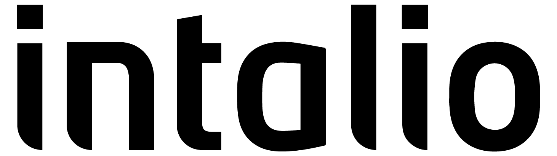
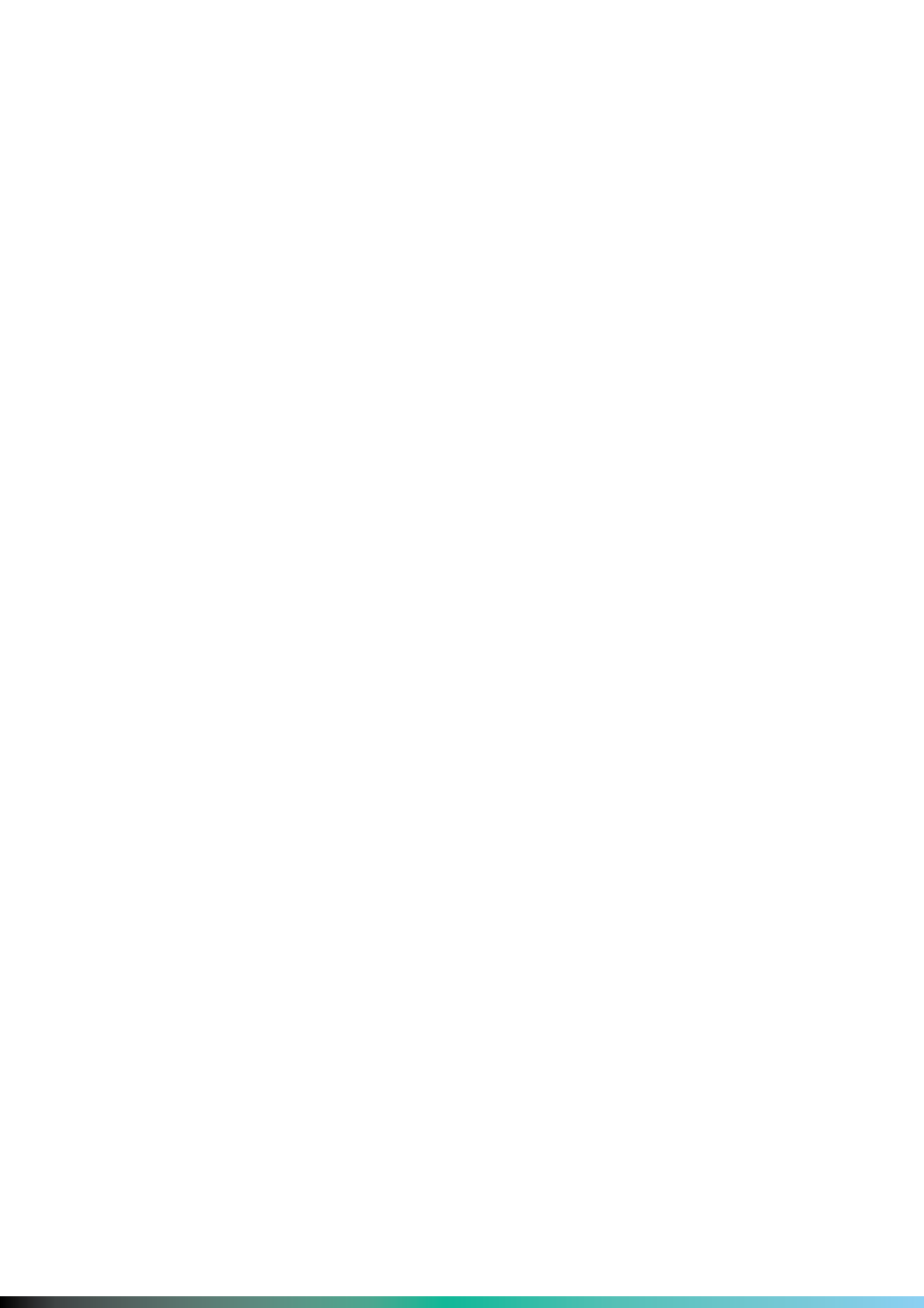
**** 

Version: 3.1.0

Intalio IAM

Installation Guide – Linux (EN)

**Vision.**

Making business simple by connecting people, processes and content.

Intalio is an international software provider with 30 years of innovation in the field of Content and Process Services. By combining cutting-edge technologies with AI and Machine Learning to introduce advanced Line of Business solutions, Intalio managed to become a trusted leader in Digital Transformation across the US, Europe, and the MENA region.

