EasyMorph Server Administrator Guide

Table of Contents

Prerequisites

- 64-bit version of Windows 7 (or above) or Windows Server 2012 (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-intense application because it processes all data in memory. The amount of RAM required depends directly on data volumes processed by EasyMorph projects. However, estimating exact memory requirements is not so straight forward. Due to aggressive on-the-fly data compression, the amount of RAM consumed strongly depends on data type 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 in a task. Add up dataset sizes for simultaneously executed tasks.

It's possible to use EasyMorph Desktop to obtain more precise memory consumption estimates because EasyMorph Server and EasyMorph Desktop employ 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? They 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.

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.
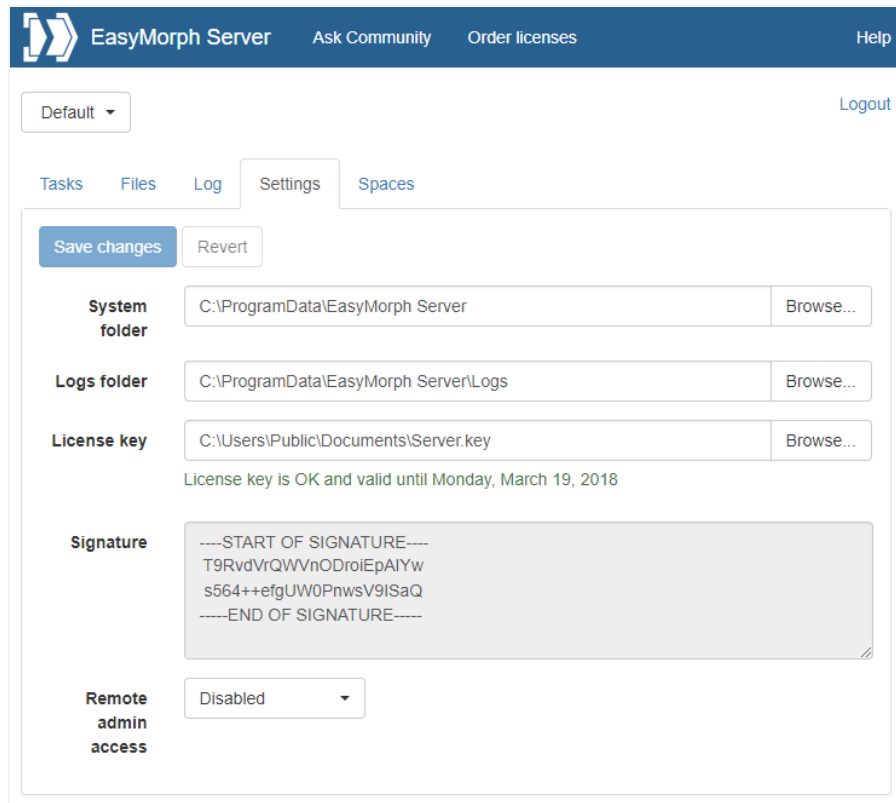
It's recommended to have a reserve of memory to avoid running out of memory. To help detect possible memory deficit, EasyMorph Server logs warnings into the Server log when available RAM falls below 20%.

Installation

Run the installer under a Windows administrator account and follow instructions. After successful installation the Server Settings page opens automatically at the following URL (log in as Admin):

