



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral des routes OFROU

DOCUMENTATION

IAM BSA

Guide de l'utilisateur

Édition 2025 V1.00

ASTRA 83057

Impressum

Auteurs / groupe de travail

Geringer Jolanda	OFROU DS-DTI, présidence
Gähwiler Daniel	CSI Consulting AG
Grau Rolf	CSI Consulting AG

Groupe de suivi (révision)

Crausaz Bernard	OFROU DS-UARS
Jehli Martin	UT V
Widrig Bruno	UT XI
Schlup Markus	Amstein + Walthert Progress AG

Traduction

CSI Consulting AG, la version originale en allemand fait foi.

Éditeur

Office fédéral des routes OFROU
Division Réseaux routiers N
Standards et sécurité de l'infrastructure SSI
3003 Berne

Diffusion

Le document est téléchargeable gratuitement sur le site www.ofrou.admin.ch.

© OFROU 2025

Reproduction à usage non commercial autorisée avec indication de la source.

Table des matières

Impressum	2
1 Introduction	5
1.1 Objectif	5
1.2 Champ d'application et documents de base	5
1.3 Destinataires	5
1.4 Entrée en vigueur et modifications.....	5
2 Aperçu	6
3 Configurer et gérer un compte IAM BSA	7
3.1 Demande de l'accès initial	7
3.2 Configuration de l'authentification multifactorielle (MFA).....	8
3.2.1 Token matériel MFA.....	8
3.3 Demander des rôles	8
3.4 Autres unités territoriales	8
3.5 Mot de passe oublié	9
3.6 Oubli du code PIN du token MFA.....	9
3.7 Token MFA perdu / défectueux / nouveau matériel.....	9
3.8 Contact Service Desk.....	9
4 Accès à distance aux services du réseau IP EES via IAM BSA	10
4.1 Accès via VPN.....	10
5 Questions fréquentes - FAQ	15
Glossaire	17
Bibliographie	18
Liste des modifications	19

1 Introduction

1.1 Objectif

La gestion des identités IAM BSA a pour but la saisie et le traitement uniformes des comptes d'accès au système au sein du réseau IP EES.

Ce document sert de bref aperçu et de guide pour les nouveaux utilisateurs qui souhaitent faire une demande :

- Demande d'identité par les utilisateurs ;
- Examen et validation des demandes par les organisations compétentes ;
- Gestion centralisée des autorisations d'accès et des identités tout au long du cycle de vie des identités avec une convention de nommage et des règles uniformes ;
- Gestion inter-unités territoriales et contrôle d'urgence des identités ;
- Contrôle périodique des accès.

1.2 Champ d'application et documents de base

La présente documentation est un document complémentaire à la directive OFROU 73006 OT Security Governance [1], aux directives 13040 réseau IP EES [2] et 13030 OT Security [3], et a le même champ d'application.

1.3 Destinataires

Le document s'adresse aux parties prenantes suivantes :

- Spécialistes EES et exploitation de l'OFROU ;
- Spécialistes EES et exploitation des unités territoriales ;
- Fournisseurs pour le compte de l'OFROU.

1.4 Entrée en vigueur et modifications

Ce document entre en vigueur le 19.06.2025. La « liste des modifications » est documentée à la page 19.

2 Aperçu

Les identités pour l'utilisation de l'infrastructure critique exploitée sur le réseau IP EES sont créées et gérées de manière uniforme par des services centraux. Une fois saisie, l'identité peut être attribuée aux différentes unités territoriales en fonction des besoins et reçoit les droits nécessaires sur la base du rôle sélectionné. Les droits et les rôles sont créés et attribués par les administrateurs des unités territoriales concernées.

La gestion centralisée permet, selon la situation, de modifier les identités de manière centralisée ou, le cas échéant, de les bloquer.

Pour sécuriser les accès, une authentification multifactorielle (MFA) est également utilisée et attribuée à chaque utilisateur sous la forme d'un token. Pour l'utilisation du token, le logiciel MobilePASS+ est installé sur un équipement de l'utilisateur. Selon l'application, le token est demandé en plus du nom d'utilisateur et du mot de passe.

L'accès proprement dit aux systèmes cibles respectifs est communiqué à l'utilisateur par la personne de contact respective et ne fait pas partie de la présente documentation.