Table of Contents

[1. Pre-Installation Requirements 3](#_Toc126764368)

[2. Installation and Configuration 4](#_Toc126764369)

[2.1. Nginx Configuration 4](#_Toc126764370)

[2.1.1. HTTP Configuration 4](#_Toc126764371)

[2.1.2. HTTPS Configuration 5](#_Toc126764372)

[2.2. Monitor the Application 6](#_Toc126764373)

[2.2.1. Create the Service File 6](#_Toc126764374)

[2.3. Appsettings Configuration 7](#_Toc126764375)

[2.3.1. Connection String 7](#_Toc126764376)

[2.2.1.1. Plain Text 8](#_Toc126764377)

[2.3.1.2. Encrypted 8](#_Toc126764378)

[2.3.2. Database Type 10](#_Toc126764379)

[2.3.3. Jobs 10](#_Toc126764380)

[2.3.4. Health Check 10](#_Toc126764381)

[2.3.5. Cookie Life Time 11](#_Toc126764382)

[2.3.6. OpenInIframe 11](#_Toc126764383)

[2.3.7. Cors 11](#_Toc126764384)

[2.3.8. ProxyServer 11](#_Toc126764385)

[2.4. Test the installation 12](#_Toc126764386)

1. Pre-Installation Requirements

Note: Requirements and prerequisites can be found in the compatibility matrix document.

1. Installation and Configuration
   1. Nginx Configuration

Place the content of the IAM package you received under the following location: “var/www/Intalio.IAM”.

* + 1. HTTP Configuration

To configure Nginx as a reverse proxy to forward requests to the IAM product, copy */etc/nginx/sites-available/default*, and paste it under */etc/nginx/sites-enabled*, rename the file to iam.conf.

Open it in a text editor, and replace the contents with the following:

*server {*

*listen 80;*

*#listen 443 ssl;*

*server\_name identity.intalio.com;*

*client\_max\_body\_size* *20M;*

*proxy\_connect\_timeout* *120s;*

*proxy\_read\_timeout* *3600s;*

*access\_log* *off;*

*#SSL CERTIFICATE*

*#ssl\_certificate* */etc/nginx/ssl/domain\_certs/cert.crt;*

*#ssl\_certificate\_key* */etc/nginx/ssl/domain\_certs/cert.key;*

*location / {*

*proxy\_pass* *http://localhost:5000;*

*proxy\_set\_header* *Host $http\_host;*

*proxy\_set\_header* *X-Real-IP $remote\_addr;*

*proxy\_set\_header* *X-Forwarded-For $proxy\_add\_x\_forwarded\_for;*

*proxy\_set\_header* *X-Forwarded-Proto $scheme;*

*add\_header* *P3P 'CP="ALL DSP COR PSAa PSDa OUR NOR ONL UNI COM NAV"';*

*add\_header* *'Access-Control-Allow-Headers' 'DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';*

*add\_header* *'Access-Control-Allow-Credentials' 'true';*

*add\_header* *'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE';*

*}*

*}*

Notes:

* Highlighted sections are examples.
* The port number (proxy set) will be used in the following sections.

Create *proxy.conf* file under */etc/nginx* and add the following content:

*proxy\_redirect off;*

*proxy\_set\_header Host $host;*

*proxy\_set\_header X-Real-IP $remote\_addr;*

*proxy\_set\_header X-Forwarded-For $proxy\_add\_x\_forwarded\_for;*

*proxy\_set\_header X-Forwarded-Proto $scheme;*

*client\_max\_body\_size 10m;*

*client\_body\_buffer\_size 128k;*

*proxy\_connect\_timeout 90;*

*proxy\_send\_timeout 90;*

*proxy\_read\_timeout 90;*

*http {*

*...*

*include /etc/nginx/proxy.conf;*

*...*

*}*

Modify */etc/nginx/nginx.conf,* andadd the following under the http section:

*http {*

*...*

*proxy\_buffer\_size 128k;*

*proxy\_buffers 4 256k;*

*proxy\_busy\_buffers\_size 256k;*

*large\_client\_header\_buffers 4 16k;*

*include /etc/nginx/proxy.conf;*

*...*

*}*

Note: If the comment include /etc/nginx/sites-enabled/\* does not exist in /etc/nginx/nginx.conf, add the following under the http section:

*http {*

*...*

*proxy\_buffer\_size 128k;*

*proxy\_buffers 4 256k;*

*proxy\_busy\_buffers\_size 256k;*

*large\_client\_header\_buffers 4 16k;*

*include /etc/nginx/proxy.conf;*

*include /etc/nginx/sites-enabled/\*;*

*...*

*}*

Once the Nginx configuration is established, run **sudo nginx -t** to verify the syntax of the configuration files. If the configuration file test is successful, force Nginx to pick up the changes by running **sudo nginx -s reload**.