http://localhost:6330/settings/edit
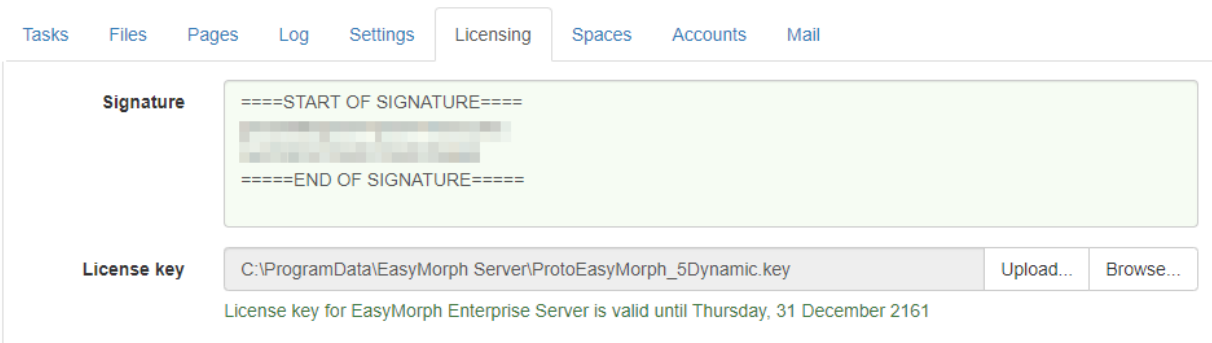
Note: by default the Settings page can be opened only on the computer where EasyMorph Server is installed (i.e. localhost).

Screenshot 1: Server Settings page

License key

Send the digital signature from the Licensing page (see "Screenshot 2: Installation signature in the Licensing page." below) to support@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.

Screenshot 2: Installation signature in the Licensing page.

A license key may have a mix of Server and Desktop signatures. The license certificate (a PDF file) that comes with the license key shows what signatures are linked to the key. The same key can be used for

Server and Desktops. Note that when computer name or domain name changes the Server signature also changes.

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 Windows account that has necessary permissions in the Server settings, and use the account for the space which tasks require the permissions (more on spaces in chapter "Configuring spaces"). Read more on configuring Windows accounts in EasyMorph Server in chapter "Configuring accounts".

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 from which the connection is established. Use explicit login/passwords for accessing databases, instead of integrated Windows authentication, if necessary. Alternatively, add the default service account (*NT AUTHORITY\LocalService*) to database logins.

Changing Server service account

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

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

1) Make sure that the new account can assess the system folders and log folders of EasyMorph Server.
2) Stop the service and change the "Log On" account in the EasyMorph Server service properties in Windows Services panel.
3) Start the Service.

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 demanded 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). Change the account to another one, if necessary (See Server service account).
6) Start the Server service using either EasyMorph Server Monitor, or Windows Services panel.

Connector repository

EasyMorph uses pre-configured connectors in order to access database servers, email servers, and various external services and applications. The connectors are stored in a repository which is technically a SQLite database file.

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 a new database connectors to the repository use the Connector Manager of desktop EasyMorph (it can work with arbitrary repository files).

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 it technically can use the same repository file shared together with desktop editions (e.g. located on a shared network folder). Note that EasyMorph Server service by default is running under a special Windows account (Local Service) which can't access folders in C:\Users\...\AppData which is the default location for repositories created by EasyMorph Desktop. You may want to move or copy the repository file to a folder that can be accessed by the Server service.

A better approach from a security standpoint is to use Server-hosted repositories on Desktops. For more details read the chapter "Connector repository access for Desktop users" below.

Repository locking

Since repositories can contain connectors to sensitive data, as an additional protection measure a repository can be encrypted and locked to the Server where it was created. For this, tick "Repository: Encrypt and lock to this Server" when creating a space. Encryption is done by Windows on a deep system level and is highly secure. When a repository file is encrypted and locked it can't be used (as a file) in another Server or Desktop. The only way to access from Desktops the connectors in such repository is via a Server space on the Server where it was created.

Warning! If you backup Server system files and folders keep in mind that locked repositories can't be restored on another Server. All connectors in such repository will have to be recreated.

Also, a repository can be encrypted only when it's created. An existing repository can't be encrypted or decrypted.

Configuring spaces

Spaces are used 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
- Public folder (accessible through a web-browser or by other means, e.g. API)
- Windows account under which tasks are executed and files are accessed
- Connector repository and its availability to Desktop users
- Root folder for Pages (if Pages are enabled)
- User access list (for spaces with Windows Authentication)
- Security settings
- File/folder picker locations

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.