3 Configurer et gérer un compte IAM BSA

3.1 Demande de l'accès initial

Pour la première demande d'identité, l'utilisateur est invité par la personne de contact de l'OFROU ou des unités territoriales (UT) concernées à s'enregistrer via le portail.

<https://portal.nationalstrassen.admin.ch/>

Les informations suivantes sont nécessaires pour la demande :

- Prénom et nom de la personne qui fait la demande
(nom complet tel qu'indiqué sur la pièce d'identité officielle)
- Nom de l'entreprise de l'employeur
(nom complet de l'entreprise tel qu'indiqué dans le registre du commerce)
- Adresse professionnelle
(pour vérifier l'identité)
- Numéro de téléphone (mobile)
(pour une vérification alternative de l'identité par SMS)
- Date de naissance
(comme indiqué sur la pièce d'identité officielle)
- Langue de communication préférée
- Copie d'une pièce d'identité officielle
(passeport ou carte d'identité ; pour les cartes d'identité, le recto suffit ; non pixellisé et non noirci ; noir et blanc ou couleur ; au format JPG, ou PNG, taille du fichier max. 4MB)
- Zone d'exploitation
(zone d'exploitation initiale selon les instructions de la personne de contact si d'autres unités territoriales doivent être desservies, elles seront sélectionnées ultérieurement dans le système).
- Type d'employé
(externes, collaborateurs de l'unité territoriale ou collaborateurs fédéraux).
- Adresse e-mail de la personne de contact
(personne de contact OFROU / UT qui vous a demandé de vous enregistrer).

Les données du formulaire sont vérifiées dans un certain délai par la zone d'exploitation concerné et approuvées ou refusées en conséquence.

En cas de refus, le demandeur n'est pas automatiquement informé.

Au cours de l'autorisation, le demandeur reçoit successivement par e-mail son nom d'utilisateur, son mot de passe initial, l'invitation à activer l'authentification multifactorielle (voir chap. 3.2) ainsi que d'autres informations.

3.2 Configuration de l'authentification multifactorielle (MFA)

Pour l'authentification multifactorielle (MFA), l'application / le logiciel MobilePASS+ de Thales doit être installé sur un appareil du demandeur afin de générer les codes numériques nécessaires à l'authentification multifactorielle.

Le logiciel Thales SafeNet MobilePASS+ est disponible pour diverses plates-formes et doit être installé au préalable.

SafeNet MobilePASS+ peut être obtenu dans les AppStores respectifs ou directement auprès du fabricant :

<https://cpl.thalesgroup.com/access-management/authenticators/mobilepass-otp-download>

Une fois l'installation réussie de SafeNet MobilePASS+ sur l'appareil du demandeur, le token logiciel peut être activé dans l'application SafeNet MobilePASS+ à l'aide de l'e-mail d'enregistrement d'IAM BSA. Pour ce faire, sélectionnez l'option « Pas de code QR ? » en bas de l'écran lorsque vous êtes invité à scanner un code QR.

Pour sécuriser le token logiciel, l'utilisateur doit définir un PIN séparé qui protège le token logiciel. Cela fait partie du processus d'activation.

Ensuite, l'utilisateur peut accéder aux services du réseau IP EES (voir chap. 4).

3.2.1 Token matériel MFA

Si la politique de l'entreprise du demandeur interdit l'installation de SafeNet MobilePASS+ sur un appareil du demandeur ou pour tous les utilisateurs qui attribuent des droits et des utilisateurs admin, un token matériel peut également être demandé dans des cas exceptionnels.

La commande d'un token matériel se fait par l'intermédiaire du service desk (voir contact Service Desk au chap. 3.8).

3.3 Demander des rôles

Au sein du système IAM BSA OFROU, un utilisateur peut demander d'autres rôles. Pour cela, l'utilisateur doit déjà être connecté au réseau IP EES (voir chap. 4).

La demande se fait via l'interface web de l'application IAM BSA au sein du réseau IP EES :

<https://sailpoint.bd.nationalstrassen.admin.ch/>

L'utilisateur commande les accès dont il a besoin via le menu « Manage Access / Manage My Access » sur la base des noms de groupe qu'il connaît. Ceux-ci sont accordés ou refusés selon le processus d'autorisation par l'unité administrative compétente.

Si les noms des groupes ne sont pas connus, l'utilisateur doit les demander à sa personne de contact.