* + 1. HTTPS Configuration

Note: Google chrome version 84.x+ is required for https.

Modify /etc/nginx/sites-enabled/iam.conf*,* andenable the following in red section:

*server {*

*listen 80;*

*listen 443 ssl;*

*server\_name identity.intalio.com;*

*client\_max\_body\_size* *20M;*

*proxy\_connect\_timeout* *120s;*

*proxy\_read\_timeout* *3600s;*

*access\_log* *off;*

#SSL CERTIFICATE

*ssl\_certificate /etc/nginx/ssl/domain\_certs/cert.crt;*

*ssl\_certificate*\_key /etc/nginx/ssl/domain\_certs/cert.key;

*location / {*

*proxy\_pass* *http://localhost:5000;*

*proxy\_set\_header* *Host $http\_host;*

*proxy\_set\_header* *X-Real-IP $remote\_addr;*

*proxy\_set\_header* *X-Forwarded-For $proxy\_add\_x\_forwarded\_for;*

*proxy\_set\_header* *X-Forwarded-Proto $scheme;*

*add\_header* *P3P 'CP="ALL DSP COR PSAa PSDa OUR NOR ONL UNI COM NAV"';*

*add\_header* *'Access-Control-Allow-Headers' 'DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';*

*add\_header* *'Access-Control-Allow-Credentials' 'true';*

*add\_header* *'Access-Control-Allow-Methods' 'GET, POST, PUT, DELETE';*

*}*

*}*

Note: generate a certificate to support https and provide cert.crt and cert.key.

* 1. Monitor the Application

The server is setup to forward requests made to *http://<serveraddress>:80* on to the IAM product running on Kestrel at *http://127.0.0.1:5000*. However, Nginx isn't set up to manage the Kestrel process. **systemd** can be used to create a service file to start and monitor the underlying IAM product. **systemd** is an init system that provides many powerful features for starting, stopping, and managing processes.

Note: The highlighted 5000 is the previously created port number.

* + 1. Create the Service File

Create the service definition file:

*sudo nano /etc/systemd/system/kestrel-Intalio.IAM.service*

The following is an example service file for the IAM product:

*[Unit]*

*Description=Intalio.IAM App*

*[Service]*

*WorkingDirectory=/var/www/Intalio.IAM*

*ExecStart=/usr/bin/dotnet /var/www/Intalio.IAM/Intalio.IAM.dll*

R*estart=always*

*# Restart service after 10 seconds if the dotnet service crashes:*

*RestartSec=10*

*KillSignal=SIGINT*

*SyslogIdentifier=Intalio.IAM*

*User=www-data*

*Environment*=*ASPNETCORE\_ENVIRONMENT=Production*

*Environment=DOTNET\_PRINT\_TELEMETRY\_MESSAGE=false*

*Environment=ASPNETCORE\_URLS=http://+:5000*

*[Install]*

*WantedBy=multi-user.target*

Note:

* The working directory is the location of the package.
* In the preceding example, the user that manages the service is specified by the User option. The user (www-data) must exist and have a proper ownership of the IAM product’s files.
* The highlighted 5000 is the previously created port number.

Save the file and enable the service.

*sudo systemctl enable kestrel-Intalio.IAM.service*

Start the service and verify that it's running.

*sudo systemctl start kestrel-Intalio.IAM.service*

*sudo systemctl status kestrel-Intalio.IAM.service*

*◝ kestrel-Intalio.IAM.service - Intalio.IAM App*

*Loaded: loaded (/etc/systemd/system/kestrel-Intalio.IAM.service; enabled)*

*Active: active (running) since Thu 2016-10-18 04:09:35 NZDT; 35s ago*

*Main PID: 9021 (dotnet)*

*CGroup: /system.slice/kestrel-Intalio.IAM.service*

*└─9021 /usr/local/bin/dotnet /var/www/Intalio.IAM/Intalio.IAM.dll*

* 1. Appsettings Configuration
     1. Connection String

The connection string can be:

* Plain text.
* Encrypted.

2.2.1.1. Plain Text

Go to **“Intalio.IAM” 🡪 “appsettings.json”** and edit the highlighted keys in the ConnectionStrings section.

* Microsoft SQL Server

Use one of the below modes:

* + Windows authentication.

