentication)

Anonymous

In this mode, anyone can access the space. No authentication is performed.

Password-protected

A space can be password-protected. In this case, users should provide the correct password in order to access tasks and/or files in the space.

Performing operations through the Server API (e.g. using the "ems-cmd" utility) with password-protected spaces also requires providing a password.

Windows Authentication (Enterprise edition only)

In this mode, there is an explicit list (whitelist) of users and user groups that are permitted to access the space. Users are identified by their Windows accounts (e.g. DOMAIN\username) and verified against an Active Directory service. A valid connection to Active Directory must be configured in the Server Settings page in order to use this access mode for a space.

Add new User AD group

Name

Note

User/group	Note	
DOMAIN\User301		
DOMAIN\User401		
DOMAIN\tdtestuser		
DOMAIN\LS	it's a group	
DOMAIN\GS	it's another group	

Screenshot 5: Configuring users and groups of a space.

Note that AD groups must be of "Security" type (configured in Windows AD group properties) to be authenticated by EasyMorph Server. If a group's type is set to "Distribution", the group can't be used for user authentication in EasyMorph Server.

Accessing the Public folder

The public folder of a space is configured in the space settings.

The folder is meant for:

- Storing EasyMorph projects (.morph files) used by Server tasks
- Storing/sharing EasyMorph datasets (.dset files)
- Collecting data files required for Server tasks
- Publishing/sharing output files produced by Server tasks
- Sharing EasyMorph projects between users

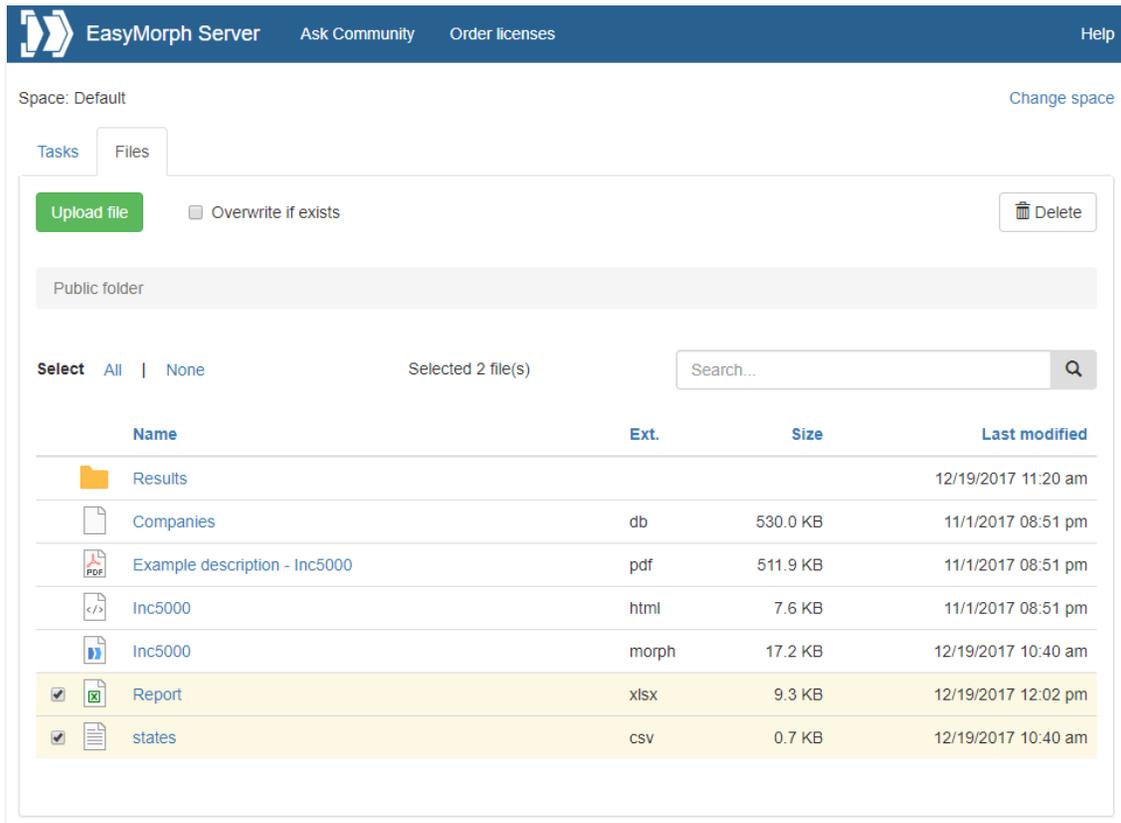
For convenience, it is recommended to store EasyMorph projects in a folder structure with a common root folder, separately from data files. Storing all projects under a common root folder is convenient for performing backup/restore or using a 3rd party version control system (such as git). It also allows using relative paths to refer to input data and helper files, which is convenient for publishing projects from a user's computer to Server.