3.4 Autres unités territoriales

Les utilisateurs existants peuvent être enregistrés pour d'autres unités territoriales par leur contact ou leur administrateur d'unité territoriale au sein du système IAM BSA. La communication à ce sujet se fait en dehors du système, dans le cadre de l'attribution et de la discussion avec la personne de contact de l'UT.

Attention : en raison des exigences d'autonomie et de la gestion des identités et des autorisations liées à l'UT, l'utilisateur est automatiquement invité à définir un nouveau mot de

se passe lorsqu'il est ajouté à une nouvelle unité territoriale (comme lors de l'enregistrement initial). Ce mot de passe est ensuite communiqué à toutes les zones d'exploitation, de sorte que le nouveau mot de passe peut être utilisé dans toutes les unités. Si l'utilisateur est connecté pendant le changement automatique de mot de passe, il peut continuer à travailler pendant environ une heure avant d'être bloqué en raison du changement.

3.5 Mot de passe oublié

Si le mot de passe n'est plus connu, une réinitialisation du mot de passe peut être initiée via le portail :

<https://portal.nationalstrassen.admin.ch/>

L'identité du demandeur est confirmée via un lien de sécurité dans l'e-mail et un mot de passe temporaire est délivré. Celui-ci doit être modifié par l'utilisateur lors de la prochaine connexion après une authentification réussie au moyen d'un softtoken MFA (ou, dans des cas exceptionnels, d'un token matériel).

Sans token MFA, la réinitialisation du mot de passe doit être demandée via le Service Desk (contact voir chap. 3.8).

3.6 Oubli du code PIN du token MFA

Si le code PIN du token MFA a été oublié, il faut contacter le service desk (contact voir chap. 3.8).

3.7 Token MFA perdu / défectueux / nouveau matériel

Si le token MFA a été perdu, le Service Desk (contact voir chap. 3.8) doit être informé immédiatement afin que le token puisse être bloqué.

Si le token est défectueux (par exemple, il n'affiche pas le code du token), il faut également contacter le service desk pour analyser l'erreur et éventuellement se faire attribuer un token de remplacement.

Le transfert d'un soft token vers un nouveau matériel (ordinateur portable ou mobile) se fait également à l'aide du service desk.

3.8 Contact Service Desk

Le Service Desk responsable de l'IAM BSA OFROU peut être contacté comme suit :

Courrier électronique : noc@axpo-systems.com

Tél. : 0800 99 74 38

4 Accès à distance aux services du réseau IP EES via IAM BSA

4.1 Accès via VPN

Pour accès à distance aux services du réseau IP EES il est possible d'accéder depuis Internet aux jumpstations des sites BD via [Checkpoint Mobile Agent](#), en passant par les sites de services de base BD-A et BD-B

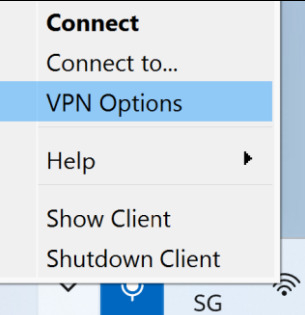
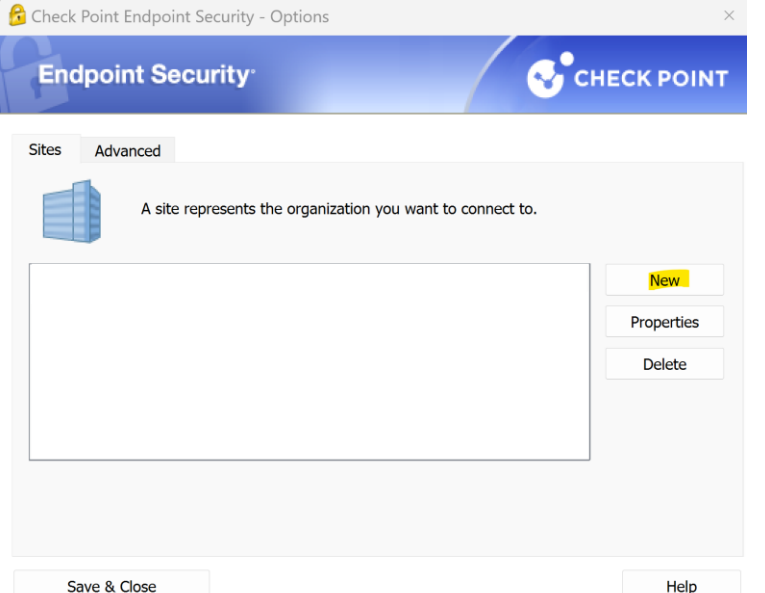
L'agent mobile Checkpoint nécessaire à cet effet peut être obtenu directement auprès du fabricant (sélectionner "Checkpoint Mobile Agent" lors de l'installation) :