*"DbConnection":*

*"Server=ETGS-MAL\\SQL14;Database=IAM;MultipleActiveResultSets=true;Integrated Security=True;"*

* + SQL server authentication.

*"DbConnection":*

*"Server=ETGS-*

*MAL\\SQL14;Database=IAM;MultipleActiveResultSets=true;Integrated Security=False;User=ES;Password=ES;"*

* PostgreSQL.

*"DbConnection": "User ID=postgres;Password=P@$$w0rd;Server=localhost;Port=5432;Database=IAM;Integrated Security=true;Pooling=true;"*

* MYSQL.

*"DbConnection": "Server=localhost;Database=iam;Uid=root;Pwd=P@$$w0rd;"*

* Oracle.

*"DbConnection": "User ID=IAM;Password= IAM;Data Source=localhost:1521/orcl.everteam-mea.com"*

Note: You must create IAM user in Oracle having privileges to create and modify schemas before running the app for the first time.

For Oracle, the package will work with a new database only, due to a known Hangfire issue, which does not create its related tables on Oracle database. For Hangfire to open and function properly, “Hangfire.Oracle.Install.sql” needs to be executed on the Oracle IAM database before starting the IAM application (the file can be found in the package).

2.3.1.2. Encrypted

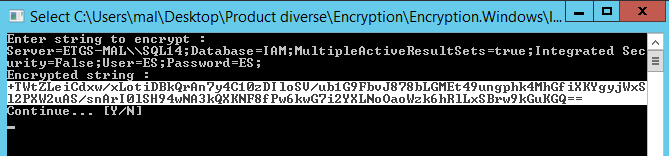
To use an encrypted connection string in IAM, edit **appsettings. json** and add the following:

*"IsConnectionStringEncrypted": "true"*

In the **DbConnection**section, replace its plain text value with its related encrypted value.

The encrypted connection string can be obtained using the encryption tool **Encryption.Windows** provided in the package under **/Tools/Encryption.**

Double click **Intalio.Encryption.exe** enter the plain text value and get its encryption:



The appsettings should be similar to the following:

*{*

*"Logging": {*

*"LogLevel": {*

*"Default": "Information",*

*"Microsoft": "Warning",*

*"Microsoft.Hosting.Lifetime": "Information"*

*}*

*},*

*"AllowedHosts": "\*",*

*"ConnectionStrings": {*

*"DbConnection": "+TWtZLeiCdzq+4PWOhRxY8DPLctlkMh3U32/HCoORGEanAMYrWdusOnLgOw9QC7+G2vxiObqLOE+jgzy9eIC23PqJqo+8Wx+4RcBR74et1T027KHyam0Ic02xrd1eBCYqQNHvbrAkuyjXAAxwwX1hnw7ZMUQivQl"*

*},*

*"DatabaseType": "PostgreSQL",*

*"IsConnectionStringEncrypted": "true"*

*}*

* + 1. Database Type

Go to **“Intalio.IAM” à “appsettings.json”** and select one value of Database Type, based on the chosen connection string, as follows:

*For PostgresSQL:*

*“DatabaseTypes”: “PostgresSQL”*

*For MSSQL:*

*“DatabaseTypes”: “MSSQL”*

*For Oracle:*

*“DatabaseTypes”: “Oracle”*

* + 1. Jobs

Go to “**Intalio.IAM**” 🡪 “**appsettings.json**” and edit the following values:

|  |  |
| --- | --- |
| **Configuration** | **Description** |
| **EnableBackgroundJobs** | To enable/disable background jobs (integration jobs). If disabled, only data source page is displayed from integration section. |
| **SchedulePollingInterval** | Hangfire Server periodically checks the schedule to enqueue scheduled jobs to their queues, allowing workers to execute them. By default, check interval is equal to 15 seconds, but you can change it by setting the SchedulePollingInterval property. |
| **StatsPollingInterval** | Interval which Hangfire UI periodically checks the database. |

* + 1. Health Check

Go to “**Intalio.IAM**” 🡪 “**appsettings.json**” and edit the following values:

|  |  |  |
| --- | --- | --- |
| **Configuration** | **Description** | |
| **HealthChecks > Name** | | Application name. | This section (Name, URI) should be added for each application to be monitored. |
| **HealthChecks > Uri** | | Application URI. |
| **SystemEmail** | | The list of emails that should receive health check notifications is assigned to this value. | |
| **EvaluationTimeInSeconds** | | Number of elapsed seconds between health checks. | |
| **MinimumSecondsBetweenFailureNotifications** | | The minimum seconds between failure notifications to avoid receiver flooding | |