Access to the public folder can be done in one of the following ways:

- Using the built-in Web File Manager (i.e. via a web browser)
- Making the folder a shared network share
- Using the ["EasyMorph Server Command" action](#)
- Using *ems-cmd* command line utility (see Command-line API client below)
- Installing a 3rd party FTP or SSH server

Web File Manager

EasyMorph Server has a built-in Web File Manager that allows uploading files to and downloading files from a public folder via a browser. Click the tab Files to open the Manager.



Screenshot 6: Web File Manager.

The Web File Manager allows performing the following file operations:

- Browse folders
- Upload one or multiple files by dragging them into browser, or by pressing the “Upload file” button
- Download a file by clicking its name
- Create, rename, or delete a folder
- Rename 1 selected file
- Delete one or more selected file(s)
- Find a file in the current folder

Note that in the current version it’s not possible to delete folders that are not empty. All files and folders must be removed from a folder and only then it can be deleted.

Network Share

Alternatively, the Public folder can be exposed as a network share accessible across the local network. Once it’s shared you can place projects and data files into that folder (or its subfolders) and create Server tasks that run them.

EasyMorph Server Command

The “EasyMorph Server Command” action allows uploading/downloading files to/from a public folder (or its subfolders) from EasyMorph projects executed on desktops or other Servers. No additional software installation is required.

Third party FTP or SSH server

You can setup a 3rd party FTP or SSH server and upload/download files to the Public folder over the FTP or SSH protocol (e.g. by using the “File transfer” action in EasyMorph).

Leasing licenses to Desktop users from Server

Assigning Dynamic licenses

A license key may include one or more packs of Dynamic licenses. When a license key with at least one valid pack of Dynamic licenses is applied on EasyMorph Server, the Server can assign (lease) licenses to Desktop users dynamically.

For example, a pack contains 5 Dynamic licenses. It means that 5 Desktop users can be assigned a license from Server by a Server administrator. If a Dynamic license needs to be transferred to another user or revoked, a Server administrator can do this right from the Server's web console.

Tasks Files Pages Log Settings **Licensing** Spaces Accounts Mail

Signature ====START OF SIGNATURE====
[Redacted]
=====END OF SIGNATURE=====

License key

License key for EasyMorph Enterprise Server is valid until Thursday, 31 December 2161

License packs

Pack name	License type	Expiration date	Total	Available	Assigned	Oversubscribed
Main pack	Professional	2021-01-14	5	2	3	-
Total Professional			5	2	3	0

Assigned user licenses

Select [All](#) | [None](#)

User	Pack name	License type	Tags	Last activity	Status
CORP\kristina	Main pack	Professional	sales	a minute ago	In use (4.5.2.4) <input type="button" value="edit"/>
CORP\peter	Main pack	Professional	sales	Never	Unused <input type="button" value="edit"/>
CORP\dmitry	Main pack	Professional	IT, admin	6 minutes ago	In use (4.5.2.4) <input type="button" value="edit"/>

[Download list](#)

Screenshot 7: Dynamic license assignment.

A new license assignment can be created by pressing the "Assign license" button visible in the screenshot above. When a new assignment is created, it's added to the license assignment table also visible in the screenshot above.

For Desktop users, in order to lease a license from Server, the Server Link must be configured (see "Desktop to Server Link" below), and the "Lease license from Server" must be selected in the "License setup" dialog (invoked by pressing the "Setup license key" in the Start screen of EasyMorph Desktop).

Each license lease lasts for 48 hours and is renewed automatically every 48 hours for each user who is assigned a license from Server. For a license to be renewed automatically, the Server Link must remain configured on Desktop, and Server must be reachable by network.

A license assignment can have one of the following statuses:

- **Unused** – user never requested a license from Desktop.
- **In use (version number)** – user has successfully leased and is currently using a dynamic license.

- **Quarantined** – license was recently deleted or transferred to another user and therefore is temporarily blocked from use (more on the quarantine below).
- **Oversubscribed** – user should have been assigned a license from a pack but there are more license assignments than available licenses in the pack.
- **Missing pack** – user should have been assigned a license from a pack but the pack is missing in the current license key.
- **Expired pack** – user should have been assigned a license from a pack but the pack is expired in the current license key.

Quarantine

When a license assignment record was deleted or edited, the license that was assigned may be temporarily quarantined. The purpose of the quarantine is to prevent a simultaneous use of a Dynamic license by two or more users (which would be a violation of the software licensing terms). The duration of the quarantine depends on when the license was last used before it was deleted or re-assigned. If the license was used more than 48 hours ago, then no quarantine enforced at all and the license is immediately released. If it was used less than 48 hours ago, then it's quarantined until 48 hours since its last use. Quarantine can never last longer than 48 hours. Once the quarantine ends the license returns to the pool of available licenses and can be assigned to another user.

Oversubscription

If the number of Dynamic licenses available in a license pack is less than the number of users that should be assigned a license from the pack, some license assignments will not be successful and will switch in the "Oversubscribed" status. For instance, if pack "Marketing" contains 5 licenses, but the assignment table has 12 users assigned a license from this pack, then 7 assignments (i.e. $12 - 5 = 7$) will fail and the respective users won't be able to lease a license from Server.

In case of oversubscription, the license assignment algorithm favors more active users (i.e. users that most recently used a license). In the example above, the 5 most active users will still be able to lease a license while the 7 least active users won't be assigned a license.

User licensing for Data Catalog

Unlike with other Server features, accessing the Data Catalog of EasyMorph Server requires users to have a valid license configured in tab "Licensing" of EasyMorph Server.

There are two user roles: "Professional users" and "Regular users". These two roles have different licensing mechanisms described below.

User role	Licensing mechanism	Catalog permissions
Professional User	Per-user (assigned by Server)	Full access
Regular User	Per-space (unlimited Regular users)	Read-only; optionally, creating static items

Table 2: Data Catalog user licensing.

Professional users (creators)

Professional users are usually the users that create and manage Catalog items. They are assigned a Professional user license as described in "Leasing licenses to Desktop users from Server" above.

Professional users can access Data Catalog in any space to which they have been given access and can create, consume, and modify Catalog items of any type.

Regular users (consumers)

Regular users can only consume Catalog items and, optionally, create static (not computed) items. They can't create computed items and can be prohibited from modifying any Catalog items (the read-only mode).

Unlike Professional users, Regular users are not licensed per-person. Instead, a per-space license allows an unlimited numbers of Regular users in one space. Therefore, if a space is assigned an "Unlimited Regular users" license any user that can access the space can access its Data Catalog.

Besides per-space licenses, a full unlimited "Infinity" license is available and permits unlimited Regular users in unlimited spaces.

Accessing the Catalog

In order to use the Data Catalog, it must be enabled in the space settings.

For licensed users and spaces, the Catalog can be accessed from both EasyMorph Desktop and from Server's web UI. However, certain limitations apply (see below):

Space authentication	Pro users	Regular users
Active Directory	Yes	Yes (with free edition)
Password	Yes	Yes (with free edition)
Anonymous	Yes	Yes (with free edition)

Table 3: Accessing the Catalog from EasyMorph Desktop.

Space authentication	Pro users	Regular users
Active Directory	Yes	Yes
Password	Only as Regular user	Yes
Anonymous	Only as Regular user	Yes

Table 4: Accessing the Catalog from EasyMorph Server's web UI.

Journal

EasyMorph Server writes a journal that records various user actions and system events, such as:

- Workflow completions (successful or not). The event record includes parameters, errors, notifications, status messages, start and elapsed times, initiator, and other metadata.
- Successful user actions
 - Logged in
 - Task triggered / changed / deleted
 - File uploaded / downloaded / deleted
 - Folder created / renamed / deleted
 - Repository connector created / edited / deleted
 - Catalog item retrieved / created / edited / deleted
 - Catalog directory created / edited / deleted

From a technical standpoint, the journal is a database table. Two types of database connections are supported: embedded and ODBC:

Connection	Description	Editions
Embedded (default)	Embedded SQLite database, comes with Server installation, requires no configuration. No access restrictions. No failover.	Team / Enterprise
External	ODBC (MS SQL Server or Postgres). Doesn't come with Server installation and must be configured separately. Allows restricting access. Automatic failover switching to the embedded journal database if the external database is not available.	Enterprise

Regardless of whether an embedded or external ODBC database connection is used, the journal format is the same.

The embedded journal database is a SQLite file "C:\ProgramData\EasyMorph Server\journal.db".

Failover switching

If the embedded journal database becomes unavailable, the Server will start accumulating events in memory and keep retrying to access the database. If 500'000 events have been accumulated in memory and the database journal is still not available, the events will be discarded from memory and lost.

If the external journal database becomes unavailable, the Server will automatically switch to the embedded journal database. Switching back to the external database should be done manually from the Server's web-console (tab Journal). The records created in the internal database during a failover switch should be copied to the external database manually, if required.