<https://www.checkpoint.com/quantum/remote-access-vpn/#downloads>

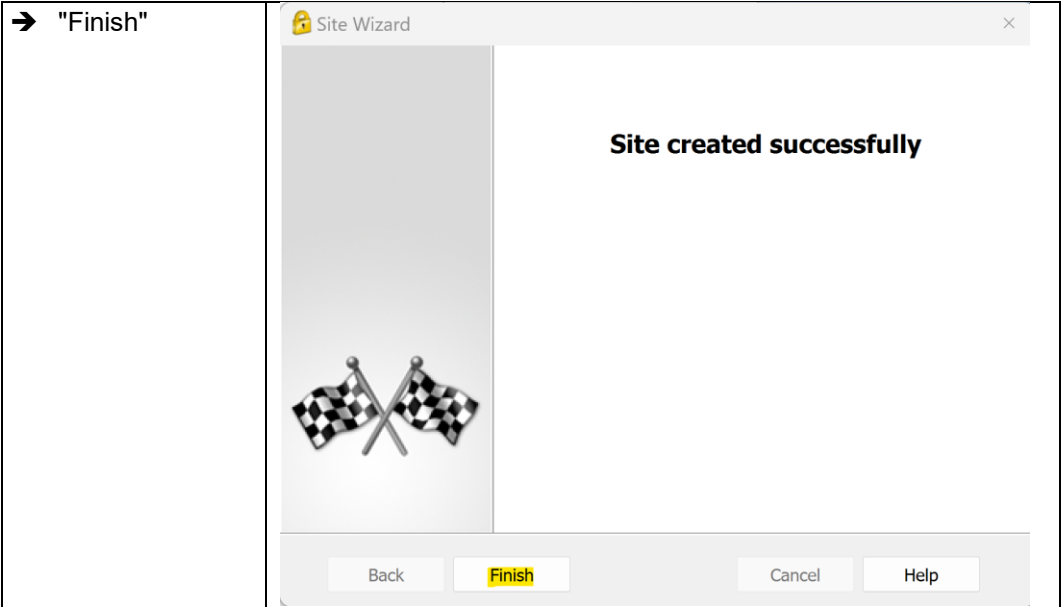
Une fois Checkpoint Mobile Agent installé avec succès sur l'équipement du demandeur, celui-ci peut être configuré comme suit pour accéder aux jumpstations dans les services de base.

Les adresses nécessaires à cet effet pour accéder aux systèmes cibles respectifs sont communiquées à l'utilisateur par la personne de contact concerné.

