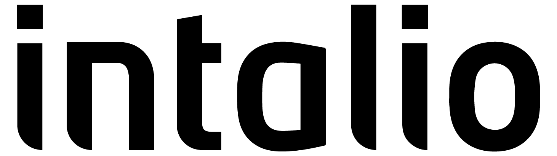
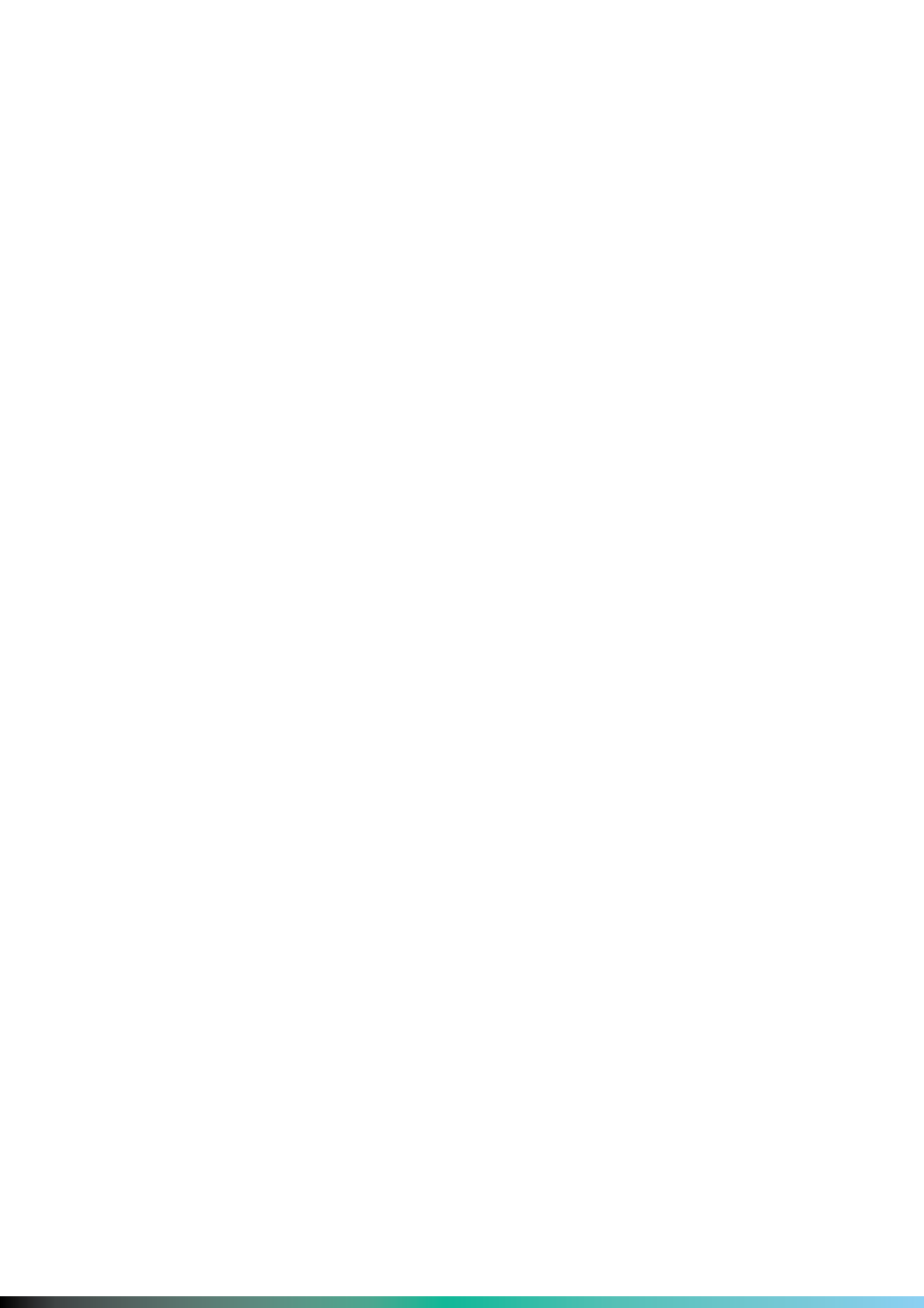
**** 

Version: 3.1.0

Intalio IAM

Installation Guide - Linux (FR)

**Vision.**

Making business simple by connecting people, processes and content.