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 Server administrator.
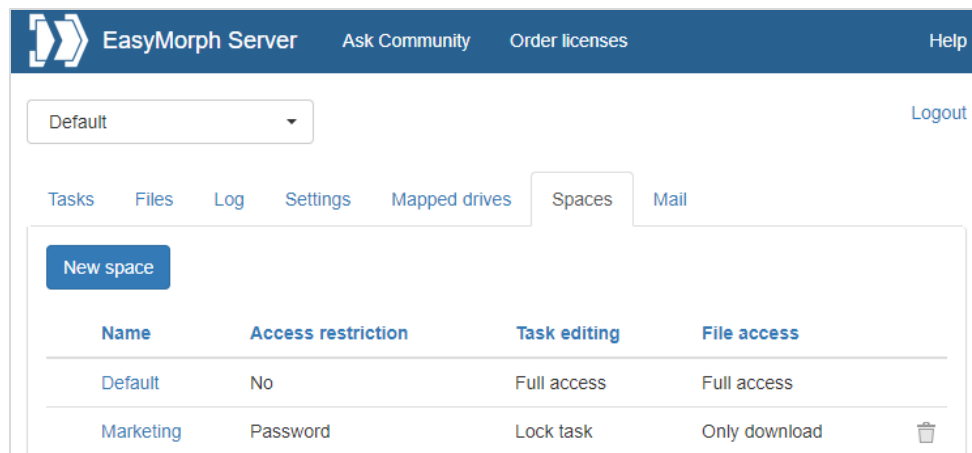
Screenshot 3: Spaces.

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 account

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 account.

However, it is possible to assign another Windows account to a space (in EasyMorph Server Enterprise edition only). In this case, the space will run tasks and access files using the provided Windows account instead of the Default account. In order for a space to use other account than Default, the account must be configured first. For more information read "Configuring accounts" below.

Task and file 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 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	Disabled	Upload only

provide files with source data.		
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

EasyMorph projects can include actions that effectively can execute an arbitrary code (e.g. a script or an application). Under certain conditions this can be undesirable from a security standpoint. The "Arbitrary code execution" setting can be used to prevent projects from executing actions "Run program", "Iterate program", "PowerShell", and "SSH Command".

File/folder picker locations

The "Locations" tab in the space settings allows specifying drives that are show in the file/folder picker dialog. The dialog can be 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 the drives 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

There are three access modes possible for a space:

- Anonymous
- Password-protected
- Windows Authentication (uses Active Directory)

Anonymous

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

Password-protected

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

Performing operations through API 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 allowed to have access to the space. Users are identified by their Windows accounts (e.g. DOMAIN\username) and verified against 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.

Screenshot 4: Configuring users and groups of a space.

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 in Server tasks
- Storing/sharing EasyMorph datasets (.dset files)
- Collecting source files with data required for the projects
- 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 version control system (requires 3rd party applications). It also allows using relative paths to refer to source and helper files, which is convenient for publishing projects from a user's computer to Server.