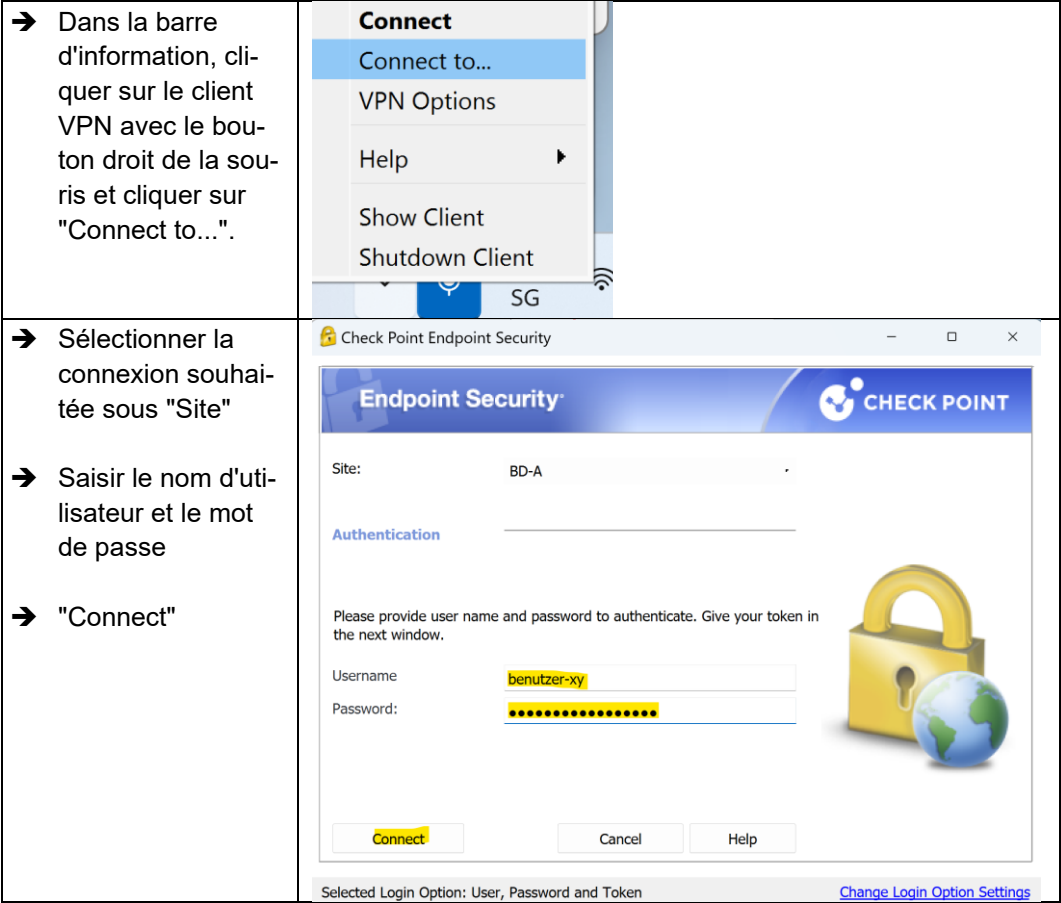
La configuration doit être effectuée séparément pour BD-A et BD-B :

<p>➔ Dans la barre d'information, cliquer sur le client VPN avec le bouton droit de la souris et cliquer sur "VPN Options".</p>	
<p>➔ "New"</p>	

<div>→ "Next"</div>	<div><div><div>Site Wizard</div><div><div></div><div>Welcome to the Site Wizard</div><div>The wizard will guide you through the configuration of a new site for the VPN client.</div><div></div></div><div><div>Back</div><div>Next</div><div>Cancel</div><div>Help</div></div></div></div>
<div><div>→ Server address or Name : indiquer le site de service de base souhaité, selon les informations fournies par la personne de contact</div><div>→ Display name : par exemple "BD-A" ou "BD-B"</div><div>→ "Next"</div></div>	<div><div><div>Site Wizard</div><div><div>Welcome to the Site Wizard</div><div>A site is your gateway to network resources.</div></div><div>To continue, fill in the required information and click next.</div><div><div>Server address or Name:</div><div>123.45.678.901</div></div><div><div><input checked="" type="checkbox"/> Display name:</div><div>BD-A</div></div></div><div><div>Back</div><div>Next</div><div>Cancel</div><div>Help</div></div></div>
<div><div>→ sélectionner "Username, Password and Token" (nom d'utilisateur, mot de passe et jeton)</div><div>→ "Next"</div></div>	<div><div><div>Site Wizard</div><div><div>Login Option Selection</div><div>Select your login sequence choice from the options set by your administrator</div></div><div>Please select your preferred login option from the following list</div><div><div>Username Password (Default)</div><div>Username Password (Default)</div><div>User, Password and Token</div></div></div><div><div>Back</div><div>Next</div><div>Cancel</div><div>Help</div></div></div>