* + 1. Cookie Life Time

Go to “**Intalio.IAM**” 🡪 “**appsettings.json**” and edit the following values:

|  |  |
| --- | --- |
| **Configuration** | **Description** |

|  |  |
| --- | --- |
| **PersistentCookieLifeTime** | Support configuring the persistent cookie lifetime from the appsettings (cookie lifetime when remember me is checked)  The default lifetime of the specified cookie is 604800 seconds (7 days) |

* + 1. OpenInIframe

Go to “**Intalio.IAM**” à “**appsettings.json**” and edit the following values:

|  |  |
| --- | --- |
| **Configuration** | **Description** |

|  |  |
| --- | --- |
| **OpenInIframe** | Enable IAM to open in iframe to allowed urls separated by ,. |
| **Enabled** | When true, open iframe feature is enabled. |
| **URLs** | List of URL that are allowed to open in iframe. |

* + 1. Cors

Go to “**Intalio.IAM**” à “**appsettings.json**” and edit the following values:

|  |  |
| --- | --- |
| **Configuration** | **Description** |

|  |  |
| --- | --- |
| **CORS** | Cross-Origin Resource Sharing (CORS) is an HTTP-header based mechanism that allows a server to indicate any origins (domain, scheme or port) other than its own from which a browser should permit loading resources. |
| **URLs** | List of URL that are allowed to use IAM for security reasons. |

* + 1. ProxyServer

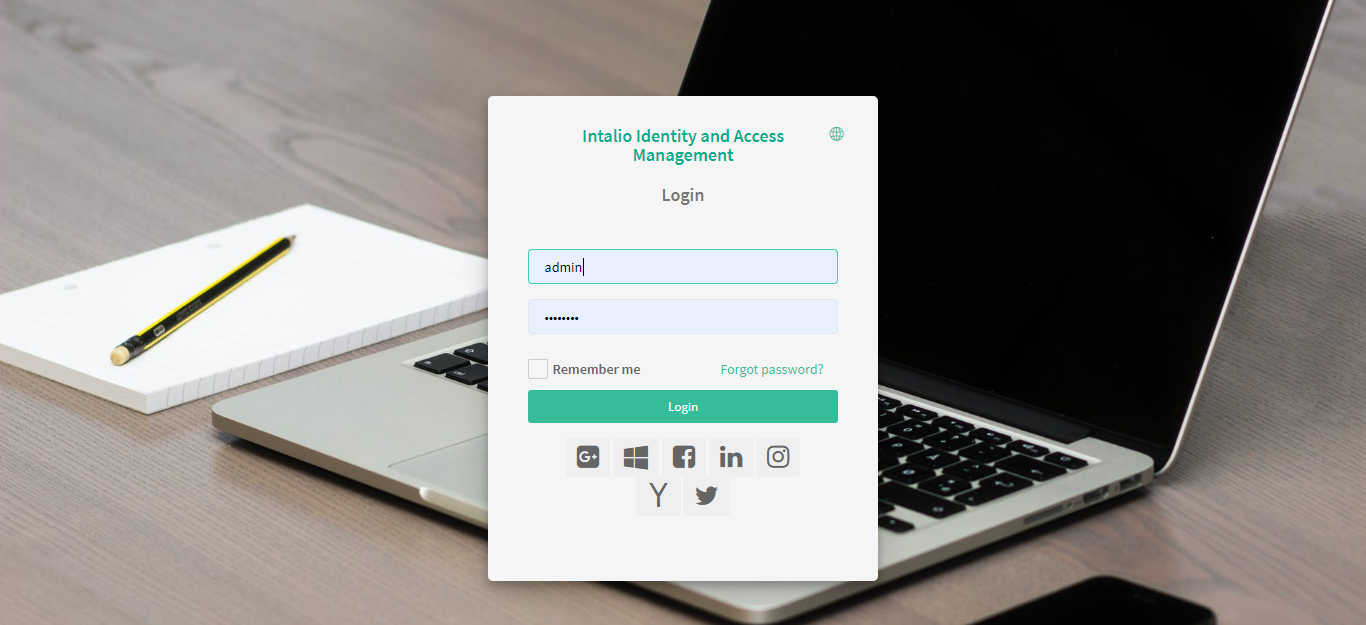
Go to “**Intalio.IAM**” à “**appsettings.json**” and edit the following values:

|  |  |
| --- | --- |
| **Configuration** | **Description** |

|  |  |
| --- | --- |
| **ProxyServer** | Name of the proxy server and is used when the environment is using proxy server. |

* 1. Test the installation

Login with Intalio IAM URL to test that the application is working correctly:



Enter the admin credentials, the system should redirect you to the following:

