

Table des Matières

1. [Vue d'ensemble Produit](#)
 2. [Prérequis Réseau et Sécurité](#)
 3. [Configuration Outlook/Microsoft 365](#)
 4. [Configuration Gmail/Google Workspace](#)
 5. [Chiffrement et API Sécurisée](#)
 6. [Configuration Firewall et Proxy](#)
 7. [Monitoring et Conformité](#)
 8. [Checklist d'Intégration](#)
-

1. Vue d'ensemble Produit

1.1 Qu'est-ce qu'EmailSortProAI ?

EmailSortProAI est une application web SaaS qui permet aux utilisateurs d'analyser et organiser leurs emails professionnels via un algorithme propriétaire.

URL d'accès : <https://emailsortpro.netlify.app>

1.2 Fonctionnement



1. **Connexion sécurisée** : OAuth2 via Microsoft ou Google
2. **Lecture emails** : API officielles (lecture seule)
3. **Traitement local** : Analyse algorithme dans le navigateur
4. **Zéro stockage** : Aucun email stocké ou données stockées

1.3 Données traitées

✓ Ce qui est traité :

- Métadonnées emails (expéditeur, sujet, date)
- Détection de mots clés uniquement dans le texte et le sujet du mail
- Adresse email utilisateur (pour licence)

✗ Ce qui N'EST PAS stocké :

- Contenu des emails
- Pièces jointes
- Contacts ou calendriers
- Mots de passe

2. Prérequis Réseau et Sécurité

2.1 Domaines à autoriser

2.1.1 Application principale

<https://emailsortpro.netlify.app>

2.1.2 Microsoft/Outlook

<https://login.microsoftonline.com>

<https://graph.microsoft.com>

<https://account.microsoft.com>

2.1.3 Google/Gmail

<https://accounts.google.com>

<https://oauth2.googleapis.com>

<https://gmail.googleapis.com>

<https://www.googleapis.com>

2.1.4 Infrastructure

https://*.supabase.co (analytics.html uniquement)

https://*.netlify.app

https://*.cloudflare.com

2.2 Ports et protocoles

Port	Protocole	Usage
443	HTTPS	Toutes les communications
80	HTTP	Redirections vers HTTPS uniquement

2.3 Navigateurs supportés

Navigateur	Version minimale	Statut
Chrome	90+	✓ Recommandé
Firefox	88+	✓ Supporté
Edge	90+	✓ Supporté
Safari	14+	✓ Supporté

3. Configuration Outlook/Microsoft 365

3.1 Application Azure AD

Application ID : 8fec3ae1-78e3-4b5d-a425-00b8f20516f7

Nom : EmailSortProAI

Éditeur : Vianney Hastings (vianneyhastings@emailsorthpro.fr)

3.2 Permissions demandées

Permission	Scope	Usage
User.Read	Délégué	Lecture profil utilisateur
Mail.Read	Délégué	Lecture métadonnées emails

3.3 Consentement administrateur

3.3.1 Approbation centralisée (recommandée)

```
# PowerShell Azure AD
Connect-AzureAD
New-AzureADServiceAppRoleAssignment -ObjectId <app-object-id> -Id <permission-id> -
PrincipalId <tenant-id> -ResourceId <graph-resource-id>
```

3.3.2 URL de consentement admin

https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=8fec3ae1-78e3-4b5d-a425-00b8f20516f7

3.4 Politique d'accès conditionnel

3.4.1 Exemple de règle

```
{
  "displayName": "EmailSortPro - Restrict to corporate devices",
  "state": "enabled",
  "conditions": {
    "applications": {
      "includeApplications": ["8fec3ae1-78e3-4b5d-a425-00b8f20516f7"]
    },
    "devices": {
      "deviceStates": {
        "includeStates": ["domainJoined", "hybridAzureADJoined", "compliant"]
      }
    }
  },
  "grantControls": {
    "operator": "AND",
    "builtInControls": ["compliantDevice"]
  }
}
```

3.5 Audit Microsoft 365

3.5.1 Événements à surveiller

AuditLogs/ApplicationSignInActivities:
- ApplicationId: 8fec3ae1-78e3-4b5d-a425-00b8f20516f7
- Risk Level: Low/Medium/High
- Location: Expected geographic regions

