

Guide d'utilisation du Portail IAM

Le présent guide s'adresse aux personnes se connectant au Portail IAM, et vous guide dans les opérations suivantes :

- Accéder au Portail IAM.
- Vous authentifier.
- Accéder à vos applications.
- Editer votre profil.
- Gérer une application mobile et l'authentification forte.

Il présente également des évolutions liées à la dernière version du portail IAM.

Evolutions du Portail

Le portail IAM adopte la charte graphique de l'État de Vaud.

Cela lui permet en particulier de s'adapter aux supports mobiles comme les tablettes ou les smartphones.

Le portail IAM met à disposition de ses usagers l'authentification par certificat : SG-PKI* depuis le réseau intranet de l'administration.

* *Swiss Government Public Key Infrastructure*, en français : infrastructure à clé publique de l'administration fédérale suisse.

Signaler un incident – demander du support – contacter le Helpdesk

Vous pouvez signaler un incident ou demander des explications complémentaires au Helpdesk :

- Par téléphone au 021 316 26 60.
- Par e-mail à l'adresse helpdesk@vd.ch

Cependant, avant d'appeler le Helpdesk, les opérations suivantes peuvent éventuellement solutionner un problème :

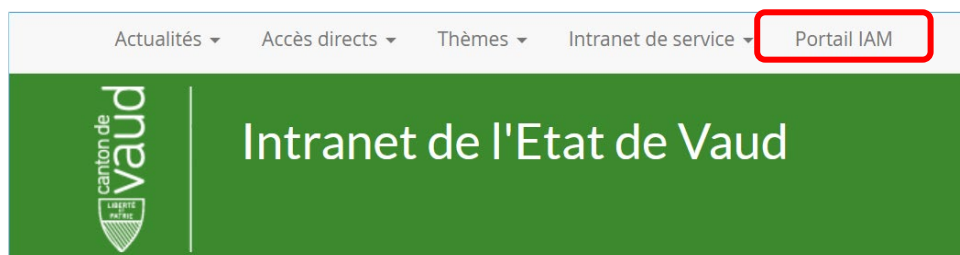
- Utiliser un autre navigateur.
- Supprimer les cookies.
- Effacer l'historique de navigation.
- Essayer avec la navigation en mode privé.

Accéder au Portail IAM

Accéder au Portail IAM depuis l'Intranet

Une personne peut accéder au portail IAM depuis l'Intranet par 3 canaux principaux :

1. Avec le raccourci vers le portail IAM disponible sur le bureau : 
2. Avec l'adresse Web suivant : <https://portail.etat-de-vaud.ch>. 
3. Avec le lien direct disponible dans le menu du site intranet de l'Etat de Vaud, cliquez sur le lien Portail IAM.



À la suite de la mise en œuvre du *Desktop SSO*, l'utilisateur n'a plus à saisir son identifiant ou son mot de passe pour lancer le portail IAM Intranet ou toute application disponible sur le portail IAM Intranet en authentification simple.

Pour plus de détails concernant l'authentification forte, veuillez-vous référer à la rubrique Authentification forte, plus loin dans ce document.

Accéder au Portail IAM depuis Internet

L'accès au portail IAM depuis Internet s'effectue en 4 étapes :



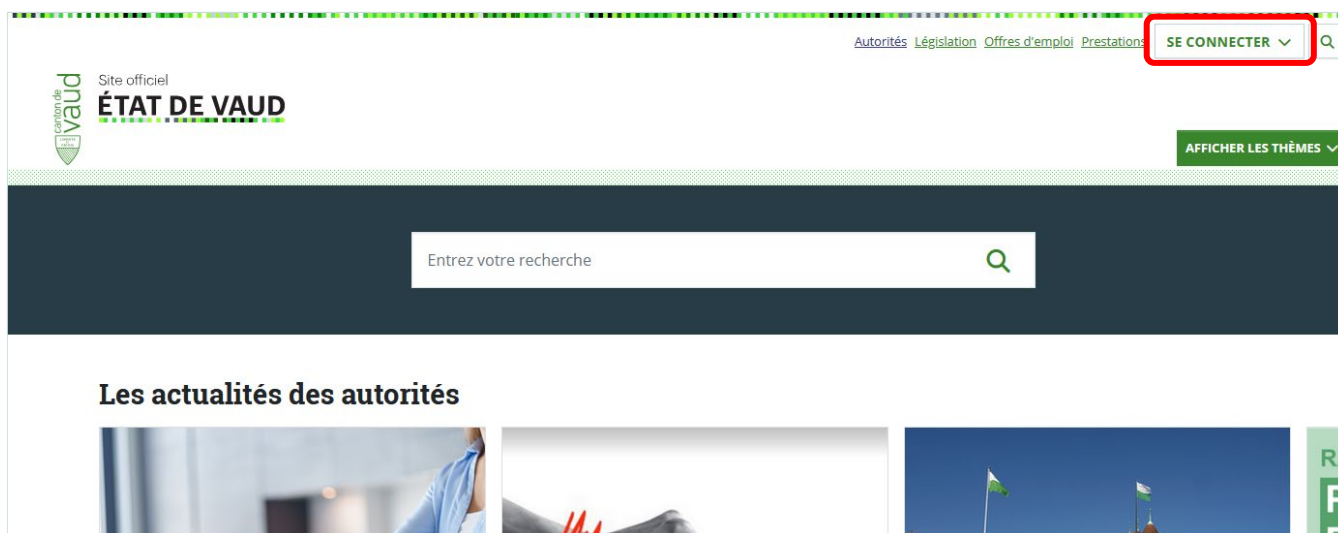
Etape 1 – Connexion à www.vd.ch

Le site officiel du Canton de Vaud est disponible à l'adresse suivante : <http://www.vd.ch>.

En utilisant cette URL dans votre navigateur, vous accéderez au portail de l'État de Vaud.

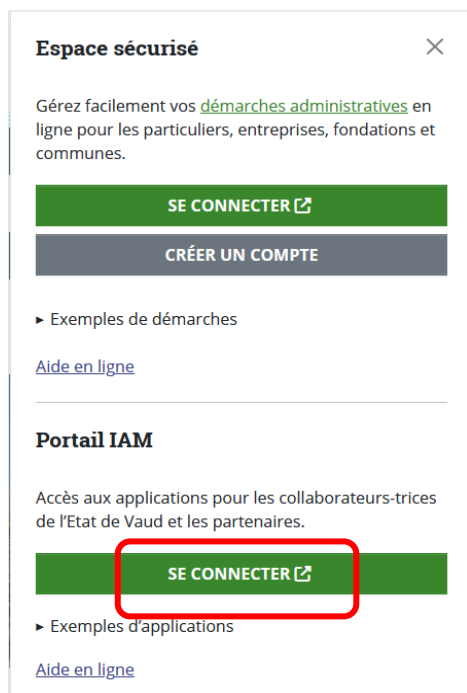
Etape 2 – Cliquer sur « SE CONNECTER »

Cliquez sur le bouton « **SE CONNECTER** » encadré en rouge ci-dessous.



Etape 3 – Connexion au Portail sécurisé IAM

Dans le menu, sélectionner « **SE CONNECTER** » dans la partie Portail IAM.



Etape 4.1 – Authentification simple

La plupart des applications mises à disposition par l'Etat de Vaud via le portail IAM sont disponibles à travers une authentification simple.

L'authentification simple est basée sur le couple « identifiant / mot de passe » et ne requiert aucun autre moyen.

Vous devez d'abord saisir votre identifiant, puis votre mot de passe :

Une fois ces champs remplis, cliquez sur le bouton « **ENVOYER** ».

- Si votre saisie est validée, vous serez redirigé vers le portail IAM et la liste des applications auxquelles vous avez accès vous sera affichée.
- Si votre identifiant ou votre mot de passe sont erronés : le système affiche un message d'erreur et vous disposez de 2 tentatives supplémentaires pour vous connecter. En cas d'échecs répétés, votre compte est bloqué.

Pour le personnel de la DGEO ou de la DGEP (uniquement les gymnases ou écoles professionnelles en pilote spécifiés), en accédant au portail IAM depuis le réseau internet, cliquez sur le bouton correspondant afin d'accéder aux moyens d'authentification spécifiques à chacun de ces départements.

Etape 4.2 – Authentification forte

L'authentification forte est basée sur le couple « identifiant / mot de passe », et requiert **en plus** un second moyen d'authentification parmi la liste ci-dessous :

- Application mobile.
- Une carte OTP (*One Time Passcode*).
- Un certificat SG-PKI (réseau intranet uniquement).

Authentification

Authentification forte par application mobile

L'authentification forte par application mobile nécessite :

- Que vous disposiez d'un téléphone portable sur lequel l'application mobile soit installée.
- Que le portail IAM soit enregistré dans l'application mobile (voir la rubrique **Gestion de l'application mobile**, plus loin dans ce document).

Après avoir validé votre identifiant et votre mot de passe, le système vous demande d'entrer le code à usage unique fourni dans l'application mobile.

ÉTAT DE VAUD // IAM

Accès Internet sécurisé

Veuillez saisir le code affiché par votre application mobile

Code OTP :

ENVOYER

☐ Je souhaite sauter cette étape pour mes futures connexions à partir de cet appareil.

[Je souhaite changer de moyen d'authentification forte](#)

Après avoir saisi votre code OTP, cliquez sur le bouton « **ENVOYER** ». Vous êtes alors authentifié, et redirigé vers la page d'accueil de l'application demandée.

En cochant la case « **Je souhaite sauter cette étape pour mes futures connexions à partir de cet appareil** », vous pouvez éviter de devoir récupérer systématiquement un code sur l'application mobile pendant 3 mois.

Authentification forte par carte OTP

L'authentification forte par carte OTP (*One Time Passcode*) nécessite :

- Que vous disposiez au préalable d'une carte OTP fournie par la DGNSI.
- Que la carte OTP soit configurée dans votre profil IAM (voir la rubrique **Gestion de la carte OTP**, plus loin dans ce document).

Après avoir validé votre identifiant et votre mot de passe, le système vous demande d'entrer le code à usage unique affiché sur la carte.

ÉTAT DE VAUD // IAM

Accès Internet sécurisé

Veuillez saisir le code affiché par votre application mobile

Code OTP :

Code OTP

ENVOYER

☐ Je souhaite sauter cette étape pour mes futures connexions à partir de cet appareil.

[Je souhaite changer de moyen d'authentification forte](#)

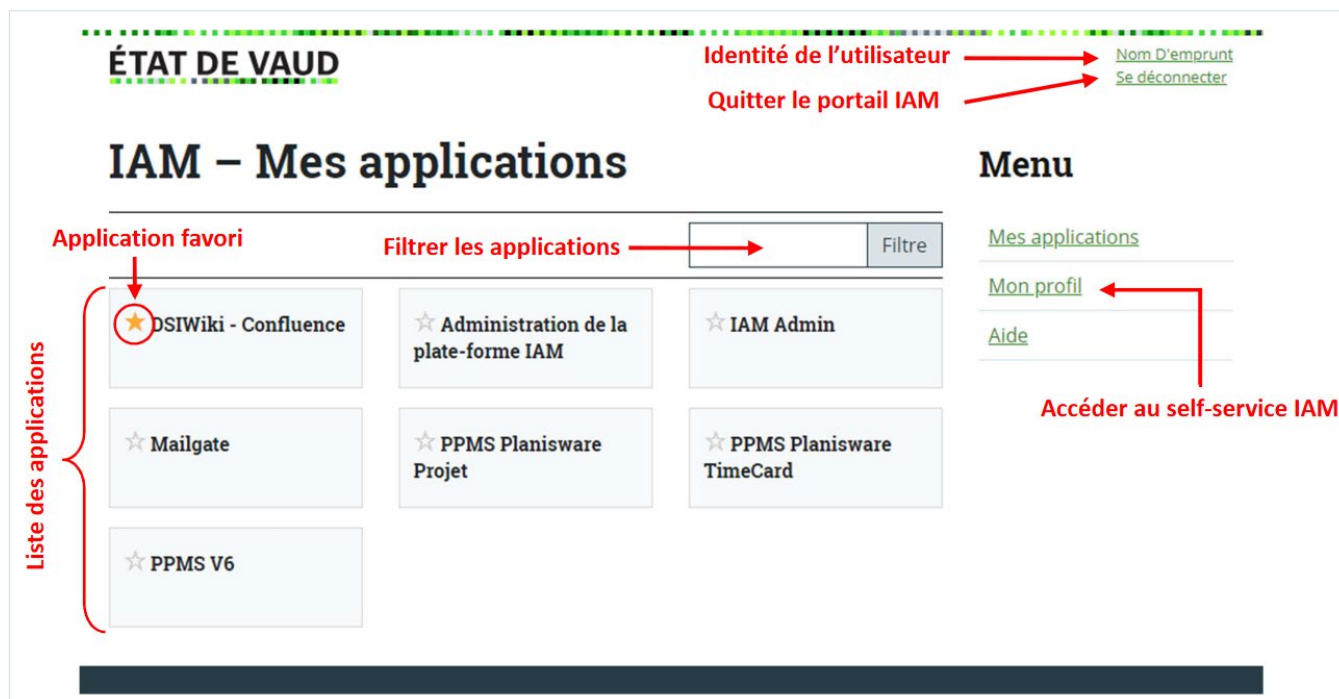
Après avoir saisi votre code OTP, cliquez sur le bouton « **ENVOYER** ». Vous êtes alors authentifié, et redirigé vers la page d'accueil de l'application demandée.

En cochant la case « **Je souhaite sauter cette étape pour mes futures connexions à partir de cet appareil** », vous pouvez éviter de devoir récupérer systématiquement un code sur la carte OTP pendant 3 mois.

Utilisation du Portail IAM

Accès aux applications

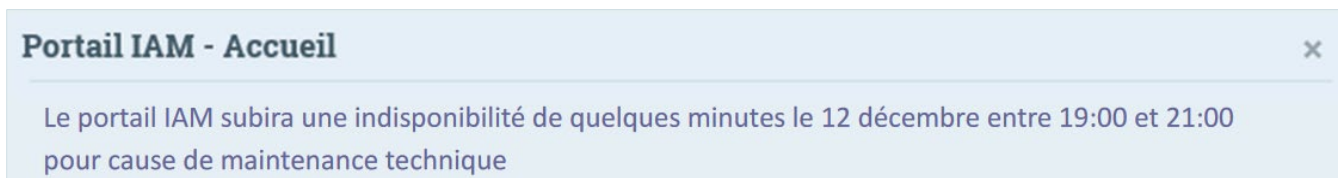
Une fois authentifié, le système vous affiche la page d'accueil du Portail IAM, illustrée ci-dessous :



- Pour **accéder à une application** présente dans la liste (« Mes applications »), vous pouvez cliquer sur le titre de l'application. Dans ce cas, l'application s'affichera dans l'onglet courant du navigateur. En d'autres termes, la page du Portail IAM disparaît au profit de l'application ciblée.
- Pour définir un **favori**, activez l'étoile de l'application s'y rapportant en cliquant dessus. Cette application sera ensuite affichée en premier dans la liste et non plus selon son ordre alphabétique.
- Le **filtre** permet aux utilisateurs de retrouver rapidement une application en saisissant simplement les lettres de son nom ou de sa dénomination technique.
- Pour accéder aux fonctionnalités de gestion de votre compte, cliquez sur « **Mon profil** ».
- Pour **quitter le Portail** et clore votre session IAM, veuillez utiliser le lien « **Se déconnecter** ».

Messages d'information par application

Le Portail IAM vous informe des événements de maintenance prévus sur les applications pour lesquelles vous disposez de droits d'accès en affichant un message sur fond bleu, tel l'illustration suivante :



Ces messages sont, en général, affichés plusieurs jours avant l'intervention sur les applications. Ainsi, les utilisateurs du Portail IAM peuvent prendre note de l'indisponibilité de l'application et s'organiser en conséquence.

Mon profil

Le lien « **Mon profil** », dans le menu du Portail IAM, vous permet de gérer les paramètres de votre compte.

Cette fonction vous permet par exemple de déclarer un nouveau moyen d'authentification, tel que l'authentification forte, et de configurer à cette occasion une application mobile ou une carte OTP.

