EasyMorph Software Architecture & Security Overview

May 5, 2023

Table of Contents

Overview

EasyMorph is self-service no-code data preparation and automation software intended for internal use by business users in organizations with no or low IT support. EasyMorph includes the following products:

- EasyMorph Desktop, a Windows desktop application
- EasyMorph Server (optional), a Windows service with a web UI
- Command-Line Worker (a.k.a. CLW, optional), a Windows command-line utility for workflow execution

The software is installed on premises and it doesn't require a connection to the internet or a cloud service to operate[1]. EasyMorph is entirely passive in the sense that it retrieves data from or sends to external systems only when explicitly instructed by a user to do so using an EasyMorph workflow.

The most typical deployments are Desktop-only, or Desktop + Server. The CLW utility is only used in integration scenarios when 3rd party applications need to execute EasyMorph workflows on demand from the command line. CLW is covered in a separate chapter in this document. From this point on, we will talk about Desktop + Server as the typical deployment scenario.

Workflows

The main purpose of EasyMorph is automation of data transformation and data flows. Users use EasyMorph Desktop to design automation workflows visually. The workflows can be executed either in EasyMorph Desktop, or on EasyMorph Server.

---
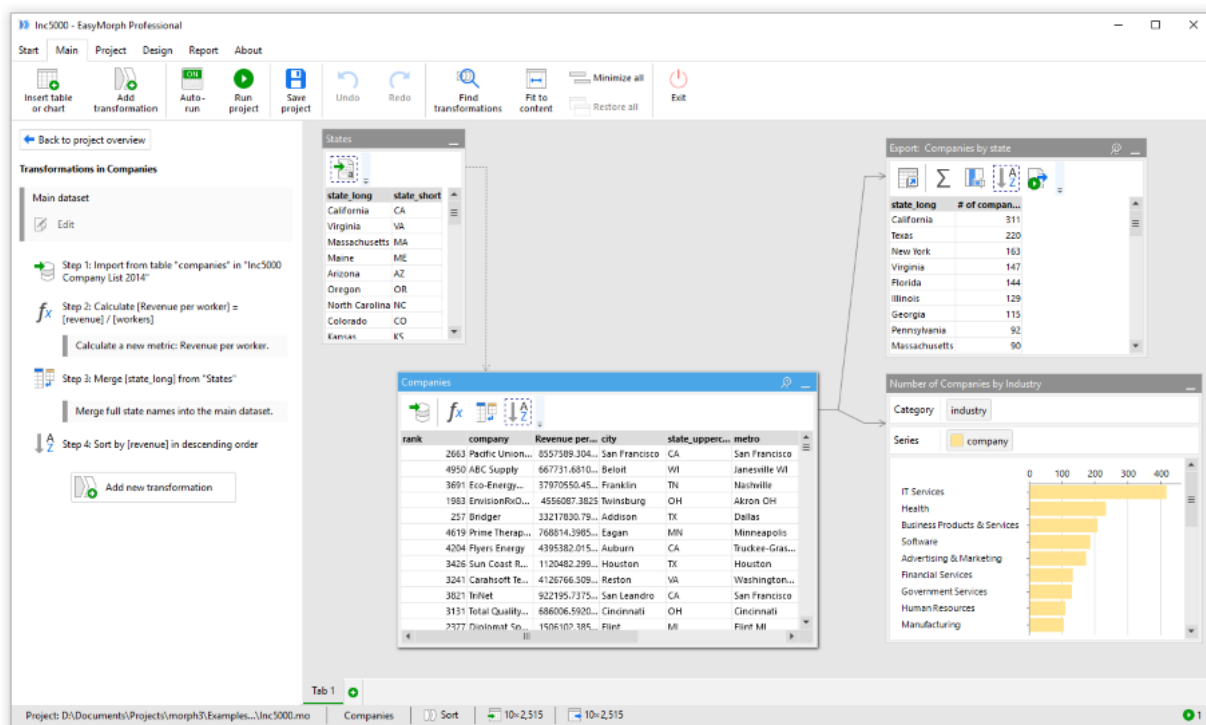
[1] EasyMorph can work in air-gapped networks.