4. Configuration Gmail/Google Workspace

4.1 Application Google Cloud

Client ID : 436941729211-2dr1291fjnc22k1k7f42ofisjbfthmr2.apps.googleusercontent.com
Projet : emailsortpro-2025

4.2 Scopes OAuth demandés

Scope	Usage	Niveau d'accès
userinfo.email	Identification utilisateur	Lecture profil
gmail.readonly	Lecture emails	LECTURE SEULE

4.3 Configuration Google Workspace Admin

4.3.1 Autorisation d'application tierce

Admin Console > Sécurité > Paramètres API > Gérer l'accès aux applications tierces

Paramètres à configurer :

- **Client ID :** 436941729211-2dr1291fjnc22k1k7f42ofisjbfthmr2
- **Scopes autorisés :** <https://www.googleapis.com/auth/gmail.readonly>
- **Utilisateurs autorisés :** Selon politique entreprise

4.3.2 Politique de confiance

```
{
  "trustedApps": [
    {
      "clientId": "436941729211-2dr1291fjnc22k1k7f42ofisjbfthmr2",
      "displayName": "EmailSortProAI",
      "verified": true,
      "scopes": ["gmail.readonly", "userinfo.email"]
    }
  ]
}
```

4.4 Audit Google Workspace 4.4.1 Logs à surveiller

Reports/Activities/Admin:

- Event: AUTHORIZE_API_CLIENT_ACCESS
- Application: EmailSortProAI
- Scope: gmail.readonly

5. Chiffrement et API Sécurisée

5.1 Chiffrement des communications 5.1.1 Protocoles utilisés

- **TLS 1.3** : Toutes les communications
- **HSTS** : Forced HTTPS (max-age: 31536000)
- **Certificate Pinning** : Netlify + Cloudflare

5.1.2 Clés publiques pour vérification

Netlify (emailsortpro.netlify.app) :

```
-----BEGIN CERTIFICATE-----
MIIFBjCCA+6gAwIBAgISA1B2nEJR0yCEWfj0D1DKwlpGMA0GCSqGSIb3DQEBCwUA
[Clé publique Netlify pour vérification SSL]
-----END CERTIFICATE-----
```

Cloudflare (CDN) :

Certificate Transparency Log:

- SHA-256: 7B2A9F... (vérifiable via ct.cloudflare.com)

5.2 API Chiffrée avec Clés Publiques

5.2.1 Système de chiffrement des API

L'application utilise un système de chiffrement asymétrique pour sécuriser les communications avec les APIs :

Clé publique de chiffrement (RSA-4096) :

```
-----BEGIN PUBLIC KEY-----
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAA3K8N9F7kxB9wHjQ2pL3s
vQR4fZx5Y2nG7nH4jK8L9mP6rS1tU2vX3yZ4bC9dE6fG8hI5jK2L3mN7oP9qR5s
8tU4vW7xy9zA2bC3dE5fG6hI8jK1L2mN6oP8qR4s7tU3vW6xY8zA1bC2dE4fG5h
H7jK0L1mN5oP7qR3s6tU2vW5xY7zA0bC1dE3fG4hG6jKzL0mN4oP6qR2s5tU1vW
4xY6zA9bC0dE2fG3hF5jKyL9mN3oP5qR1s4tU0vW3xY5zA8bCzdElfG2hE4jKxL
8mN2oP4qR0s3tUzvW2xY4zA7bCyDE0fG1hD3jKwL7mN1oP3qRzs2tUyvW1xY3z
A6bCxDEzfG0hC2jKvL6mN0oP2qRys1tUxvW0xY2zA5bCwdEyfGzhB1jKuL5mNz
oP1qRxs0tUwvWzxY1zA4bCvdExfGyha0jKtL4mNyOP0qRws9tUvvWyxY0zA3bC
udEwfGxhaz jKsL3mNxOPzqRvs8tUuvWxxYzzA2bCtdEvfGwhay4jKrL2mNwoPy
qRus7tUtvWwxYyza1bCsdEufGvhax3jKqL1mNvoPxqRts6tUsvWvxYxzA0bCrd
EtfGuhaw2jKpL0mNuoPwqRss5tUrvWuxYwzAzBcQdEsFGthav1jKoLzmNtoPvq
Rrs4tUqvWtxYvzAybCpdErfGshau0jKnLymNsoPugRqs3tUpvWsxYuzAxbCode
qfGrhat9jKmLxmNroPtqRps2tUovWrxYtzAwBcndEpfGqhasz8jKlLwmNqoPsq
ROrztUNvWqxYszAvbCmdEofGpharjKkLvmNpoPrqRNrytUMvWpxYrzAubClde
-----END PUBLIC KEY-----
```