Intalio est un fournisseur international de logiciels avec 30 ans d'innovation dans le domaine des services de contenu et de processus. En combinant des technologies de pointe avec l'IA et l'apprentissage machine pour introduire des solutions de secteur d'activité avancées, Intalio a réussi à devenir un leader de confiance dans la transformation numérique aux États-Unis, en Europe et dans la région MENA.

Table des matières

[1. Conditions prérequis à l'installation 3](#_Toc126764272)

[2. Installation et Configuration 4](#_Toc126764273)

[2.1. Configuration Nginx 4](#_Toc126764274)

[2.1.1. Configuration HTTP 4](#_Toc126764275)

[2.1.2. Configuration HTTPS 5](#_Toc126764276)

[2.2. Surveiller l'application 6](#_Toc126764277)

[2.2.1. Créer le fichier de service 6](#_Toc126764278)

[2.3. Configuration Appsettings 7](#_Toc126764279)

[2.3.1. Chaîne de connexion 7](#_Toc126764280)

[2.4.1.1. Texte brut 8](#_Toc126764286)

[2.4.1.2. Crypté 8](#_Toc126764287)

[2.3.2. Type de base de données 9](#_Toc126764288)

[2.3.3. Emplois 10](#_Toc126764289)

[2.3.4. Health check 10](#_Toc126764290)

[2.3.5. Cookie Life Time 11](#_Toc126764291)

[2.3.6. OpenInIframe 11](#_Toc126764292)

[2.3.7. Cors 11](#_Toc126764293)

[2.3.8. ProxyServer 12](#_Toc126764294)

[2.4. Tester l'installation 12](#_Toc126764295)

1. Conditions prérequis à l'installation

Remarque : les exigences et les prérequis peuvent être trouvés dans compatibility matrix document.

1. Installation et Configuration
   1. Configuration Nginx

Placez le contenu du package IAM à l'emplacement suivant : « var/www/Intalio.IAM »

* + 1. Configuration HTTP

Pour configurer Nginx en tant que proxy inverse pour transférer les requêtes vers le produit IAM, copiez */etc/nginx/sites-available/default* et collez-le sous */etc/nginx/sites-enabled*, renommez le fichier en iam.conf.

Ouvrez-le dans un éditeur de texte et remplacez le contenu par ce qui suit :

*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';*

*}*

*}*

**Remarques** :

* Les sections surlignées sont des exemples.
* Le numéro de port (proxy pass) sera utilisé dans les sections suivantes.

Créez le fichier proxy.conf sous /etc/nginx et ajoutez le contenu suivant :

*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;*

Modifier /etc/nginx/nginx.conf, et ajoutez ce qui suit dans la section http :

*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;*

*...*

*}*

Remarque : Si le commentaire include /etc/nginx/sites-enabled/\*  n'existe pas dans /etc/nginx/nginx.conf, ajoutez ce qui suit sous la section http :

*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/\*;*

*...*

*}*

Une fois la configuration Nginx établie, exécutez **sudo nginx -t** pour vérifier la syntaxe des fichiers de configuration. Si le test du fichier de configuration réussit, forcez Nginx à récupérer les modifications en exécutant **sudo nginx -s reload**.

* + 1. Configuration HTTPS

Remarque : la version 84.x+ de Google Chrome est requise pour https.

Modifier /etc/nginx/sites-available/default et ajoutez le contenu rouge suivant :

*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';*

*}*

*}*

Remarque : générez un certificat pour prendre en charge https et fournissez cert.crt et cert.key.

* 1. Surveiller l'application

Le serveur est configuré pour transférer les demandes adressées à *http://<serveraddress> :80* vers le produit IAM exécuté sur Kestrel à l'adresse *http://127.0.0.1:5000*. Cependant, Nginx n'est pas configuré pour gérer le processus Kestrel. **systemd** peut être utilisé pour créer un fichier de service pour démarrer et surveiller le produit IAM sous-jacent. **systemd** est un système d'initialisation qui fournit de nombreuses fonctionnalités puissantes pour démarrer, arrêter et gérer les processus.

Remarque : Le 5000 en surbrillance est le numéro de port créé précédemment.

* + 1. Créer le fichier de service

Créez le fichier de définition de service :

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

Voici un exemple de fichier de service pour le produit IAM :

*[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*

Remarques :

* Le répertoire de travail (working directory) est l'emplacement du package.
* Dans l'exemple précédent, l'utilisateur qui gère le service est spécifié par l'option Utilisateur. L'utilisateur (www-data) doit exister et être propriétaire des fichiers du produit IAM.
* Le 5000 en surbrillance est le numéro de port créé précédemment.

Enregistrez le fichier et activez le service.

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

Démarrez le service et vérifiez qu'il est en cours d'exécution.

*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. Configuration Appsettings
     1. Chaîne de connexion

La chaîne de connexion peut être soit :

* Texte brut.
* Crypté.

2.4.1.1. Texte brut

Accédez à « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les clés surlignés dans la section ConnectionStrings.

* Serveur Microsoft SQL

Utilisez l'un des modes ci-dessous :

* 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"*

Remarque : vous devez créer un utilisateur IAM dans Oracle avec des privilèges pour créer et modifier des schémas avant d'exécuter l'application pour la première fois.

Pour Oracle, le package fonctionnera uniquement avec une nouvelle base de données, en raison d'un problème connu de Hangfire, qui ne crée pas ses tables associées sur la base de données Oracle. Pour que Hangfire s'ouvre et fonctionne correctement, « Hangfire.Oracle.Install.sql » doit être exécuté sur la base de données Oracle CTS avant de démarrer l'application CTS (le fichier se trouve dans le package).

2.4.1.2. Crypté

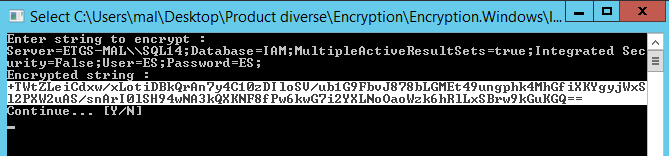
Pour utiliser une chaîne de connexion chiffrée dans IAM, modifiez **appsettings.json** et ajoutez les éléments suivants :

*"IsConnectionStringEncrypted": "true"*

Dans la section **DbConnection**, remplacez sa valeur en texte brut par sa valeur chiffrée associée.

La chaîne de connexion cryptée peut être obtenue à l'aide de l'outil de cryptage **Encryption.Windows** fourni dans le package sous **/Tools/Encryption**.

Double-cliquez sur **Intalio.Encryption.exe**, saisissez la valeur en texte brut et obtenez son cryptage :



Les paramètres d'application doivent ressembler à ce qui suit :

*{*

*"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. Type de base de données

Accédez à « **Intalio.IAM** » 🡪 « **appsettings.json** » et sélectionnez une valeur de type de base de données, en fonction de la chaîne de connexion choisie, comme suit :

*For PostgresSQL:*

*“DatabaseTypes”: “PostgresSQL”*

*For MSSQL:*

*“DatabaseTypes”: “MSSQL”*

*For Oracle:*

*“DatabaseTypes”: “Oracle”*

* + 1. Emplois

Allez dans « **Intalio.CTS** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

|  |  |
| --- | --- |
| **Configuration** | **Description** |
| **EnableBackgroundJobs** | Pour activer/désactiver les tâches en arrière-plan (tâches d'intégration). Si elle est désactivée, seule la page de la source de données est affichée à partir de la section d'intégration. |
| **SchedulePollingInterval** | Hangfire Server vérifie périodiquement le calendrier pour mettre en file d'attente les tâches planifiées dans leurs files d'attente, permettant aux travailleurs de les exécuter. Par défaut, l'intervalle de vérification est égal à 15 secondes, mais vous pouvez le modifier en définissant la propriété SchedulePollingInterval. |
| **StatsPollingInterval** | Intervalle auquel l'interface utilisateur Hangfire vérifie périodiquement la base de données. |

* + 1. Health check

Allez dans « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

|  |  |  |
| --- | --- | --- |
| **Configuration** | **Description** | |
| **HealthChecks > Name** | | Nom de l'application. | Cette section (Nom, URI) doit être ajoutée pour chaque application à surveiller. |
| **HealthChecks > Uri** | | Application URI. |
| **SystemEmail** | | La liste des e-mails qui doivent recevoir des notifications de vérification de l'état est affectée à cette valeur. | |
| **EvaluationTimeInSeconds** | | Nombre de secondes écoulées entre les vérifications de l'état. | |
| **MinimumSecondsBetweenFailureNotifications** | | Les secondes minimales entre les notifications d'échec pour éviter l'inondation du récepteur. | |