User interface

The journal UI in EasyMorph Server allows simple filtering:

- By date
- By project
- By initiator (user, scheduler, API request, etc.)
- By status (success, failed, canceled, etc.)

Filters of the same or different types can be combined, so multiple filters can be applied at once.

Since the journal is just a database table, it can be queried using the Query Editor in EasyMorph, or any SQL-compatible data visualization tool such as Tableau or Power BI.

Besides completed events, the journal displays in real time:

- Currently running workflows (administrators can cancel any workflow in any space, users can cancel workflows in their spaces only)
- Currently logged in users (administrators can log out any user)

This data is not recorded in the journal and is only available via the Server's web interface.

Task journal

The task journal is available for each task (in task details) and represents a subset of journal records related to task.

Journal cleanup

The journal works in the "always append" mode and therefore the number of records in the journal always increases. While the embedded journal database can handle billions of records, over time with extensive Server use the journal database may grow very large.

EasyMorph Server doesn't remove old records from the journal database automatically. The journal data retention policy is left to the Server admins who can design and schedule an EasyMorph project that would automatically remove old journal records.

Workers

A worker in EasyMorph Server is a Windows process that executes all operations of a Server space: run tasks, access files, etc. One worker can be used by multiple spaces. Although, one space can use only one worker to perform all its operations.

The Server service (with the built-in Default worker) and additional workers are Windows processes with the names **Morph.Server.WebConsole.exe** and **Morph.Server.Worker.exe** accordingly. Their process IDs (PIDs) can be seen in the "Workers" tab of Server settings (depicted below). These PIDs correspond to the PIDs that can be seen in Windows Task Manager (tab "Details").

Tasks Files Pages Log Settings Spaces **Workers** Mail

[New worker](#)

Workers that can be used to run tasks in spaces.

Worker	Status	PID	Jobs	RAM	CPU	Spaces	Mapped drives	
Default	In use	20540	2	258.2 MB	35 %	3	M, Z	
test	Starting	7008		11.4 MB	17 %	1	-	
CORP/dbreadonly	Idle	49356		37.3 MB	0 %	1	-	
CORP/marketing	Idle	29088		40.0 MB	0 %	2	-	

Workers that have been detached and will be shut down when tasks finish running.

Worker	Status	PID	Jobs	RAM	CPU
test	In use	7864	1	65.4 MB	9 %

Screenshot 8: Workers of EasyMorph Server.

The Default worker

The Default worker is a special worker. Unlike other workers, it's embedded in the Server service and therefore runs under the service's account (by default, it's NT AUTHORITY/LocalService).

In EasyMorph Server, the Default worker can't be deleted, edited, or recycled.

Note that tasks in spaces that operate under the Default account have full access to the system folders and files of Server (e.g. server settings). Therefore, in environments with high demands for security, it is recommended to avoid using the Default account for spaces.

Additional workers (Enterprise edition)

Additional workers are separate processes that are attached to the process of the Server service. They can run under a different Windows account than the service.

Before a worker can be used for a space, it must be created and configured in the tab "Worker".

Run spaces under different Windows accounts

With the help of workers EasyMorph Server allows running tasks and accessing files under multiple Windows. Technically, the Server service does this by spawning and running pre-configured child processes (workers) to execute tasks and access files of designated spaces under specific Windows accounts. The picture below shows a sample configuration of workers that allows different spaces to run tasks under different Window accounts. In this configuration:

- Space 1 and Space 2 use the Default worker (the worker that is built in the EasyMorph Server service)

- Space 3 uses a worker that runs under Account A
- Spaces 4 and 5 use a worker that runs under Account B
- One more worker is configured to use Account C but is not used by any space.



Figure 1: The main and child (agent) processes of EasyMorph Server.

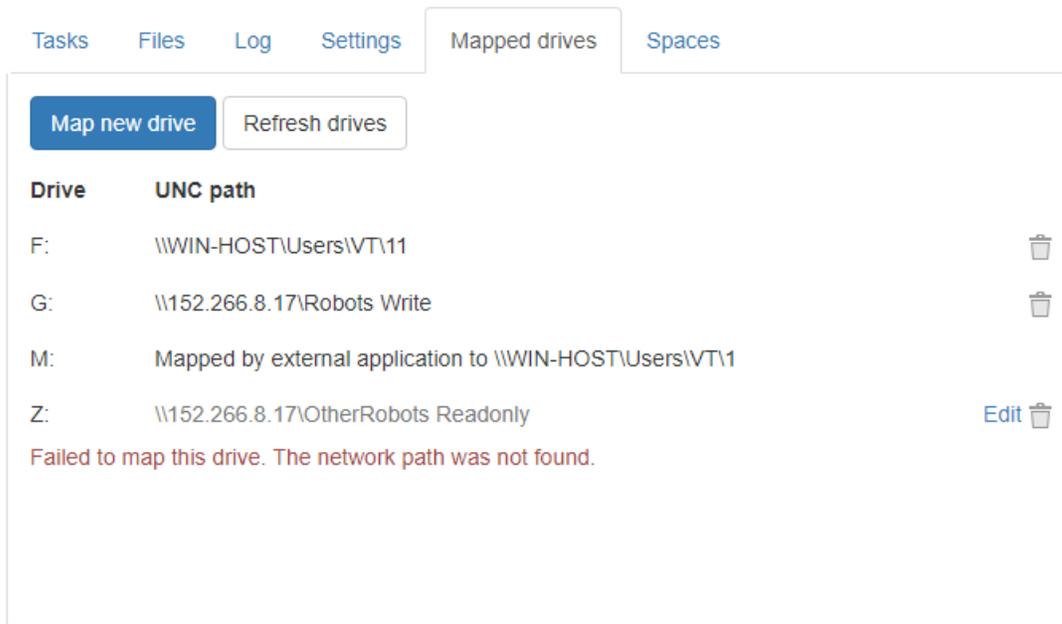
Recycling workers

All accounts except the Default account can be *recycled*. Recycling an account detaches its current agent process from the Server service and attaches a new one. The detached agent process automatically self-terminates when all tasks that it ran have been finished or cancelled.

Recycling provides a graceful and safe way to forcefully terminate tasks that "misbehave" (e.g. freeze, or lock memory up) as well as delete/reconfigure accounts without restarting the Server service. If necessary, remove a detached agent process manually using the Windows Task Manager. The agent process can be identified by its process ID (PID).

Mapped drives

In Windows, network folders are mapped individually for each Windows account. Therefore, even if a mapped network drive or folder is accessible for one Windows account it will not be accessible by default for another account. To configure mapped drives of an account, open the account settings in EasyMorph Server and go to the "Mapped drives" tab of the account (see "Screenshot 9: Mapped drives." below).



Screenshot 9: Mapped drives.

To map a new drive, pick an available drive letter, provide a UNC path to the shared network folder, and press the “Map” button. If mapping is successful then the new mapped drive becomes available right away.

To re-connect a failed mapping (e.g. when the specified network location that was not available at the moment of Server start), press “Edit” to open the mapping settings of the drive, and then press “Map” to initiate drive mapping. If mapping was successful the new drive becomes available right away.

To remove a mapped drive, press the trash bin icon of the mapped drive. The drive will be removed after the Server service is restarted (for the Default account), or when the account is recycled (for other accounts than Default).

Note that a mapped drive becomes available for all spaces that use the account.

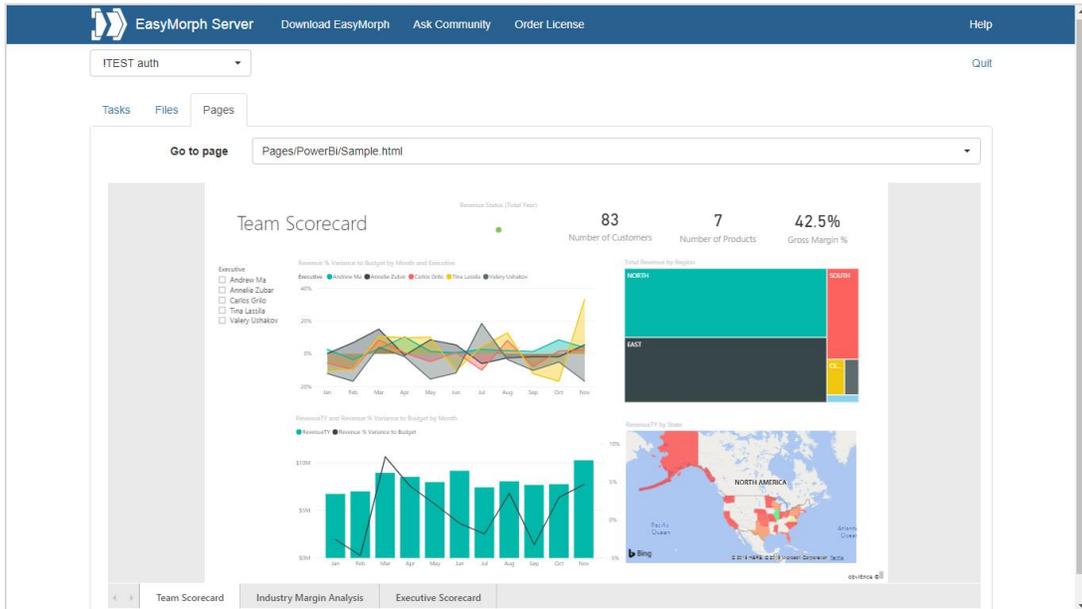
Tab Pages

When enabled, the tab “Pages” offers a simple built-in web-server that can display custom HTML pages to users of a space. The HTML files must be located in the Pages’ root folder that is specified in the Space settings. The folder can have subfolders with HTML files as well. When index.html is present in the root folder, it’s displayed by default. Otherwise, Pages display an HTML file that happened to be found first. HTML pages can display any information that a web-page can display. For instance:

- Welcome page
- An HTML table with result data generated by an EasyMorph task
- Quick tutorial with a few embedded YouTube videos.
- Embedded Power BI / Tableau Online / Google Data Studio dashboard, or a mix of them

- Charts showing EasyMorph Server usage statistics (RAM, CPU, etc.)

In the screenshot below, the Pages tab contains a custom HTML page with embedded Power BI dashboard.



Screenshot 10: Custom HTML page in the Pages tab.

Email notifications about failed scheduled tasks

If the integration with an email service has been configured, EasyMorph Server will automatically send notifications to a designated email address (or addresses) about failed scheduled tasks. If a task was triggered manually or through the API and failed, no notification will be sent.

Screenshot 11: Email notification settings.

Note that multiple default recipients can be specified – just separate their emails with commas.

Email notifications in spaces

By default, all notifications about failed scheduled tasks are sent to the recipients stated in the Server settings (tab Notifications). However, in space settings, it's possible to configure recipients (up to 10) that will receive notifications about failed tasks only in that particular space. In this case, notifications from this space won't be sent to the default recipient(s) configured in Server settings.

File locations

To specify paths to data files, it is recommended to use a project/task parameter for the root data folder and calculated parameters for paths to specific files used in the project. In this case, you can copy projects to Server from your local computer, and specify another value of the root folder path parameter in the task properties.

For instance, if you design an EasyMorph project on your local computer and it needs to read `C:\My documents\MyData\myfile.csv` you can create two parameters:

1. Parameter {Data root} = `C:\My documents\`
2. Calculated parameter {CSV file} = `combinepath({Data root}, 'MyData\myfile.csv')`

To specify the file location in an import transformation use parameter {CSV file} instead of a hardcoded path. When copied the project to EasyMorph Server, create a task and in task properties specify the data root parameter using a path to a server folder:

```
{Data root} = M:\SharedDataRoot
```

When the Server runs the task, it will read the CSV file from *M:\SharedDataRoot\MyData\myfile.csv* instead of the location specified in the project (i.e. *C:\My documents\MyData\myfile.csv*).