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

- Using the built-in Web File Manager (i.e. via a 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.
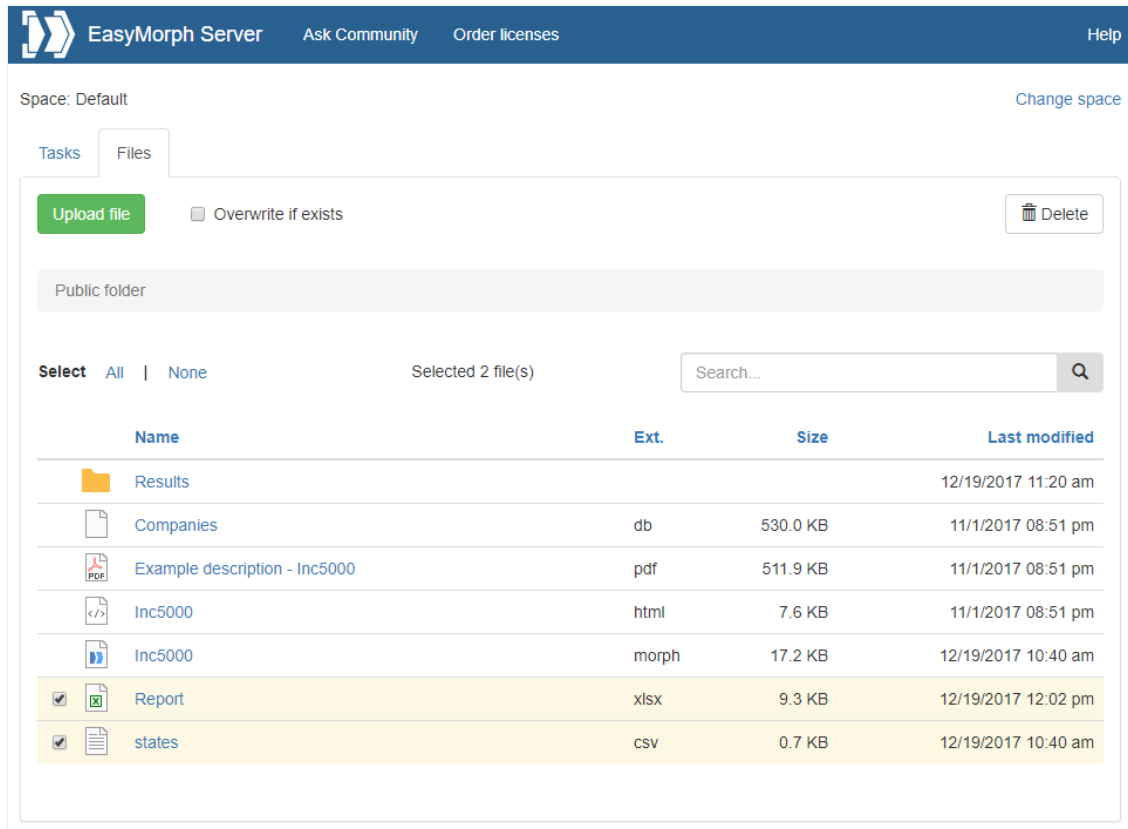
Screenshot 5: Web File Manager.

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).

Configuring accounts

EasyMorph Server (Enterprise edition only) allows running tasks and accessing files under multiple Windows accounts. Technically, the Server service does this by spawning and running pre-configured child processes (agents) to execute tasks and access files of designated spaces under specific Windows accounts. One account can be used by multiple spaces. Although, one space can use only one account.

The picture below shows a sample configuration of processes used to provide multiple accounts. In this configuration:

- Space 1 and Space 2 use the Default account (the account that is used to run the EasyMorph Server service)
- Space 3 uses Account A
- Spaces 4 and 5 use Account B
- Account C is configured and an according agent process is spawned and attached but is not in use by any space.

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

The Server service and the account agents are Windows processes with the names **Morph.WebConsole** and **Morph.Agent** accordingly. Their process IDs (PIDs) can be seen in the "Accounts" 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 | **Accounts** | Mail |

New account

Accounts that can be used to run tasks in spaces.

Account	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	-	♻	🗑

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

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

Screenshot 6: List of configured accounts.

The Default account

The Windows account (usually, it's NT AUTHORITY/LocalService) that is used to run the Server service is called the Default account. In EasyMorph Server, the Default account can't be deleted, edited, or recycled. The Default account can be used for any space or no space at all.

Note that tasks in spaces that operate under the Default account have full access to the system folders and files of Server. These files may contain potentially sensitive information such as values of task parameters or task logs. Therefore, for better security, it is recommended to avoid using the Default account for spaces that have arbitrary code execution enabled (see "Arbitrary code execution").

Other (non-default) accounts

Before an account can be used for a space, it must be created and configured. New accounts can be created in the tab "Accounts".