* + 1. Cookie Life Time

Allez dans « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

|  |  |
| --- | --- |
| **Configuration** | **Description** |
| **PersistentCookieLifeTime** | Prise en charge de la configuration de la durée de vie des cookies persistants à partir des paramètres d'application (durée de vie des cookies lorsque se souvenir de moi est coché)  La durée de vie par défaut du cookie spécifié est de 604800 secondes (7 jours) |

* + 1. OpenInIframe

Allez dans « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

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

|  |  |
| --- | --- |
| **OpenInIframe** | Activez IAM pour qu'il s'ouvre dans l'iframe aux URL autorisées séparées par ,. |
| **Enabled** | Lorsqu'il est vrai, la fonction d'ouverture d'iframe est activée. |
| **urls** | Liste des URL autorisées à s'ouvrir dans l'iframe. |

* + 1. Cors

Allez dans « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

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

|  |  |
| --- | --- |
| **cors** | Cross-Origin Resource Sharing (CORS) est un mécanisme basé sur un en-tête HTTP qui permet à un serveur d'indiquer toute origine (domaine, schéma ou port) autre que la sienne à partir de laquelle un navigateur doit autoriser le chargement des ressources. |
| **urls** | Liste des URL autorisées à utiliser IAM pour des raisons de sécurité. |

* + 1. ProxyServer

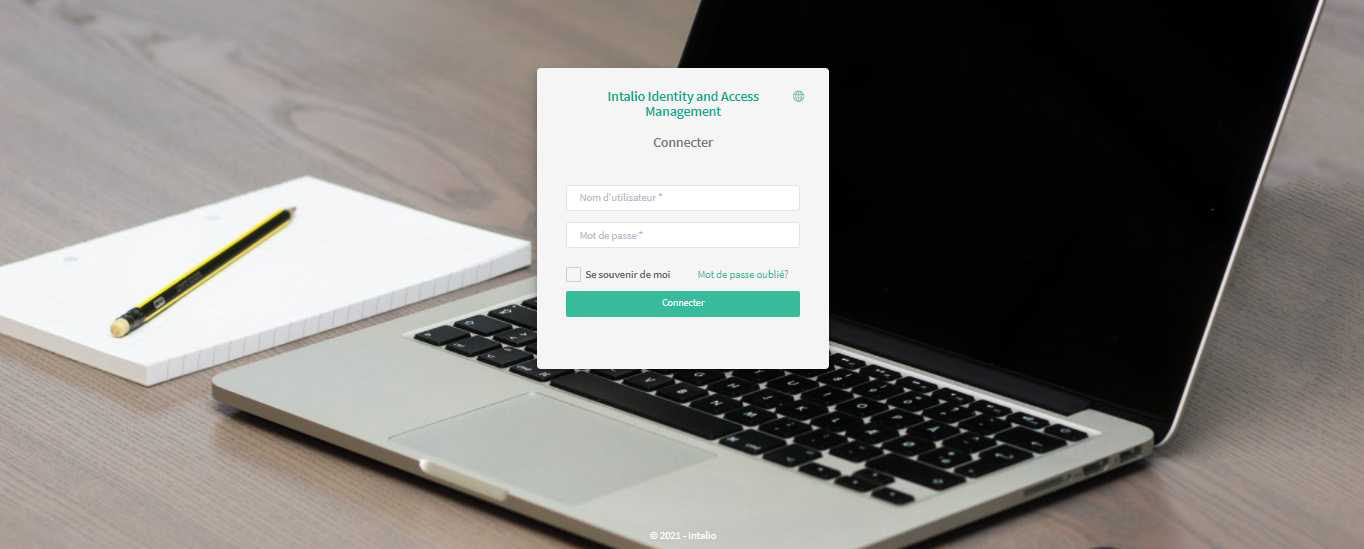
Allez dans « **Intalio.IAM** » 🡪 « **appsettings.json** » et modifiez les valeurs suivantes :

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

|  |  |
| --- | --- |
| **ProxyServer** | Nom du serveur proxy et est utilisé lorsque l'environnement utilise un serveur proxy. |

* 1. Tester l'installation

Connectez-vous avec l'URL Intalio IAM pour tester le bon fonctionnement de l'application :



Entrez les informations d'identification de l'administrateur, le système devrait vous rediriger vers ce qui suit :