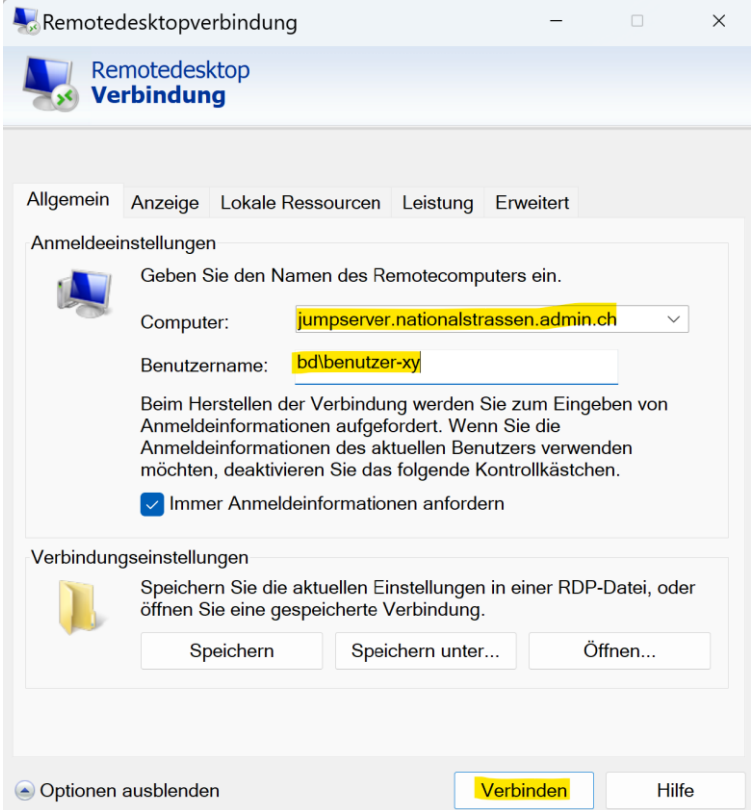


L'établissement de la connexion se déroule comme suit :



<div><div>→ Saisir le jeton MFA de SafeNet MobilePASS+.</div><div>→ "Next"</div></div>	<div><div><div>Check Point Endpoint Security</div><div><div>Endpoint Security</div><div>CHECK POINT</div></div><div>Site: BD-A</div><div>Authentication</div><div><div>Authenticating user 'jordan'. Please fill the required input.</div><div>Please respond to the challenge: Enter a passcode.</div><div>Response:</div><div>ConnectCancelHelp</div></div><div>Selected Login Option: User, Password and Token</div><div><div>VPN</div><div>Active site is BD-A</div><div>Connected</div></div></div></div>
<div><div>→ Si l'inscription est réussie, elle est annoncée par un son correspondant et la fenêtre est fermée.</div><div>→ Lorsque vous ouvrez à nouveau Checkpoint Mobile Agent, la connexion réussie s'affiche.</div></div>	

Vous pouvez ensuite vous connecter à un serveur Jump à l'aide d'une connexion Bureau à distance :

<ul style="list-style-type: none"> ➔ Démarrez l'application de connexion au bureau à distance. ➔ Computer: indiquez l'adresse du serveur Jump souhaité, conformément aux informations fournies par votre personne de contact ➔ Benutzername: saisir bd\User-name ➔ «Verbinden» (connecter) 	
--	---

Une fois la connexion établie avec la jumpstation, il est possible d'accéder aux systèmes cibles du site BD respectif :

- Accéder à une application web à l'aide d'un navigateur web
- Utiliser RDP (app pour prise de contrôle à distance) pour accéder aux autres serveurs
- Accéder à un serveur de fichiers à l'aide d'un explorateur de fichiers

Veuillez également consulter les instructions supplémentaires relatives à l'utilisation des services de base dans le répertoire principal du dossier OPERATIONS (O:) pour obtenir une aide supplémentaire.

Important :

- Actuellement, il est possible d'accéder à une jumpstation en BD-A un FW de périmètre en BD-A ou à un FW de périmètre en BD-B - mais pas sur plusieurs sites ;
- Deux (!) sessions RDP simultanées sont disponibles par Jumphost. Il faut donc veiller à ne pas laisser la session RDP ouverte inutilement longtemps et à la déconnecter une fois les travaux terminés.

5 Questions fréquentes - FAQ

Existe-t-il des alternatives à l'IAM BSA, comme par exemple l'eIAM ?

Non, les services au sein de l'infrastructure critique exploitée sur le réseau IP EES ne sont accessibles qu'à l'aide d'IAM BSA.

Combien coûte l'utilisation de l'IAM BSA ?

L'utilisation de l'IAM BSA est gratuite.

Quelle adresse e-mail dois-je enregistrer auprès de l'IAM BSA ?

