

Sommaire

- Il était une fois FusionDirectory 1.4
- Nouveautés cœur et plugins
- Une nouvelle interface
- Nouveautés pour l'éducation
- Support multi distribution
- Webservices REST
- Des nouveaux outils pour les développeurs



Il était une fois FusionDirectory 1.4

L'histoire de FusionDirectory 1.4

- FusionDirectory 1.4 était initialement prévu sortir fin 2019
- La participation a deux projets d'envergure a retardé sa sortie de près de deux ans.
- Le covid et un décès dans l'équipe on encore retardé sa sortie
- Les projets :
 - Du Campus Condorcet
 - Télécom SudParis
 - Université d'orléans
 - Renater

ont apportés de nombreuses fonctionnalités et innovations

Améliorations techniques

- Pour répondre au nouveaux besoins de gestion des identités FusionDirectory à du évoluer
- FusionDirectory est passe d'un logiciel de gestion des identités à un portail de gestion des identités :
 - Webservices REST
 - Moteur de tâches
 - Moteur de modèles de mails
 - Gestion de l'archivage des comptes
 - Fusiondirectory Orchestrator : Orchestrateur avec endpoint REST
 - Fusiondirectory Integrator : ensemble de librairies pour construire des applications en mode console



Nouveauté cœur et plugins

Nouvelles fonctionnalités du coeur

- Tâches
- Modèle de mail

Nouveaux plugins 1/3

- Gestion utilisateurs et groupes
 - ✓ Archive
 - ✓ Dynngroups
 - ✓ Nextcloud
 - ✓ Schac
 - ✓ Subscriptions

Nouveaux plugins 2/3

- Messagerie
 - ✓ zimbra
 - ✓ Mailinblack
 - ✓ Migration-mailrouting

- Réseau
 - ✓ Autofs5
 - ✓ ipam

Nouveaux plugins 3/3

- Workflow
 - ✓ Invitation
 - ✓ Public forms
- Sécurité
 - ✓ Webauthn



Une nouvelle interface

Un nouveau système de filtres

- Multi sélection sur les champs de recherche
- Pop-up sur le type d'objet montre l'objectClass LDAP
- Écran dynamique en fonction des extensions installées
- Les types de filtres s'adaptent à la rubrique filtrée
- Possibilité de mettre un filtre ldap dans le champ de recherche

Filtre

Types

Utilisateur

Modèle

Onglet

Unix

Personnel

Courriel

Samba

SSH

Quota

Ftp

Freeradius

SupAnn

État SupAnn

Certificats

Sous traitance

SpamAssassin

Bulletin d'actualités

GPG

EJBCA

Chercher dans les sous-arbres

Q

Appliquer le filtre

Listes dynamiques

- Il est possible de choisir ce que l'on veut afficher et le rendre permanent

Utilisateurs

Base / Actions

	Nom de famille ▼	Prénom	Identifiant	Propriétés	Actions
<input type="checkbox"/>	Administrator	System	fd-admin		
<input type="checkbox"/>	bilbo	thegrey	bilbo		
<input type="checkbox"/>	peter	antoine	user		

3

Utilisateurs

Base / Actions

	Nom de famille ▼	Prénom	Identifiant	courriel	Propriétés	Actions
<input type="checkbox"/>	Administrator	System	fd-admin			
<input type="checkbox"/>	bilbo	thegrey	bilbo			
<input type="checkbox"/>	peter	antoine	user	peter@acme.com		