EasyMorph workflows can be very complex and include advanced integration and execution capabilities such as querying databases and web APIs, execution of external applications or Excel VBA macros. Therefore from a security standpoint they should be treated similarly to PowerShell or Python scripts. Note, however, that unlike with scripting, execution of arbitrary code from workflows can be disabled in EasyMorph Server settings.

EasyMorph projects (.morph files) are digitally signed which allows detecting tampering. Execution of projects with broken digital signature (which means they were modified outside of EasyMorph) is by default prohibited on EasyMorph Server.

Connectors and connection credentials

Connection settings and credentials required for connecting to external systems are stored in a connector repository that can be shared (i.e. used simultaneously) by several Desktops and the Server. The Server also can host such repositories and serve them over a network to authenticated and authorized Desktop users for use in workflows.

Every connector repository is encrypted with an industry-standard 2048-bit algorithm and can be additionally protected with read and write passwords.

Both Desktop and Server have the same automation engine that executes the workflows. The engine contains all the drivers required for connecting to external systems such as databases (e.g. SQL Server), enterprise and cloud applications (e.g. SharePoint, Gmail), web APIs (e.g. REST APIs), and enterprise services (e.g. SFTP). The full list of available integrations is available here: https://easymorph.com/all-integrations.html

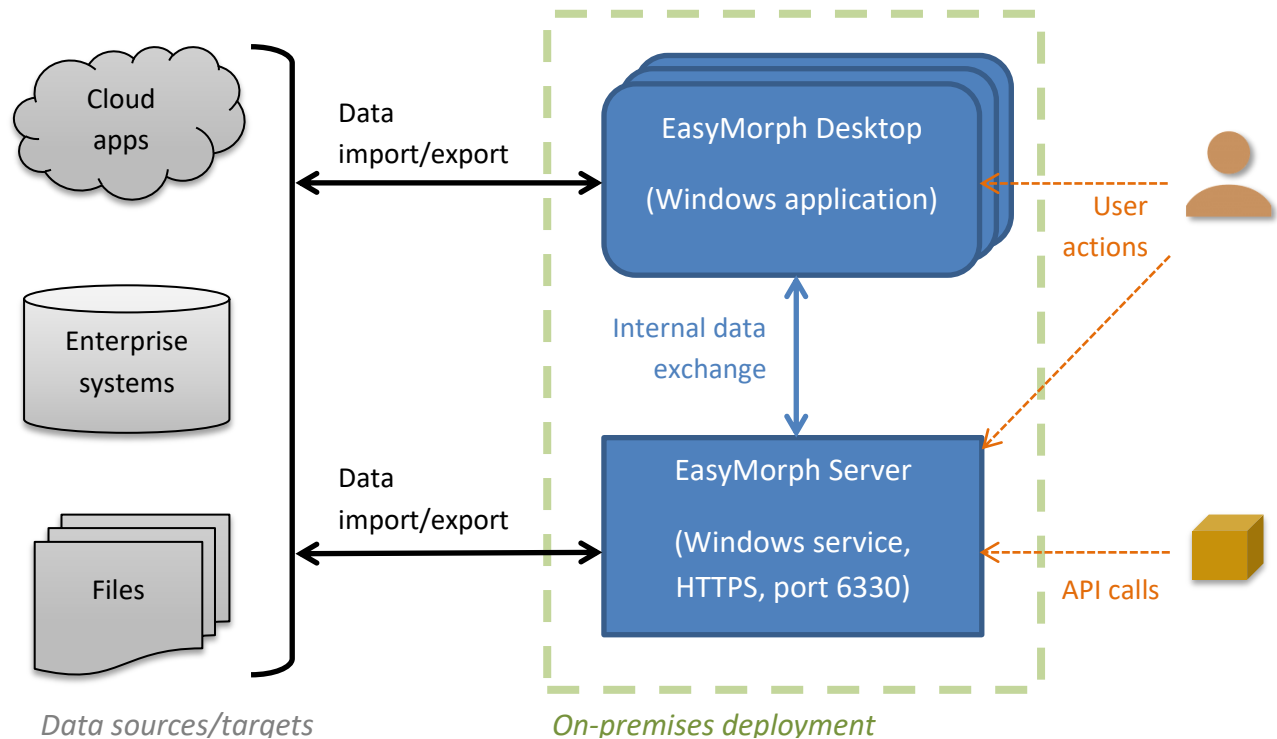*Software architecture and data flow diagram*

Figure 1: Server and Desktop deployment diagram.