Remote administration

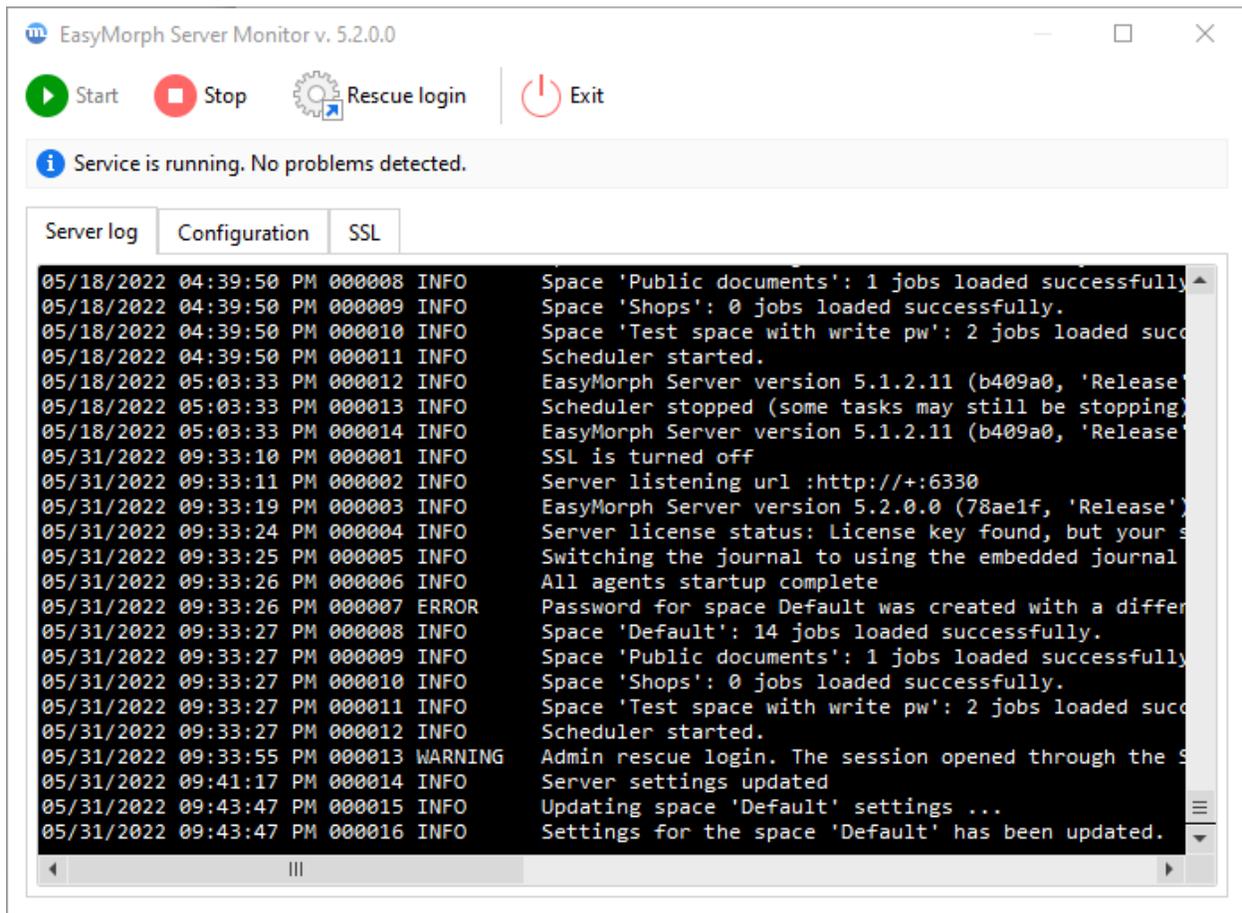
By default, the Server settings pages (Settings, Spaces, Accounts, etc.) can be accessed only by using the "rescue login" in the Server Monitor. However, it is possible to enable remote administration and configure the Server settings from a remote computer. For this, enable "Remote admin access" on the Server settings page, and provide a password.

Enable remote administration in a trusted network only. Do not enable remote administration if EasyMorph can be accessed directly from the open internet.

Server Monitor

EasyMorph Server Monitor is a standalone utility that allows performing the following operations:

- Perform the password-less "rescue login" to access Server settings
- See the service status (running/stopped/error)
- See the server log
- Start/stop the service
- Enforce/disable the SSL mode
- Change the service port (the service must be stopped prior to changing port)



Screenshot 12: EasyMorph Server Monitor

The Monitor minimizes to the system tray. To exit the Monitor when it's minimized, right-click the tray icon and choose Exit.

Similarly to any other Windows service, EasyMorph Server service can also be started/stopped using the Windows Task Manager or Windows Services.

HTTPS-only mode

The HTTPS-only mode uses the SSL encryption for all traffic between Server and clients (web-browser, Desktop, API clients). When turned on, all Server URLs will start from **https://** instead of **http://**.

To switch the Server to the HTTPS-only mode perform the following actions:

- 1) Open the Monitor.
- 2) Stop the service.
- 3) Go to the SSL tab in the Monitor and tick "Use HTTPS"
- 4) Pick an SSL certificate from the list of installed certificates, or install a new certificate. Press Apply.
- 5) Start the service.

Note that SSL certificates that are installed using the Monitor are installed into the Windows certificate store.

Security considerations

EasyMorph Server is technically a web application therefore all security considerations relevant to web applications apply.

Cloud hosting

If you decided to host EasyMorph Server on a cloud instance (e.g. Amazon EC2, Azure, or Google Cloud) and you're not using a VPN to access it, you may effectively expose it to the threats of open internet. In this case make sure that:

- No space is configured to use the anonymous access mode
- All passwords used for password-protected spaces are sufficiently strong and have at least 20 characters (check out this [xkcd](#) about creating long passwords)
- Web Files disabled unless it's necessary
- If Web Files need to be enabled then disable uploading files unless it's necessary
- Arbitrary code execution is disabled unless it's necessary
- Spaces that have arbitrary code execution enabled
- Prohibit execution of unsigned projects
- Do not use the Default worker for spaces; make sure that the Windows account(s) used for the workers that run spaces can't access system folders, including the system folder of EasyMorph Server
- SSL is configured and enforced, SSL certificate is valid and not expired; self-signed certificates are not used
- Remote admin access is disabled in the Server Settings (instead, use Remote Desktop for Server administration and use "rescue login")

It is highly recommended to use the cloud provider's firewall to limit access to your Server instance only for the IP addresses (or IP ranges) that you use.