3

Listes dynamiques

- Une configuration fine est possible

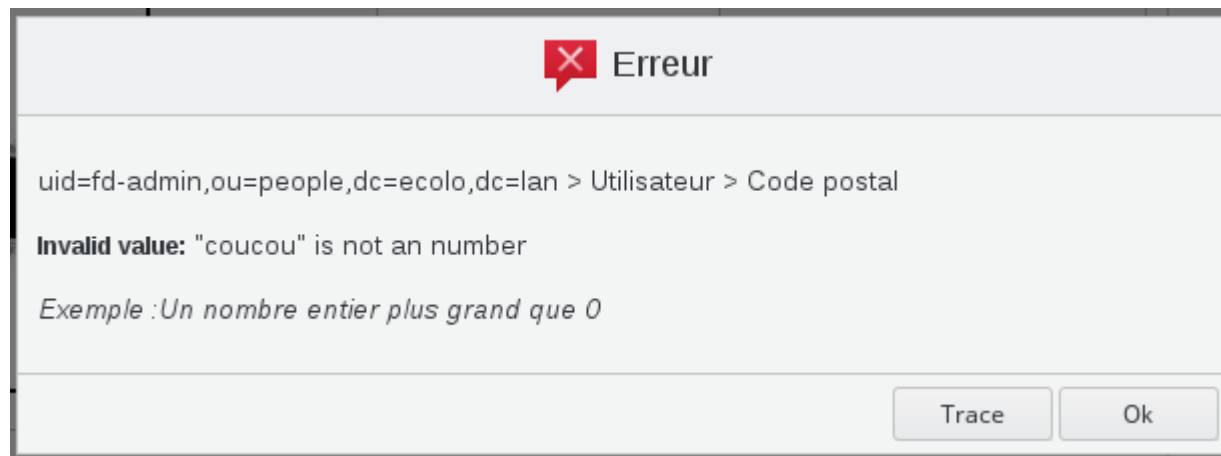
Configuration des listes

	ObjectTypeColumn		▼ ✎ 🗑️
	LinkColumn	sn	▲▼ ✎ 🗑️
	LinkColumn	givenName	▲▼ ✎ 🗑️
	Column	uid	▲▼ ✎ 🗑️
	LinkColumn	mail	▲▼ ✎ 🗑️
	PropertiesColumn		▲▼ ✎ 🗑️
	ActionsColumn		▲ ✎ 🗑️

Type* ▼
 Attribut
 Étiquette
 Ajouter
 Persistant
 Oublier ma configuration persistante

Nouvelle gestion des erreurs

- Message d'erreurs plus clairs
- Message unifié entre l'interface et le webservice
- Explique sur quel onglet et attribut l'erreur s'est produite





Nouveautés pour l'éducation

Supann 2018 révision 2

- Création d'un cadre de cohérence pour la mise en œuvre des annuaires dans l'enseignement supérieur et la recherche.
- Données administratives et techniques par rapport à un utilisateur.
- Ressources attribuables par utilisateur et permettent une gestion différenciée de chacune de ces ressources.
- Carte multi-service, une carte combinant badge d'accès physique, carte de cantine, carte de bibliothèque, le tout sur un même support.
- Consentement utilisateur vis a vis de ses données et services.

Structures






















- La représentation des structures et des établissements dans l'annuaire permet notamment (liste non limitative) :
 - d'obtenir les libellés des entités d'affectation et des établissements de rattachement des utilisateurs
 - de constituer un organigramme de l'établissement, grâce aux parentés entre structures (`supannCodeEntiteParent`), pour visualisation dans une application
 - de filtrer les accès à des ressources ou applications en fonction des affectations ou des rôles des utilisateurs.



Structures

Structures SupAnn



 Actions ▾

<input type="checkbox"/>		Nom ▾	supannCodeEntite	Parent	Description	Actions
<input type="checkbox"/>		DSI	54322	53056	Direction service informatique	     
<input type="checkbox"/>		nouvelle caledonie	53056		Université nouvelle caledonie	     
<input type="checkbox"/>		RH	54321	53056	service RH	     

 1
  2

Utilisateurs

- Les personnes sont l'objet des principaux usages de l'annuaire, dont notamment (liste non limitative) :
 - "Apprenant" : inscription à une formation dispensée par l'établissement,
 - "Personne ressource" : en sa qualité d'enseignant, chercheur, personnel technique, administratif ou d'encadrement, exerçant son activité dans l'établissement ou une de ses structures rattachées
 - "Externe" : du fait de toute relation, quelle qu'en soit la durée et le degré de formalisme, à partir du moment où son identité doit être connue de l'établissement