Besides communicating with external systems, the Desktop and the Server can also communicate with each other. The Server can provide connector repositories to Desktops. Besides that, the Server sometimes can be used as file storage (although it's optional). In this case, files stored in a designated folder of the Server can be consumed by the workflows or by external applications via the Server API.

All communication with the Server is done via HTTP(S) through a single port (by default, 6330).

Authentication

EasyMorph Desktop is a Windows desktop application so user authentication is done by Windows.

EasyMorph Server users access it via a web browser. They can be authenticated via Active Directory. AD groups are supported.

Account permissions

Both Desktop and Server don't require a Windows account with elevated privileges (i.e. administrator account) to operate. Note, however, that the Server installer does require an administrator account.

The overall approach to permissions in based on two principles:

- "Don't trust, instead control" meaning that EasyMorph is highly controllable and **you can reliably control it with Windows permissions and firewall settings**,

- "Delegate permission enforcement and management to Windows whenever possible" meaning that EasyMorph mostly relies on Windows and Active Directory for user authentication and user access separation.

Data persistency and privacy

Generally speaking, EasyMorph doesn't store data unless it's explicitly instructed to save data as a local file. Data transformation is performed entirely in-memory with no disk footprint.

However, EasyMorph stores the following information persistently:

- Connection settings required in workflows
- Debug logs (rotated every 14 days in Desktop, not rotated in Server)
- Server logs
- Server-based journal of user actions which may include metadata such as file names and parameter values

EasyMorph doesn't send telemetry to the vendor. All diagnostic information needed for troubleshooting is human-readable and can be reviewed (and redacted, if needed) before sending to the vendor. The vendor doesn't have access to EasyMorph installations remotely. The application has no backdoors.

Software updates

Software updates are installed manually, typically by rolling over a newer version using an installer downloaded from the vendor's website. The installer and the deployed software are signed with a code-signing certificate.

Source code scanning

In order to pass Google CASA (Cloud Application Security Assessment), EasyMorph's source code has been scanned using [FluidAttacks scanner](#) and assessed against OWASP. Besides that, the source code is routinely scanned by GitHub's Dependabot.

Threat vectors

While there are numerous security mechanisms and practices used by EasyMorph Server, nevertheless, it is intended for internal use and is not intended for exposure to the public internet. The security mechanisms of EasyMorph Server are built with the assumption that a malicious actor doesn't have elevated permissions (i.e. not a local administrator) on the machine where EasyMorph Server is installed and can't access the configuration files and binaries of the application.

EasyMorph Desktop

Description

EasyMorph Desktop is a Windows .NET application with a graphical user interface. The users can use EasyMorph Desktop for:

- Designing and execution of data preparation and automation workflows
- Querying databases, web APIs and retrieving information from external systems
- Data analysis
- Creating and configuring shared data connectors in an EasyMorph connector repository
- Publishing workflows to EasyMorph Server, opening workflows from EasyMorph Server
- Publishing datasets to EasyMorph Server, retrieving datasets from EasyMorph Server

Installation

The EasyMorph Desktop installer is downloaded and executed from the vendor's website. The installer and the application itself are signed with a code-signing certificate.

Installation is done into the userspace [2]and doesn't require a Windows account with elevated privileges (i.e. administrator account). Silent installation is possible.

The installer installs two applications:

- EasyMorph Desktop
- EasyMorph Launcher

The Launcher is a system tray utility complementary to EasyMorph Desktop. It's a Windows desktop application that runs under the same Windows account as EasyMorph Desktop and is used for scheduling and launching EasyMorph workflows under that account.

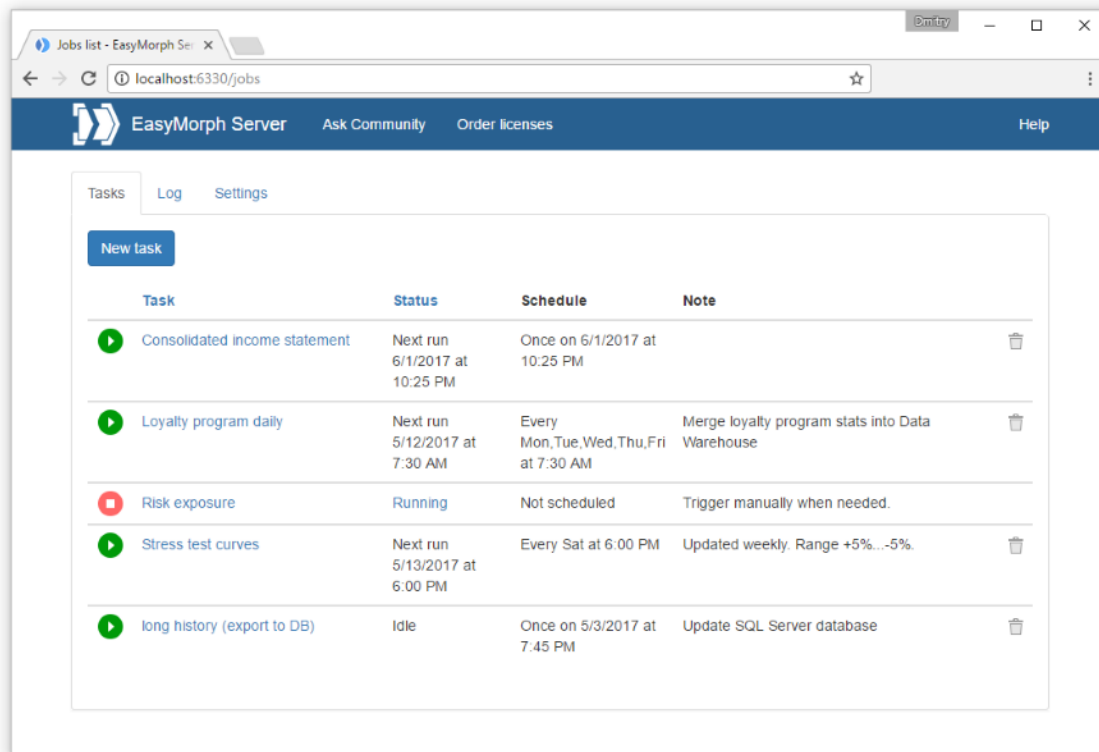# EasyMorph Server

Description

EasyMorph Server is an ASP.NET Core application with a built-in web server. It is installed and operates as a Windows service with a web UI and is accessible via a browser. EasyMorph Server is used for the following:

- Running EasyMorph workflows designed in EasyMorph Desktop
    - workflows can be triggered manually, on schedule, or by an API event
    - workflows can be executed under different Windows accounts
- Send automatically email notifications about failed scheduled tasks
- Uploading and downloading files to/from the Server
- Serving connector repositories to Desktop users

---

[2] The installation folder is C:\Windows\Users\<user name>\AppData\Local\EasyMorph.

- Providing centralized key-value storage for workflows executed in Desktops and Server
- Managing licenses of Desktop users
- User activity logging

Screenshot 2: EasyMorph Server tasks.

Web-server

The web server that is built in EasyMorph Server is HTTP.sys which the standard web-server for ASP.NET Core applications. HTTP.sys is mature technology that protects against many types of attacks and provides the robustness, security, and scalability of a full-featured web server. Microsoft IIS itself runs as an HTTP listener on top of HTTP.sys[3].

The web-server supports TLS 1.1 and TLS1.2. Earlier versions of TLS are forbidden.

Installation

The EasyMorph Server installer is downloaded and executed from the vendor's website. The installer and the application itself are signed with a code-signing certificate.