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 7: Mapped drives." below).
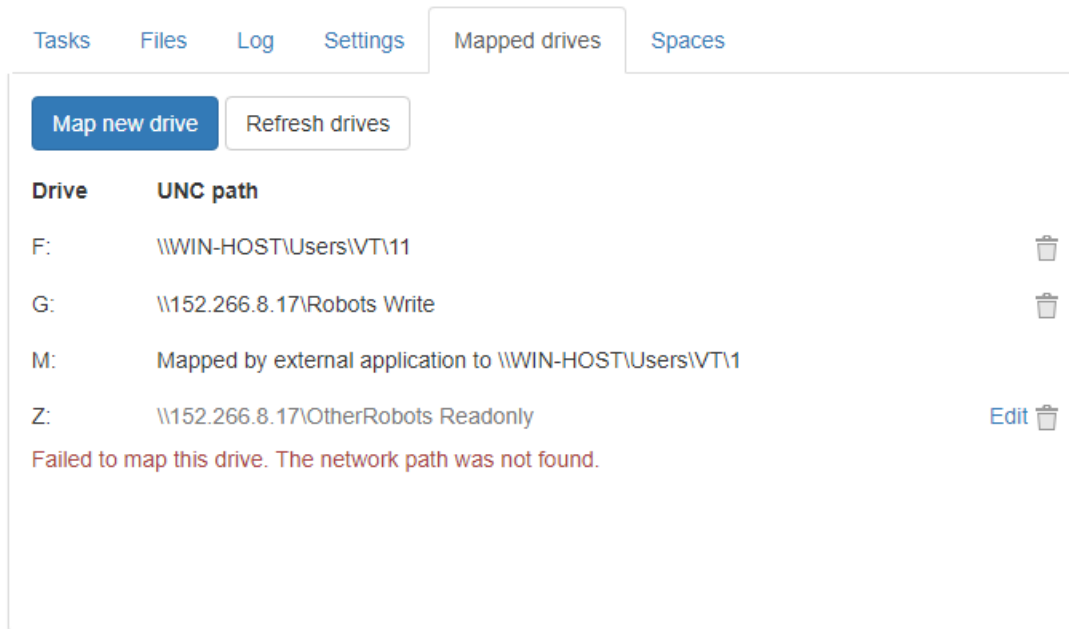
Screenshot 7: Mapped drives.

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.

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====

=====END OF SIGNATURE=====

License key C:\ProgramData\EasyMorph Server\ProtoEasyMorph_5Dynamic.key   Upload... Browse...

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

Assign license   Search... 🔍

Select All | None   🗑 Delete

User	Pack name	License type	Tags	Last activity	Status	
CORP\kristina	Main pack	Professional	sales	a minute ago	In use (4.5.2.4)	✎
CORP\peter	Main pack	Professional	sales	Never	Unused	✎
CORP\dmitry	Main pack	Professional	IT, admin	6 minutes ago	In use (4.5.2.4)	✎

Download list

Screenshot 8: 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.

Tab Pages

The tab "Pages" when enabled 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
- 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.)
- An HTML table with result data generated by an EasyMorph task

In the screenshot below, the Pages tab contains a custom HTML page with embedded Power BI dashboard.
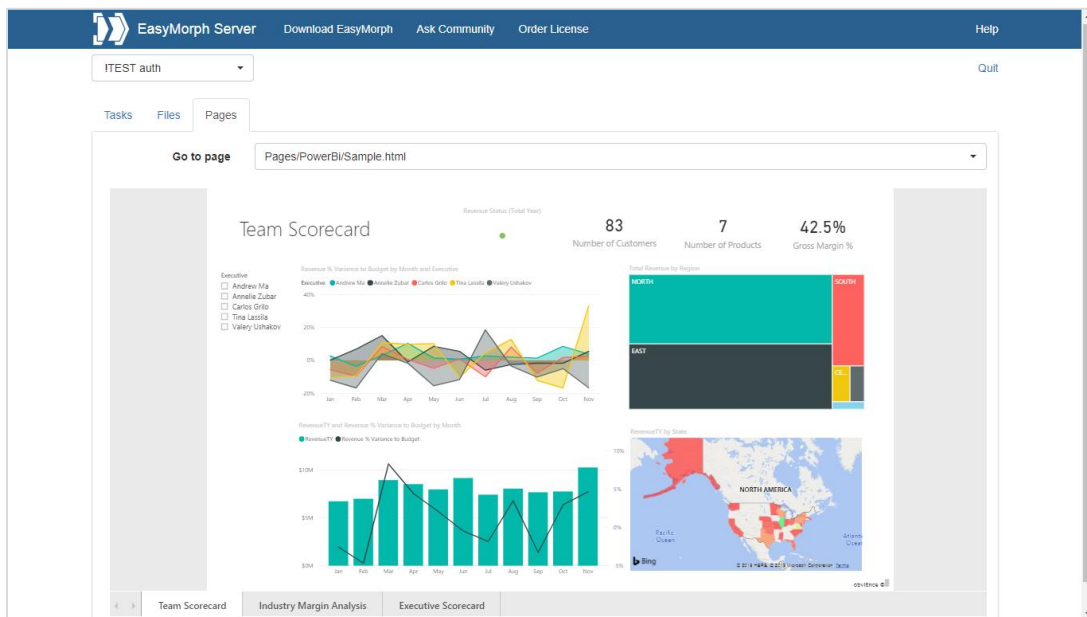
Screenshot 9: Custom HTML page in the Pages tab.