Utilisateurs

Utilisateur Unix Personnel Courriel **Groupes et rôles** Samba SSH Quota Ftp Freeradius Groupe NIS **SupAnn** Etat SupAnn Carte multi service Inscription Certificats Sous traitance **Sinaps** SpamAssassin **Sécurité** Politique de mot de passe Bulletin d'actualités Kerberos G

Ce compte a les paramètres SupAnn activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.
Retirer les paramètres SupAnn

Identité

Civilité

Alias de l'identifiant

Nom principal eduPerson

Surnom

Ids de références

Contact

Autres numéros de téléphone

Numéros de téléphone privés

GSM personnel

Autres adresses e-mail

Adresses e-mail personnelles

Adresses e-mail privées

Personnel

Adresses privées

Affectation

Affectation principale

Affectations

Types d'entité

Utilisateurs

Affiliation

Affiliation principale Personnel rémunéré (employee) ▼

Affiliations

Personnel rémunéré (employee)
 Personnel non pédagogique (staff)

Ancien étudiant gardant des relations avec l'établ... ▼
Ajouter
Supprimer

Établissement

nouvelle caledonie ({{UAI:9830445S}})

▼
Ajouter
Supprimer

Parrain

(Empty field)

Ajouter
Supprimer

Utilisateurs

Profil personnel

Identifiant personnel

Corps d'appartenance NCORPS ▾ AGENT DES SERV.TECH. RECH.ET FORMATION ▾

Activité

REFERENS ▾ ASS.D' ORIENTATION ET D'INSERTION PROF. ▾ Ajouter Supprimer

Rôles

SUPANN: ADJOINT AU CHARGE DU SERVICE	SUPANN: Pôle (Niveau 1)	DSI (Direction service informatique)	
--------------------------------------	-------------------------	--------------------------------------	--

Rôle générique ▾ Aucun ▾ Type d'entité SUPANN: Pôle (Niveau 1) ▾ Entité Aucun ▾ Ajouter

Consent

Consent	Picture	Authenticated		
	Email	Intern		
	Mobile	Resource people		

Picture ▾ APPRENANTS ▾ Ajouter

Cycle de vie

- La norme SupAnn 2018 permet de gérer le cycle de vie du compte
- Les ressources sont attribuables par utilisateur et permettent une gestion différenciée de chacune de ces ressources
- Par exemple verrouiller le compte utilisateur mais laisser le compte de messagerie opérationnel
- Cela permet aussi de faire de l'approvisionnement de compte, par exemple en vue de la rentrée scolaire sans activer les comptes immédiatement

Cycle de vie

Utilisateur | Unix | Personnel | Courriel | **Groupes et rôles** | Samba | SSH | Quota | Ftp | Freeradius | Groupe NIS | **SupAnn** | **Etat SupAnn** | Carte multi service | SpamAssassin | Certificats | Sous traitance | **Sinaps** | **Sécurité** | **Politique de mot de passe** | Bulletin

Ce compte a les paramètres État SupAnn activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres État SupAnn

Statut

Ressource	Statut	Sous-état	Début	Fin	
Courriel	Active	Aucune	2020-10-28	2021-03-08	 
Compte	Suspendu	Verrouillage administratif	2020-10-28	2020-11-05	 

Ressource*

Compte ▾

Statut*

Active ▾

Sous-état

Aucune ▾

Début

mm / dd / yyyy

Fin

mm / dd / yyyy

Ajouter

Carte Multi service



- La norme SupAnn 2018 permet de gérer les cartes multi-service
- On entend par carte multi-service, une carte combinant badge d'accès physique, carte de cantine, carte de bibliothèque, le tout sur un même support
- Le stockage de ces données dans la gestion des identités marque un tournant car jusqu'à présent seul le logiciel de création de carte possédait ces données
- Aujourd'hui elles peuvent être stockées au sein de la gestion des identités de manière centralisée au niveau de l'utilisateur, rendant la gestion des cartes beaucoup plus souple