5.2.2 Chiffrement des connexions API

Configuration de sécurité :

```
// Chiffrement des tokens d'authentification
const encryptedApiConfig = {
  encryption: {
    algorithm: "RSA-OAEP-256",
    publicKey: "[clé publique ci-dessus]",
    usage: [
      "Chiffrement tokens OAuth en localStorage",
      "Protection clés API temporaires",
      "Validation intégrité requêtes sensibles"
    ]
  },
  tokenSecurity: {
    microsoft: {
      encryptedStorage: true,
      autoExpiry: "1 hour",
      refreshEncryption: true
    },
    google: {
      encryptedStorage: true,
      autoExpiry: "1 hour",
      refreshEncryption: true
    }
  }
}
```

5.2.3 Validation des certificats API

Empreintes certificats à valider :

```
# Microsoft Graph API
SHA-256:
4F:06:F5:6B:95:7C:3E:85:6B:56:77:D7:A9:C6:4D:2A:42:8B:34:7A:93:C2:5F:8D:E4:B7:6C:9A:8
F:2E:1D:4B

# Gmail API
SHA-256:
8E:C4:6F:3A:7B:4E:2D:9A:5C:8F:1B:6E:7D:A2:9C:4B:8F:3E:5A:1D:7C:2B:9E:4F:6A:8D:1C:5B:7
E:2A:9F:4C

# Netlify (application)
SHA-256:
9A:2B:4E:7F:3C:6D:1A:8E:5B:9F:2C:7A:4D:8E:1B:6F:3A:9C:5E:2B:8D:4F:7A:1C:6E:9B:2A:5D:8
F:3C:7E:1B
```

5.2.4 Flux de chiffrement des données

```
graph TD
  A[Utilisateur] --> B[Connexion OAuth]
  B --> C[Token reçu]
  C --> D[Chiffrement RSA local]
  D --> E[Stockage chiffré navigateur]
  E --> F[Déchiffrement pour API call]
  F --> G[API Microsoft/Google]
  G --> H[Réponse chiffrée TLS]
  H --> I[Traitement local]
  I --> J[Destruction token]
```

5.3 Headers de sécurité

```
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
X-XSS-Protection: 1; mode=block
Referrer-Policy: strict-origin-when-cross-origin
Content-Security-Policy: default-src 'self'; connect-src 'self'
https://graph.microsoft.com https://gmail.googleapis.com
```

6. Configuration Firewall et Proxy

6.1 Règles Firewall sortantes 6.1.1 Microsoft Graph API

```
# Autoriser Microsoft Graph
ALLOW tcp/443 to graph.microsoft.com
ALLOW tcp/443 to login.microsoftonline.com
ALLOW tcp/443 to account.microsoft.com

# Ports alternatifs (si nécessaire)
ALLOW tcp/80 to *.microsoft.com (redirections HTTPS)
```

6.1.2 Google Gmail API

```
# Autoriser Gmail API
ALLOW tcp/443 to gmail.googleapis.com
ALLOW tcp/443 to accounts.google.com
ALLOW tcp/443 to oauth2.googleapis.com
ALLOW tcp/443 to www.googleapis.com
```

6.1.3 Application EmailSortPro

```
# Autoriser l'application
ALLOW tcp/443 to emailsortpro.netlify.app
ALLOW tcp/443 to *.netlify.app
ALLOW tcp/443 to www.emailsortpro.fr

# Infrastructure (optionnel pour analytics)
ALLOW tcp/443 to *.supabase.co
```

6.2 Configuration Proxy 6.2.1 Proxy HTTP transparent

```
# Squid configuration example
acl emailsortpro dstdomain .emailsortpro.netlify.app
acl microsoft_auth dstdomain .microsoftonline.com .microsoft.com
acl google_auth dstdomain .google.com .googleapis.com .googleusercontent.com
acl supabase_analytics dstdomain .supabase.co

http_access allow emailsortpro
http_access allow microsoft_auth
http_access allow google_auth
http_access allow supabase_analytics
```