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 about failed scheduled tasks. If a task was triggered manually or through the API and failed no notification will be sent.

Screenshot 10: Email notification settings.

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

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 from *localhost*. 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:

- 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)
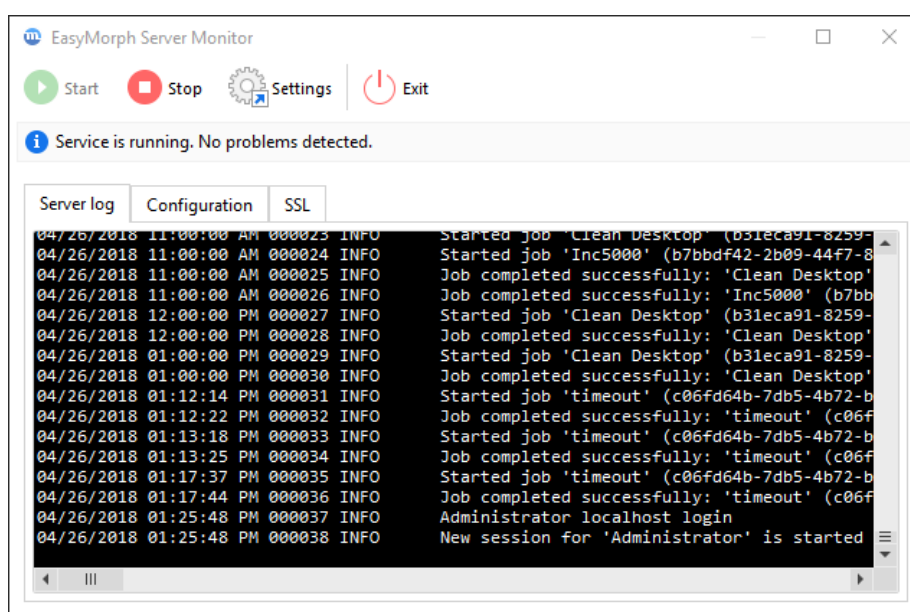
Screenshot 11: EasyMorph Server Monitor

The Monitor minimizes to the system tray. To exit the Monitor 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 SSL encryption for all traffic between Server and clients (web-browser, Desktop, API clients). 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
- Do not use the Default account for spaces; make sure that the Windows account(s) used for 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 login to localhost)

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 two types of logs: the Server log and task logs. All logs are written into the log folder specified on the Server settings page. Having a dedicated folder for logs makes it convenient to collect and analyze logs by 3rd party tools, if needed.

If the log folder is not accessible to the Server service (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 doesn't require a database to run. 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 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 doesn't remove task files, configuration files, connector repositories and logs – 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 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 dynamic license from Server

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

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.
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 Server service account (by default it's *NT AUTHORITY\LocalService*). 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 Server service account (by default it's *NT AUTHORITY\LocalService*).
Server can't access a mapped drive	Re-connect the failed mapped drive. See chapter "**Error! eference source not found.**".