Carte Multi service - définition de la carte

Utilisateur | Unix | Personnel | Courriel | Samba | Groupes et rôles | SSH | Quota | Ftp | Freeradius | Groupe NIS | SupAnn | État SupAnn | **Multiservice card** | Inscription | SpamAssassin | Certificats | Sous traitance | Sinaps | Sécurité

Ce compte a les paramètres Multiservice card activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres Multiservice card

Cards							
	Type	Format	Id	Valid	Source	Date de fin	
Cards	externe	Mifare XLSB	DEADBEEF000000	oui	unicampus@fusiondirectory.org		 

Type*

Format*

Id*

Valid*

Source

Date de fin

Ajouter

Carte Multi service - définition des services

Applications							
	Type	Source	Domaine	Id	Valid	Date de fin	
Applications	externe	unicampus@fusiondirectory.org	fusiondirectory.org	DEADBEEF1234	oui	2020-05-29	 

Type*







Source*

Domaine*

Id*

Consentement

- Le consentement sur l'utilisation des données des utilisateurs peut dès a présent être modélise dans supAnn 2018
- Ceci permet au applicatifs externe de demander quels données on le droit d'être consommés par type applicatifs

Consent			
Consent	Picture	Intern	 
	Email	EduGAIN	 
	Personal email	Resource people	 

Groupes

- La constitution de groupes de personnes revêt une importance fonctionnelle particulière pour des contrôles d'accès aux ressources
 - Création de liste de diffusion électroniques
 - Création de groupes pour les TP/TD/cours
 - Création de groupes à durée déterminée pour des projets
 - Désignation de superviseurs et d'administrateurs pour ces groupes

Groupes

Groupe d'objets
Courriel
Carte multi service
SupAnn
Partage
Références
LDAP

Ce compte a les paramètres SupAnn activés. Vous pouvez les désactiver en cliquant sur le bouton ci-dessous.

Retirer les paramètres SupAnn

Information

Date de fin	<input style="width: 100%;" type="text" value="04 / 22 / 2021"/>
Lecteurs	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 antoine peter </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 dufour paul </div> <div style="display: flex; justify-content: space-between; width: 100%;"> Ajouter Supprimer </div>
Administrateurs	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 dufour paul </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 </div> <div style="display: flex; justify-content: space-between; width: 100%;"> Ajouter Supprimer </div>
Ids de références	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> 👤 </div> <div style="display: flex; justify-content: space-between; width: 100%;"> Ajouter Supprimer </div>

Supann 2020

- Mise en place de la gestion des codes population
- Mise en place de l'identifiant opaque pour les fédérations



Systeme de workflow

Systeme de workflow

Il y a une demande croissante sur la possibilité d'agir de manière automatisée sur des événements en fonction des données présente dans la gestion des identités

- La désactivation automatique de certaines ressources en fonction de date de fin de validité
- L'approbation de compte créés automatiquement ou par une certaine catégorie de personnel
- De déclencher automatiquement les actions de gestion de compte (création, activation, désactivation, suppression, ...) en fonction de l'état de la ressource

Workflow : Création de tâches

- Création de taches génériques
- Création d'une tache mail associéé

Tasks
Tasks Mail
References
LDAP

Tasks Generic

Task Name*

Date

Time : :

Tasks
Tasks Mail
References
LDAP

This account has Tasks Mail settings enabled. You can disable them by clicking below.