Accès à la page d'édition de Mon profil

Vous devez au préalable vous être authentifié et vous trouver sur la page d'accueil du portail IAM.

Une fois authentifié, vous pouvez cliquer sur « **Mon profil** » dans le menu à droite du portail IAM.

En cliquant sur le lien, le système vous affiche la page ci-dessous, correspondant par défaut au menu « **Mon profil** ».

Le menu « **Mon profil** » vous permet de consulter les informations générales d'identité associées à votre compte :

- **Vos informations personnelles**
Vous pouvez visualiser et modifier vos informations personnelles.
- **Vos authentifications fortes**
Vous pouvez ajouter ou supprimer les méthodes d'authentification forte parmi celles qui vous sont attribuées ou bien modifier vos données.
- **Gérer les urgences**
Vous pouvez traiter les cas de perte de vos moyens d'authentification forte.

Informations personnelles

Vous pouvez directement modifier les attributs erronés en cliquant sur le bouton « **Modifier** ».

Vous pouvez également modifier votre mot de passe (pour les utilisateurs du portail intranet, le mot de passe Windows sera également modifié).

Si une erreur est présente pour un attribut que vous n'avez pas le droit de modifier, veuillez contacter le Helpdesk (helpdesk@vd.ch).

Authentification forte

Le menu « **Authentification forte** » vous permet de gérer vos différents moyens d'authentification forte.

- Les paramètres liés à l'utilisation de l'application mobile.
- Les paramètres liés à l'utilisation d'une carte OTP.

Urgences

Plusieurs alternatives sont mises à votre disposition pour traiter une perte de vos moyens d'authentification forte.

Gestion de l'authentification forte

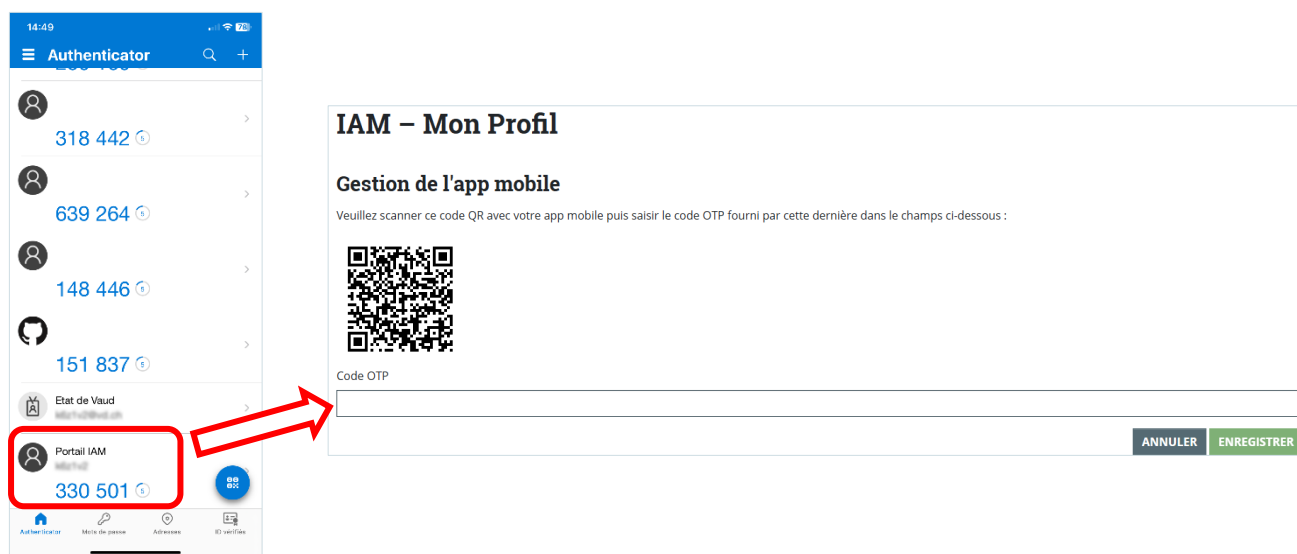
Gestion de l'application mobile

Prérequis

Il faut au préalable avoir installé une application mobile permettant de faire l'authentification forte (voir la rubrique : Installation de l'application mobile, plus loin dans ce document).