Start/stop batch scripts

It is possible to execute a custom batch script when the Server service is starting or stopping. Modify **onstart.bat** or **onstop.bat** located in C:\Program Files\EasyMorph Server\systemscripts accordingly.

Logging

The Server writes a log file located in the log folder specified on the Server settings page.

If the log folder is not accessible to the "EasyMorph Server" Windows account group or to Server service account (e.g. because of lack of permissions) the Server won't start and will record an application error in the Windows events log.

Data persistence and locality

The Server settings, task and space settings are stored in XML files and therefore can be easily backed up and restored using 3rd party tools, if necessary. Database connectors, the embedded event journal, and catalog metadata are stored in SQLite database files which also can be backed up and restored using the same 3rd party tools.

No user data or intermediate transformation results are stored in Server system folders. No data is sent to the cloud or to EasyMorph Inc. All data transformations are performed in memory by the EasyMorph's in-memory engine only.

Command-line API client

EasyMorph Server comes with a command-line utility *ems-cmd.exe* which is a cross-platform command-line API client. The utility allows triggering tasks, uploading/downloading files, checking server status and performing other Server operations from the command line. It can be used in batch scripts, or called from external applications as a way of integration with EasyMorph Server.

The source code, installer for standalone deployments, and documentation is available on GitHub: <https://github.com/easymorph/server-cmd>

The command-line API client is build using the .NET SDK (see below).

EasyMorph Server .NET SDK

EasyMorph Server can be programmatically integrated with 3rd party .NET applications using the .NET SDK available as a [Nuget package](#). Its source code is open and available on GitHub too: <https://github.com/easymorph/server-sdk>

Uninstallation

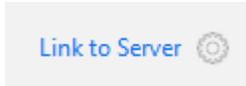
To uninstall EasyMorph Server run the uninstaller and follow instructions. The uninstaller does NOT automatically remove:

- Task configuration files
- Server configuration files
- Connector repositories
- Logs
- Embedded journal database(s)

They should be removed manually, if required.

Desktop to Server Link

EasyMorph Desktop can be linked to EasyMorph Server by configuring the Server Link on the Start screen of EasyMorph Desktop. When the link is configured, it can be used by Desktop users for:



- Publishing projects to Server
- Opening projects from Server
- Publishing datasets to Server
- Receiving datasets from Server (including secure [hot-linking](#))
- Using the repository of a Server space in Desktops
- Leasing a user license from Server
- Working with the actionable Data Catalog

See more on configuring the Server Link in this tutorial article: "[Server Link](#)".

Note that when EasyMorph Server is switched to using SSL encryption (see chapter "HTTPS-only mode" above), Desktops will automatically switch from HTTP to using HTTPS in communications with the Server. Therefore, no re-configuration of Server Links in Desktops is necessary. To make EasyMorph Desktop always use SSL encryption (and disable using unsecured HTTP) when communicating with Server, tick the "Require SSL" checkbox in the Server Link configuration in Desktop.

UI customization

The Server can use 2 themes for UI style and some elements: **default** and **custom**. The themes are located in **C:\Program Files\EasyMorph Server\wwwroot\themes**. By default, the elements from the default theme are used. However, if a customized element is added to the custom theme, then it takes precedence over the equivalent element in the default theme.

The following UI elements of the web-console can be added and customized in the custom theme:

- Logo (logo.png)
- Header hyperlinks (top-header.html)
- Colors, styles (custom.css)
- Favicon (favicon.ico)

Note that the content of the default theme is overwritten during software updates. Therefore it's not recommended to change it. The custom theme is not affected by software updates.

Troubleshooting

Symptom	Action
Web Console inaccessible	Check if EasyMorph Server service is running. If not then start it using EasyMorph Server Monitor or Windows Services.
Service doesn't start	Use EasyMorph Server Monitor to check the server log (default location is C:\Program Data\EasyMorph Server\Logs\Server log) for errors. If no errors in the server log then check system events using Windows Event Viewer. The Server doesn't start when the log folder is not accessible.
Server doesn't recognize a license key	Make sure that the license key is located in a folder that has necessary permissions set up for the "EasyMorph Server" Windows account group. Folder C:\Users\Public might work.
Server can't access a local folder	Make sure that the folder has necessary permissions set up for the for the "EasyMorph Server" Windows account group or the worker that runs the task that can't access the folder.
Server can't access a mapped drive	Re-connect the failed mapped drive. See chapter "Mapped drives".

Technical support

The [EasyMorph Community forum](#) is the main support channel and has many questions about Server administration already answered.

If your request contains sensitive information that can't be published in a public forum, please contact our technical support at support@easymorph.com.