

# Serveur de sécurité UXP 1.25

**Guide de gestion des services**

UXP-UG-SSSERVICE

# Table des matières

---

<b>Dernières notes de mise à jour</b>	<b>1</b>
<b>1. Introduction</b>	<b>3</b>
1.1. Serveur de sécurité UXP	3
1.2. Concepts UXP	4
1.3. URL importantes	8
1.4. Références	9
<b>2. Gérer mon compte</b>	<b>10</b>
2.1. Affichage de mes rôles	10
2.2. Changer de mot de passe	10
2.3. Réinitialiser un mot de passe oublié	10
2.4. Tentatives de connexion et verrouillage	10
<b>3. Sous-systèmes</b>	<b>11</b>
<b>4. Services UXP</b>	<b>12</b>
4.1. Gestion des services SOAP	12
4.1.1. Ajouter un WSDL	12
4.1.2. Actualiser un WSDL	12
4.1.3. Activer et désactiver un WSDL	13
4.1.4. Changer l'adresse d'un WSDL	13
4.1.5. Supprimer un WSDL	14
4.1.6. Changer les paramètres d'un service SOAP	14
4.1.7. Ajouter des en-têtes HTTP aux demandes SOAP	14
4.2. Gestion des API REST	16
4.2.1. Ajouter une API REST	16
4.2.2. Points de terminaison de l'API REST	17
4.2.3. Actualiser une description OpenAPI	18
4.2.4. Activer et désactiver une API REST	18
4.2.5. Changer l'URL de description OpenAPI	19
4.2.6. Paramètres de l'API REST	19
4.2.7. Ajouter des en-têtes HTTP aux demandes REST	20
4.2.8. Supprimer une API REST	22
4.3. Faire des demandes à une API REST	22

4.3.1. Exemple de configuration .....	22
4.3.2. Format des demandes REST .....	23
4.3.3. Demande en action .....	25
4.4. Sécurisation de la connexion au fournisseur de services .....	25
<b>5. Droits d'accès .....</b>	<b>27</b>
5.1. Modification des droits d'accès à un service SOAP .....	27
5.2. Changer les droits d'accès à une API REST .....	27
<b>6. Limites de débit .....</b>	<b>29</b>
6.1. Comment fonctionnent les limites de débit .....	29
6.2. Affichage des limites de débit .....	30
6.3. Ajouter une limite de débit à un service .....	30
6.4. Modifier et supprimer une limite de débit .....	31
<b>7. Groupes de droit d'accès local .....</b>	<b>32</b>
7.1. Ajouter un groupe local .....	32
7.2. Affichage et modification des membres d'un groupe local .....	32
7.3. Supprimer un groupe local .....	33
<b>8. Communication avec les systèmes d'information des clients .....</b>	<b>34</b>
8.1. Types de connexion .....	34
8.2. Certificats TLS internes au système d'information .....	35
8.3. Certificat TLS interne du serveur de sécurité .....	35
<b>9. Dépannage de l'échange de messages .....</b>	<b>36</b>
9.1. Comprendre les messages d'erreur .....	36
9.2. Erreurs provenant du système d'information du client du service .....	38
9.3. Erreurs provenant du serveur de sécurité du client du service .....	40
9.4. Erreurs provenant du serveur de sécurité du fournisseur de services .....	47
<b>10. API de gestion .....</b>	<b>52</b>
10.1. Rest API .....	52
10.1.1. API d'administration du serveur de sécurité .....	52
10.1.2. API du fournisseur d'identité .....	52
<b>Annexe A: Notes de mise à jour .....</b>	<b>53</b>