Pour configurer la distribution de code à usage unique à travers une application mobile :

1. Dans le Portail IAM : il faut aller dans le menu « **Mon Profil** » de la page d'accueil du portail IAM (voir la rubrique **Mon profil**, plus haut dans ce document).
2. Ensuite il faut aller dans le menu « **Authentification forte** ».
3. Dans la rubrique **Gestion de l'app mobile**, il faut cliquer sur le bouton « **CONFIGURER** ».
4. Sur le téléphone mobile : il faut aller dans l'application d'authentification mobile de votre choix (p.ex. : *Microsoft Authenticator*, *Google Authenticator*) et scanner le QR code présent à l'écran pour ajouter le MFA* IAM.
5. Une fois que le compte du portail IAM est ajouté à l'application mobile, il faut entrer le code à usage unique dans le champ dédié du portail IAM, comme indiqué ci-dessous :



6. Finalement, cliquer sur le bouton « **ENREGISTRER** » pour finaliser l'enregistrement du double facteur via l'application mobile.

* *Multi-Factor Authentication*, ou authentification multifacteur. Il s'agit d'une méthode de sécurité qui demande de fournir au moins deux preuves d'identité différentes pour accéder à un compte ou à une application.

Gestion de la carte OTP

La carte OTP est une alternative pour les usagers qui sont dans l'impossibilité d'utiliser l'authentification par application mobile (*téléphone non compatible, pas de téléphone mobile, etc.*).



Pour configurer une carte OTP dans son profil IAM :

1. Il faut aller dans le menu « **Authentification forte** » depuis le menu « **Mon Profil** » de la page d'accueil du portail IAM (voir la rubrique **Mon profil**, plus haut dans ce document).
2. Dans la partie **Gestion de la carte OTP**, cliquez sur le bouton « **AJOUTER UNE CARTE OTP** ».
3. Saisissez le numéro de série de votre carte OTP (que vous pouvez voir au dos de votre carte) dans le champ prévu à cet effet :

Gestion de la carte OTP

Numéro de série de votre carte : non renseigné

Veuillez saisir le numéro de série de la carte OTP (visible au dos de la carte)

012332321123

Code OTP

ANNULER ENREGISTRER

4. Cliquez sur le bouton qui se trouve sur la face avant de la carte OTP, afin d'afficher le code à usage unique et saisissez-le dans le champ prévu à cet effet :

Gestion de la carte OTP

Numéro de série de votre carte : non renseigné

Veuillez saisir le numéro de série de la carte OTP (visible au dos de la carte)

012332321123

Code OTP

ANNULER ENREGISTRER

5. Cliquez sur le bouton « **ENREGISTRER** » pour finaliser l'enregistrement de l'authentification à double facteur via la carte OTP.

Installation de l'application mobile

Pour installer une application mobile permettant de faire de l'authentification forte, veuillez :

1. Aller sur votre téléphone mobile et suivre le lien <https://aka.ms/mobileauthenticator> ou scanner le code QR suivant avec votre téléphone mobile.



2. Une fois sur le site, scannez le code QR pour aller dans le magasin (store) applicatif correspondant au système de votre téléphone mobile.
3. Télécharger l'application proposée (*Microsoft Authenticator*).
4. Ouvrez l'application et configurez-la comme indiqué dans la rubrique **Gestion de l'application mobile**, plus haut dans ce document.

Aide et conseil

Vous pouvez signaler un incident ou demander des explications complémentaires au helpdesk. Cependant, avant d'appeler, les opérations suivantes peuvent éventuellement solutionner un problème :

- Utilisez un autre navigateur.
- Supprimez les cookies.
- Effacez l'historique de navigation.
- Essayez avec la navigation en mode privé.

Le helpdesk informatique est à votre disposition pour toute demande d'assistance technique ou toute question concernant les fonctionnalités de votre poste de travail.

Helpdesk Informatique – helpdesk@vd.ch – tél. : 021 316 26 60

Département de l'agriculture, de la durabilité, du climat et du numérique
Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
vd.ch/dgnsi

VD.CH

Direction générale certifiée ISO 9001, 27001 et labellisée Numérique Responsable niveau 2