[Remove Tasks Mail settings](#)

Task Mail Object	Sender Address
Mail Template <input type="text" value="Invitations 2022"/>	Sender email address* <input type="text" value="to.be@chang.ed"/>

Recipients Users and/or Groups

Members*

Workflow : Suivi des tâches

- Tableau de bord permettant de suivre l'ensemble des taches et sous taches ainsi que leur statuts actuels

Tasks

🔄 🔗 | Actions ▾

☐	Tasks ▾	Types	Schedule	Status	Creation Date	Actions
<input type="checkbox"/>	Feuille de comptes - Vacataires	Mail Object	2022-10-27 01:00:00	Created	2022-10-27 09:55:50am	
<input type="checkbox"/>	Invitations Campus 2022	Mail Object	2022-10-27 12:30:00	Created	2022-10-27 09:52:15am	
<input type="checkbox"/>	Invitations Campus 2023	Mail Object	2023-01-01 12:30:00	Created	2022-10-27 09:52:15am	
<input type="checkbox"/>	Invitations Campus 2024	Mail Object	2023-01-01 12:30:00	Created	2022-10-27 09:52:15am	
<input type="checkbox"/>	Renouvellement abannes	Mail Object	2022-10-27 01:00:00	Processed	2022-10-27 09:54:48am	
<input type="checkbox"/>	Vacances de Noel	Mail Object	2022-12-24 01:00:00	Processed	2022-10-27 09:55:10am	

Tasks 6

Filter

Types

 Tasks

Tabs

 Tasks Mail

Workflow : FusionDirectory Orchestrator

FusionDirectory Orchestrator fournit un webservice Web avec une API REST.

Il permet :

- Une gestion granulaire de certaines tâches spécialisées.
- Offre une vue simple sur l'état de chaque tâche.
- Actuellement uniquement des taches de type mail

Orchestrateur : exemple de fonctionnement

Dans cet exemple FusionDirectory orchestrator on va récupérer des tâches mail

- Obtenir le token d'accès

```
curl -X POST -H "Content-Type: application/json" https://orchestrator.fusiondirectory.org/orchestrator/api/login -d '{"username":"admin","password":"secret"}'
```

- Obtenir toute les taches mails

```
curl -X GET -H "Content-Type: application/json" -H "Authorization: Bearer {token}" https://orchestrator.fusiondirectory.org/orchestrator/api/tasks/mail
```

- Demander l'exécution des taches mails en attente

```
curl -X PATCH -H "Content-Type: application/json" -H "Authorization: Bearer {token}" https://orchestrator.fusiondirectory.org/orchestrator/api/tasks/mail
```

- Demander de rafraichir le token

```
curl -X POST -H "Content-Type: application/json" https://orchestrator.fusiondirectory.org/orchestrator/api/refresh -d '{"token":"refresh-token"}'
```



Support multi distribution

Réécriture des outils de FusionDirectory

- Les outils en ligne de commande de FusionDirectory était à l'origine écrit en perl
- La maintenance était difficile et les distribution de type RedHat on supprime de nombreuses librairies perl
- Les outils on donc été réécrit en php pour plus de facilité
- Les outils ont été séparés par types de fonctionnalités, on trouve désormais
 - fusiondirectory-configuration-manager
 - fusiondirectory-schema-manager
 - fusiondirectory-plugins-manager
 - fusiondirectory-migration-manager

Distribution certifiées

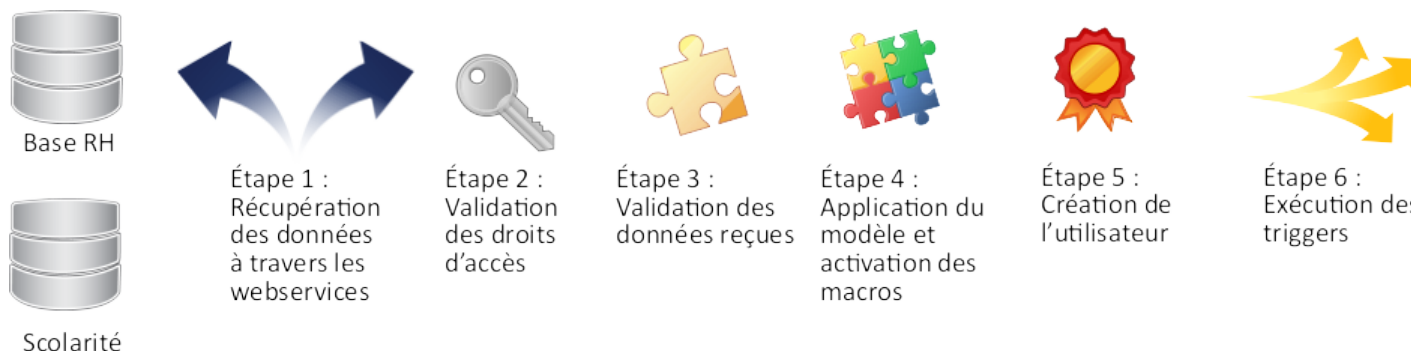
- Le fonctionnement de FusionDirectory est maintenant garanti sur un certain nombre de distributions Linux
- Le liste est disponible sur <https://www.fusiondirectory.org/distribution-certifiees/>