# Dernières notes de mise à jour

---

## 1.25.0 (11.2025)

- Ajout de la prise en charge de la mutualisation, qui permet à plusieurs membres UXP de partager un serveur de sécurité. Les utilisateurs peuvent désormais voir leur accès limité aux données de leur membre spécifique. Par défaut, la mutualisation est désactivée et peut être activée par le biais d'un indicateur de fonctionnalité. Contactez l'Autorité de gouvernance pour plus de détails.
- Présentation de l'Outil de diagnostic, une fonction conçue pour aider les administrateurs de serveurs de sécurité à identifier rapidement les problèmes potentiels en analysant les journaux du système à la recherche d'avertissements et d'erreurs. L'outil :
  - Affiche une liste concise des problèmes détectés dans l'interface utilisateur du serveur de sécurité.
  - Fournit un rapport système détaillé comprenant des informations sur le serveur, la configuration Nginx et UXP, et les fichiers journaux. Ce rapport peut être envoyé au service d'assistance en cas de besoin.
  - Examine les journaux pour y trouver des modèles d'avertissement et d'erreur courants.
  - Aide les administrateurs à identifier les problèmes sans avoir recours à SSH ou à des outils externes.
- Ajout d'un script de vérification post-installation (`uxp-installation-verification`) qui vérifie l'installation des paquets, l'état des services, la connectivité de la base de données et les rôles des utilisateurs, en fournissant des informations claires sur les réussites et les échecs. Le script répertorie également les adresses accessibles de l'interface utilisateur du serveur de sécurité et valide les connexions PostgreSQL, garantissant ainsi un bilan de santé complet après l'installation. Cela permet d'améliorer la validation post-déploiement et de réduire le dépannage manuel.
- Ajout de la prise en charge des clés EdDSA (Ed25519 et Ed448) sur les jetons logiciels et matériels qui prennent en charge le mécanisme CKM\_EDDSA\_PH. Notez que les versions 1.24 et 1.25 du Serveur de sécurité UXP sont incompatibles avec l'utilisation de clés EdDSA. Veillez à ce que les versions soient cohérentes ou évitez d'utiliser des clés EdDSA dans des environnements mixtes.
- Ajout d'une fonctionnalité de recherche à la boîte de dialogue de limitation du débit. Afin d'améliorer la convivialité dans les instances de grande taille, la boîte de dialogue de limitation du débit prend désormais en charge la recherche dynamique lors de la sélection de sous-systèmes ou de groupes. Les utilisateurs peuvent filtrer par nom ou par numéro d'identification pour trouver et sélectionner rapidement le bon sujet.
- Changements liés à la surveillance locale :
  - Les versions 9.x d'Elasticsearch et de Kibana sont désormais prises en charge.
  - La prise en charge d'Elasticsearch et de Kibana 7.x a été entièrement supprimée.
  - Un nouveau paramètre de configuration, `enable_update_existing_triggers`, a

été ajouté à `monitor-agent.ini`. Cela permet d'activer ou de désactiver les mises à jour des déclencheurs existants dans le modèle Zabbix UXP, ce qui permet d'éviter les écrasements involontaires.

- Changements liés à la gestion des utilisateurs :
  - Les exigences suivantes relatives aux noms d'utilisateur aux serveurs de sécurité ont été appliquées. Les utilisateurs existants peuvent continuer à accéder au système.
    - Les noms d'utilisateur sont désormais limités à 30 caractères.
    - Caractères autorisés dans les noms d'utilisateur : lettres (a-z), chiffres, caractères de soulignement (\_), tirets (-), points (.) et le symbole at (@).
- Augmentation de la RAM minimale recommandée de 4 Go à 6 Go.
- La fonction d'authentification automatique du jeton logiciel permet désormais de se connecter automatiquement au jeton après le démarrage de Serveur de sécurité UXP et de Serveur de registre UXP, ce qui permet un fonctionnement ininterrompu après les redémarrages. Cette fonction n'est disponible que lorsqu'elle est fournie par le service d'assistance sur demande et installée explicitement, car elle implique des considérations qui doivent être prises en compte au préalable.
- Java Runtime Environment est mis à jour vers la version 21. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Diverses corrections et améliorations mineures ont été apportées.

# 1. Introduction

---

Ce guide s'adresse aux Responsables des services, qui sont chargés de rendre les services Web disponibles sur Unified eXchange Platform (UXP) par l'intermédiaire de serveurs de sécurité.

Ce guide explique comment :

- publier les services UXP ;
- attribuer des droits d'accès aux services ;
- configurer une connexion sécurisée entre le serveur de sécurité et le système d'information fournissant les services ;
- consommer les services UXP ;
- dépanner les erreurs de service.

Ce guide n'explique pas comment faire fonctionner le serveur de sécurité UXP et suppose que l'opération est déléguée à quelqu'un d'autre (un opérateur UXP). Adressez-vous à votre opérateur UXP pour obtenir de l'aide concernant :

- la gestion des utilisateurs ;
- les nouveaux sous-systèmes ;
- la santé du serveur ;
- les journaux du système.

## 1.1. Serveur de sécurité UXP

La fonction principale d'un serveur de sécurité est de traiter les demandes de manière à préserver leur valeur probante.

Le serveur de sécurité est connecté à l'Internet public d'un côté et au système d'information au sein du réseau interne de l'organisation de l'autre côté. Dans un certain sens, le serveur de sécurité peut être considéré comme un pare-feu spécialisé au niveau de l'application, capable de servir d'intermédiaire entre les services Web SOAP et RESTful. Il doit donc être configuré en parallèle avec le pare-feu de l'organisation, qui sert d'intermédiaire pour les autres protocoles.

Le serveur de sécurité est doté de la fonctionnalité nécessaire pour sécuriser l'échange de messages entre un client et un fournisseur de services.

- Les messages transmis sur l'Internet public sont sécurisés par des signatures numériques et le cryptage.
- Le serveur de sécurité du fournisseur de services applique un contrôle d'accès aux messages entrants, garantissant ainsi que seuls les utilisateurs ayant signé un accord approprié avec le fournisseur de services peuvent accéder aux données.

## 1.2. Concepts UXP

**Instance UXP** est une installation unique de l'infrastructure UXP.

**Autorité de gouvernance UXP** est une organisation chargée de la maintenance de l'instance UXP.

**Membre UXP** désigne toute personne physique ou morale ayant adhéré à UXP afin de fournir ou de consommer des services, ou les deux.