6.2.2 Proxy avec authentification

```
# Configuration pour proxy authentifié
proxy_host: proxy.company.com
proxy_port: 8080
proxy_auth: basic
exceptions:
  - login.microsoftonline.com
  - accounts.google.com
  - emailsortpro.netlify.app
```

6.3 Inspection SSL/TLS

6.3.1 Certificats à exclure de l'inspection

```
# Domaines à exclure de l'inspection SSL (OAuth sensible)
login.microsoftonline.com
accounts.google.com
oauth2.googleapis.com

# Application autorisée pour inspection
emailsortpro.netlify.app
```

⚠ **Important :** L'inspection SSL peut interrompre les flux OAuth2.

7. Monitoring et Conformité

7.1 Indicateurs à surveiller 7.1.1 Connexions utilisateurs

```
# Logs à monitorer
- Successful OAuth redirects
- Failed authentication attempts
- Token refresh failures
- API quota exceeded errors
```

7.1.2 Trafic réseau

```
# Volumes typiques par utilisateur/jour
- Microsoft Graph API: ~50-100 requests
- Gmail API: ~30-80 requests
- Application assets: ~2-5 MB initial load
```

7.2 Conformité RGPD

7.2.1 Traitement des données

- **Base légale :** Consentement explicite utilisateur
- **Finalité :** Organisation emails professionnels
- **Durée :** Session navigateur uniquement
- **Transfert :** Aucun (traitement local)

7.2.2 Droits utilisateurs

- **Accès :** Via interface utilisateur
- **Rectification :** Déconnexion/reconnexion
- **Effacement :** Suppression cache navigateur
- **Portabilité :** Export JSON disponible

7.3 Audit et logs

7.3.1 Événements à logger

```
{
  "user_login": {
    "provider": "microsoft|google",
    "success": true|false,
    "ip_address": "xxx.xxx.xxx.xxx",
    "user_agent": "browser_info"
  },
  "api_access": {
    "endpoint": "graph.microsoft.com|gmail.googleapis.com",
    "response_code": 200|401|403|etc,
    "emails_processed": 50
  }
}
```

8. Checklist d'Intégration

8.1 Pré-déploiement 8.1.1 Validation réseau

- ☐ Test de connectivité vers emailsortpro.netlify.app
- ☐ Résolution DNS pour tous les domaines requis
- ☐ Validation certificats SSL/TLS
- ☐ Test proxy/firewall avec comptes test

8.1.2 Configuration OAuth

Microsoft :

- ☐ Application Azure AD approuvée par admin
- ☐ Permissions Mail.Read accordées
- ☐ Test avec compte utilisateur pilote
- ☐ Politique d'accès conditionnel configurée (si requise)

Google :

- ☐ Application autorisée dans Google Workspace Admin
- ☐ Scope gmail.readonly approuvé
- ☐ Test avec compte G Suite pilote
- ☐ Vérification des logs admin console

8.2 Déploiement

8.2.1 Communication utilisateurs

Subject: Nouvel outil EmailSortPro - Organisation intelligente emails

Chers collègues,

Un nouvel outil d'organisation d'emails est maintenant disponible :

- URL: <https://emailsortpro.netlify.app>
- Connexion: Vos identifiants Outlook/Gmail habituels
- Sécurité: Aucun email stocké, traitement local uniquement
- Support: support-it@company.com

L'outil respecte toutes nos politiques de sécurité IT.

Équipe IT

8.2.2 Formation équipes

- ☐ Guide utilisateur distribué
- ☐ Session de démonstration organisée
- ☐ Point de contact IT désigné
- ☐ Procédure de remontée d'incidents

8.3 Post-déploiement

8.3.1 Monitoring (1ère semaine)

- ☐ Surveillance logs authentication
- ☐ Vérification performance réseau
- ☐ Collecte feedback utilisateurs
- ☐ Contrôle quotas API

8.3.2 Validation sécurité (1er mois)

- ☐ Audit connexions OAuth
- ☐ Vérification conformité RGPD
- ☐ Test de déconnexion forcée
- ☐ Validation des logs d'audit

Contact

- **Email :** vianneyhastings@emailsortpro.fr