Webservices REST

Le webservice REST

- Le webservice REST permet l'intégration de la gestion des identités avec des applications tierces de manière plus fluide
- L'utilisation des modèles permet de construire des process de provisionnement qui valident les données
- Le déclenchement des triggers permet des actions supplémentaires



La spécification OpenAPI

- Le webservice REST propose un fichier au format OpenAPI qui liste les opérations disponibles
- Certains clients supportent directement ce format pour générer des requêtes
- La documentation officielle est générée depuis ce fichier et disponible sur <https://rest-api.fusiondirectory.info>
- Le fichier est disponible depuis votre installation, les champs sont dynamiquement adaptés pour refléter votre configuration :
<https://<hote>/fusiondirectory/rest.php/v1/openapi.json>

Exemples d'appels au webservice

GET /objects/user?base=ou=branche,dc=example,dc=com

→ { "uid=login,ou=people,dc=example,dc=com": "login" }

GET /objects/user/uid=login,ou=people,dc=example,dc=com/posixAccount/uidNumber

→ 1012

PUT /objects/user/uid=login,ou=people,dc=example,dc=com/posixAccount/uidNumber

1000

→ uid=login,ou=people,dc=example,dc=com

Exemples d'appels au webservice

GET /types/user/mailAccount

```
{ "sections": {  
  "main": {  
    "name": "Mail account",  
    "attrs": [  
      "mail",  
      "gosaMailServer",  
      "gosaMailQuota"  
    ]  
  },  
  ...  
}
```


















Sécurité

Renforcement de la sécurité

- L'audit permet la recherche d'événements par date et catégorie
- Un second facteur sous forme de TOTP ou de clefs yubiko est disponible
- Un onglet sécurité est disponible dans la fiche de l'utilisateur et recense tout les opérations de sécurité sur son compte

Renforcement de la sécurité

2020-08-06, 09:41:25	passwordRecovery	195.154.20.154	modify	plugin/mailAccount	uid=droide,ou=people,ou=community,dc=fusiondirectory,dc=org
2020-08-06, 09:41:25	passwordRecovery	195.154.20.154	modify	plugin/user	uid=droide,ou=people,ou=community,dc=fusiondirectory,dc=org
2020-08-06, 09:38:01	uid=bmortier,ou=people,ou=company,dc=fusiondirectory,dc=org	195.154.20.154	create	plugin/userRoles	uid=droide,ou=people,ou=community,dc=fusiondirectory,dc=org
2020-08-06, 09:38:01	uid=bmortier,ou=people,ou=company,dc=fusiondirectory,dc=org	195.154.20.154	create	plugin/mailAccount	uid=droide,ou=people,ou=community,dc=fusiondirectory,dc=org
2020-08-06, 09:38:01	uid=bmortier,ou=people,ou=company,dc=fusiondirectory,dc=org	195.154.20.154	remove	plugin/personalInfo	uid=droide,ou=people,ou=community,dc=fusiondirectory,dc=org
2020-08-06, 09:23:13	uid=bmortier,ou=people,ou=company,dc=fusiondirectory,dc=org	195.154.20.154	security	login	bmortier
2020-08-06, 09:07:24	uid=bmortier,ou=people,ou=company,dc=fusiondir				
2020-08-06, 09:07:10	uid=bmortier,ou=people,ou=company,dc=fusiondir				
2020-08-06, 09:07:10	uid=bmortier,ou=people,ou=company,dc=fusiondir				