Enregistrez votre adresse e-mail principale, celle que vous souhaitez utiliser à long terme. N'enregistrez PAS d'adresse e-mail jetable. Cette adresse e-mail est transmise par IAM BSA, avec votre prénom et votre nom, aux applications que vous utilisez. Elle est également nécessaire pour la réinitialisation du mot de passe dans le self-service.

Puis-je avoir plusieurs comptes IAM BSA ?

Il n'est prévu qu'un seul compte par personne physique.

Le même compte IAM BSA peut-il être utilisé par plusieurs personnes ?

Un compte IAM BSA représente toujours une seule personne physique, indépendamment du fait qu'elle utilise le compte IAM BSA pour son propre compte ou pour le compte d'autrui. C'est cette personne physique qui est responsable de l'utilisation correcte du compte IAM BSA, des applications auxquelles il donne accès et des transactions qui y sont effectuées avec cette authentification. Cela signifie que cette personne est également responsable de la conservation en toute sécurité et de l'utilisation correcte des données d'accès correspondantes (p. ex. mots de passe ou tokens).

Ai-je besoin de questions de sécurité dans IAM BSA pour l'assistance ?

Aucune question de sécurité n'est nécessaire pour identifier un utilisateur lors d'un appel ultérieur au support ; par exemple, pour une réinitialisation du mot de passe, l'utilisateur reçoit un e-mail contenant un token généré et un lien de confirmation. Le système vérifie cela et ne déclenche la réinitialisation que si les tokens correspondent.

Que se passe-t-il si les données saisies initialement, comme le numéro de téléphone ou le type d'employé, changent ?

Les données saisies initialement peuvent être modifiées ultérieurement, si nécessaire, par le biais de la personne de contact.

Puis-je utiliser un autre logiciel d'authentification multifactorielle (MFA) que Thales SafeNet MobilePASS+ ?

Non, lors de l'utilisation de l'application Thales, le token est également crypté - pour les autres applications, cela ne peut pas être imposé.

Pourquoi le mot de passe change-t-il automatiquement lorsque je suis affecté à une nouvelle UT ?

En raison des exigences d'autonomie et de la gestion des identités et des autorisations liées à l'UT, l'utilisateur est automatiquement invité à définir un nouveau mot de passe lorsqu'il est ajouté à une nouvelle unité territoriale (comme lors de l'enregistrement initial). Ce mot de passe est ensuite communiqué à toutes les zones d'exploitation, de sorte que le nouveau mot de passe peut être utilisé dans toutes les unités. Si l'utilisateur est connecté pendant le changement automatique de mot de passe, il peut continuer à travailler pendant environ une heure avant d'être bloqué en raison du changement.

Glossaire

Glossaire réseau IP EES

Voir la directive OFROU 13040 « Réseau IP EES ».

Glossaire IAM BSA

Terme/abréviation	Signification
2FA	2 Facteur d'authentification
AD	Active Directory
BD-A, BD-B	Services de base du site A, services de base du site B
DNS	Service de noms de domaine
Forest	Ensemble de domaines Active Directory avec un catalogue global, un schéma de répertoire et une configuration de répertoire communs.
IAM	Gestion des identités et des accès
IP	Protocole Internet
IIS	Serveur d'information Internet
MFA	Authentification multifactorielle
MS	Microsoft
OFIT	Office fédéral de l'informatique et des télécommunications
PAM	Gestion des accès privilégiés
PKI	Public Key Infrastructure
RAS	Service d'accès à distance
RBAC	Contrôle d'accès basé sur les rôles
RDP	Remote Desktop Protocol – protocole de bureau à distance
SAS PCE	Service d'authentification SafeNet Private Cloud Edition
TIC	Technologies de l'information et de la communication

Bibliographie

Instructions et directives de l'OFROU

-
- [1] Office fédéral des routes OFROU, « **OT Security Governance** », *instructions ASTRA 73006*, www.as-tra.admin.ch.
-
- [2] Office fédéral des routes OFROU, « **Réseau IP EES** », *directive ASTRA 13040*, www.astra.admin.ch.
-
- [3] Office fédéral des routes OFROU, « **OT Security** », *directive ASTRA 13030*, www.astra.admin.ch.
-

Liste des modifications

Édition	Version	Date	Modifications
2025	1.00	19.06.2025	Entrée en vigueur de l'édition 2025 (versions allemande, française, italienne et anglaise).