The installer requires a Windows account with elevated privileges because it installs the EasyMorph Server service and configures the Windows firewall to enable outgoing HTTP connections for the service.

The installer installs the following applications:

---

[3] Cited from https://docs.microsoft.com/en-us/aspnet/core/fundamentals/servers/httpsys?view=aspnetcore-6.0

- EasyMorph Server service (Morph.Server.WebConsole.exe) – the main service with a web-server
- EasyMorph Server Monitor (Morph.Server.Monitor.exe) – the Server configuration utility
- EasyMorph Server CLI (ems-cmd.exe) – an open-source cross-platform command-line utility for interaction with the Server API

The default account for the Server service is *NT Authority\Local Service*. This account can be changed in the Windows service settings.

EasyMorph Server Monitor is a Windows desktop application that is used to configure the basic settings of EasyMorph Server:

- Port (set to 6330 by default)
- SSL certificate (not configured by default)

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

The Server Monitor requires an administrator account to operate and has the mechanism of rescue login that allows a member of the local Administrator group to log into the Server as administrator without a password. Rescue login can't be used by not members of the local Administrator group.

The rest of the Server settings are configured using the Server's web UI (tab Settings). For more details about Server configuration see the "Server Administration Guide", a PDF document that comes with the Server installer.

Authentication

EasyMorph Server has three modes of user authentication

- Anonymous (default) – no authentication
- Shared password – only users who know the password can log in
    o Shared passwords are never stored in plain text or passed over network in plain text
- (*) Windows Identity – authentication via Active Directory

Points marked with (*) are available only in the Enterprise edition of EasyMorph Server.

By default, EasyMorph Server administrators can't log into the Server from the web UI. They must log in only through the Server Monitor, a GUI utility installed with EasyMorph. It only permits logging in for local system administrators. Any member of the local Administrators group can use the rescue login mechanism in Server Monitor to log into the Server as administrator.

Workers

A worker in EasyMorph Server is a Windows process that can run workflows under a different Windows account than the Server service. EasyMorph Server can have multiple workers configured therefore workflows can be executed under multiple Windows accounts.

Each worker can have its own set of mapped network drives accessible only for workflows that are executed by that worker.

Security recommendations

Depending on your threat analysis and subject to your business requirements, you may want to perform the following actions to tighten EasyMorph security:

- (*) Use Active Directory for authenticating EasyMorph Server users
- Configure an SSL certificate for EasyMorph Server (using the Server Monitor utility)
- Switch Desktops to use Server-hosted connector repositories
- Enforce read and write passwords for connector repositories
- Disable execution of external applications in Server workflows if it's not required
- Disable Server features (e.g. Web Files or Pages) that are not required
    - If the Web Files feature of EasyMorph Server is required, disable uploading files unless it's necessary
- Disable remote Server administration access, log in as administrator only through the Server Monitor over an RDP session
- Do not enable execution of EasyMorph projects with broken digital signature unless it's necessary
- If database queries in workflows use parameters, make sure the parameters have validation rules configured that prevent SQL injection
- Use dedicated Windows accounts in connector settings, instead of user accounts
- (*) Run Server tasks under a Windows account that is different from the web-server account
- (*) Use an external database for the Server journal

Points marked with (*) can be done only in the Enterprise edition of EasyMorph Server.

Command-Line Worker

Description

The Command-Line Worker (CLW) is a Windows console application that executes from the command line workflows designed in EasyMorph Desktop. It has the same automation engine as in Desktop or Server and is predominantly used in integration scenarios when a 3rd party application needs to execute an EasyMorph workflow on demand from the command line.

Installation

The CLW installer is downloaded and executed from the [vendor's website](). The installer and the application itself are signed with a code-signing certificate.

The installer requires a Windows account with elevated privileges and installs CLW for all users of a Windows machine. It installs two applications:

- Command-line worker (CLW)
- Configuration utility – a Windows desktop application for configuring CLW settings

Contacts

Please post questions about EasyMorph architecture and security on the [Community forum](#), or send by email to support@easymorph.com.