Security audit				
Event	Author	Origin	Time	Result
Sign out	 antoine peter	10.185.64.1	1 hour(s) ago	Logged out (Session expired)
Sign in	 antoine peter	10.185.64.1	1 hour(s) ago	Logged in successfully
Sign out	 antoine peter	10.185.64.1	1 hour(s) ago	Logged out (Sign out)
Sign in	 antoine peter	10.185.64.1	1 hour(s) ago	Logged in successfully
Sign out	 antoine peter	10.185.64.1	1 hour(s) ago	Logged out (Sign out)
Sign in	 antoine peter	10.185.64.1	1 hour(s) ago	Logged in successfully
Sign out	 antoine peter	10.185.64.1	1 hour(s) ago	Logged out (Sign out)
Sign in	 antoine peter	10.185.64.1	1 hour(s) ago	Logged in successfully
Sign out	 antoine peter	10.185.64.1	1 hour(s) ago	Logged out (Sign out)
Sign in	 antoine peter	10.185.64.1	1 hour(s) ago	Logged in successfully
Password modification	 System Administrator	10.185.64.1	1 hour(s) ago	Success
Sign out	 antoine peter	10.185.64.1	1 month(s) ago	Logged out (Sign out)
Sign in	 antoine peter	10.185.64.1	1 month(s) ago	Logged in successfully
Password modification	 System Administrator	10.185.64.1	1 month(s) ago	Success
Sign out	 antoine peter	192.168.56.1	2 month(s) ago	Logged out (Sign out)



De nouveaux outils pour les développeurs

FusionDirectory Integrator

- Lors de la réécriture de nos outils en php l'on a remarqué un manque au niveau des librairies
- On a donc créé un framework FusionDirectory Integrator qui est un toolkit de fonction pour créer des outils
- Les deux premiers modules sont LDAP et CLI sont dès à présent utilisés par nos outils
- Ces librairies vont être amenées à évoluer au cours des prochains mois

Orchestrateur : FusionDirectory Orchestrator

FusionDirectory Orchestrator fournit un webservice Web avec une API REST.

Il permet :

- Une gestion granulaire de certaines tâches spécialisées.
- Offre une vue simple sur l'état de chaque tâche.
- Actuellement uniquement des taches de type mail

Orchestrateur : exemple de fonctionnement

Dans cet exemple FusionDirectory orchestrator on va récupérer des tâches mail

- Obtenir le token d'accès

```
curl -X POST -H "Content-Type: application/json" https://orchestrator.fusiondirectory.org/orchestrator/api/login -d '{"username":"admin","password":"secret"}'
```

- Obtenir toute les taches mails

```
curl -X GET -H "Content-Type: application/json" -H "Authorization: Bearer {token}" https://orchestrator.fusiondirectory.org/orchestrator/api/tasks/mail
```

- Demander l'exécution des taches mails en attente

```
curl -X PATCH -H "Content-Type: application/json" -H "Authorization: Bearer {token}" https://orchestrator.fusiondirectory.org/orchestrator/api/tasks/mail
```

- Demander de rafraichir le token

```
curl -X POST -H "Content-Type: application/json" https://orchestrator.fusiondirectory.org/orchestrator/api/refresh -d '{"token":"refresh-token"}'
```

Références

- FusionDirectory : <https://www.fusiondirectory.org/>
- Documentation : <https://fusiondirectory-user-manual.readthedocs.io/en/1.4/index.html>
- Documentation développeurs :
<https://fusiondirectory-developer-documentation.readthedocs.io/en/1.4/index.html>
- Forge logicielle : <https://gitlab.fusiondirectory.org/>