**Sous-système** représente une partie du système d'information d'un membre UXP. Les membres UXP doivent déclarer certaines parties de leurs systèmes d'information comme sous-systèmes afin d'utiliser ou de fournir des services UXP.

Les sous-systèmes sont autonomes en termes de fourniture et d'utilisation des services UXP.

- Les droits d'accès des sous-systèmes des membres UXP sont indépendants — les droits d'accès accordés à un sous-système n'ont aucune incidence sur les droits d'accès des autres sous-systèmes du membre.
- Les services fournis par un sous-système sont indépendants des services fournis par les autres sous-systèmes du membre.

Un membre UXP peut associer plusieurs sous-systèmes différents à un serveur de sécurité, et un sous-système peut être associé à plusieurs serveurs de sécurité.

**Identifiant membre** est l'identifiant unique d'un membre UXP. L'identifiant UXP du membre se compose de trois parties : un identifiant d'instance, une classe de membre et un code de membre. Un exemple d'identifiant de membre est EE/GOV/12345678.

**Identifiant d'instance** est un code unique attribué à une instance UXP. Par exemple, le code pour l'instance de développement estonienne est EE-DEV et le code pour l'instance de production est EE.

**Classe de membre** regroupe les membres UXP ayant des propriétés similaires sous une unité commune. Par exemple, les agences publiques sont regroupées sous la classe de membre GOV, les organisations privées sont regroupées sous la classe de membre COM.

**Code membre** est associé à un certain membre UXP et est unique au sein de la classe de membre. Le code membre reste inchangé pendant toute la durée de vie du membre UXP. Par exemple, le code membre pour les organisations et les agences gouvernementales en Estonie est le code du registre du commerce.

**Code du sous-système** est ajouté à l'identifiant du membre afin de distinguer les sous-systèmes individuels des membres.

**Serveur de registre** est un composant UXP exploité par l'autorité de gouvernance qui sert de registre des informations nécessaires au fonctionnement de l'instance UXP. Le serveur de registre UXP distribue ces informations aux serveurs de sécurité sous la forme d'une configuration globale.

**Serveur de sécurité** est un composant UXP qui connecte les sous-systèmes d'un membre UXP à l'infrastructure UXP.

**Propriétaire du serveur de sécurité** est un membre UXP légalement responsable d'un

serveur de sécurité particulier.

**Client du serveur de sécurité** est un sous-système enregistré sur un serveur de sécurité. L'enregistrement doit être confirmé par l'Autorité de gouvernance et approuvé sur le serveur de registre.

**Mutualisation** est un modèle de fonctionnement du serveur de sécurité qui permet à plusieurs membres UXP de partager un seul serveur de sécurité tout en maintenant l'isolation des données et une gestion indépendante. Dans ce modèle, chaque membre opère dans son propre environnement logique, avec son propre ensemble d'utilisateurs, de rôles et de clés cryptographiques, ce qui garantit que les membres ne peuvent pas accéder aux informations des autres.

**Configuration globale** est un fichier qui contient les informations nécessaires au fonctionnement des serveurs de sécurité. Les serveurs de sécurité téléchargent régulièrement la configuration globale à partir du serveur de registre. Exemples d'informations dans la configuration globale :

- liste des membres UXP et de leurs sous-systèmes ;
- serveurs de sécurité enregistrés ;
- clients de serveurs de sécurité enregistrés ;
- certificat d'authentification enregistrés ;
- groupes globaux ;
- paramètres du système UXP ;
- adresses et clés publiques des services OCSP (si elles ne sont pas déjà disponibles via l'extension Authority Information Access des certificats) ;
- adresses et clés publiques des fournisseurs de services de certification agréés ;
- clés publiques des autorités de certification intermédiaires ;
- adresses et les clés publiques des prestataires de services d'horodatage agréés.

**Groupe global** est un groupe de droits d'accès géré au niveau du serveur de registre. Tous les sous-systèmes du groupe global disposent des droits d'accès attribués au groupe.

**Groupe local** est un groupe de droits d'accès géré au niveau du client du serveur de sécurité.

**Autorité d'horodatage (TSA)** est un fournisseur de services qui émet des horodatages.

**Services d'horodatage** sont des services fournis par la TSA afin de préserver la valeur probante des messages échangés via UXP.

**Horodatage** est une date et une heure accompagnées d'une signature délivrée par la TSA pour prouver qu'un message a existé à un moment précis.

**Autorité de certification (CA)** est un fournisseur de services de certification qui émet des certificats numériques.

**Services de certification** sont des services fournis par CA aux membres UXP, offrant des certificats numériques qui vérifient la propriété d'une clé publique.

**OCSP** signifie Online Certificate Status Protocol (protocole d'état des certificats en ligne).



Les répondeurs OCSP sont des serveurs exploités par l'autorité de certification afin de permettre la vérification de la validité des certificats.

**Clés UXP** sont des clés cryptographiques utilisées au sein de l'UXP. UXP utilise des paires de clés publiques et privées.

Une clé UXP est soit :

- une **clé de signature** — utilisée par les serveurs de sécurité pour signer numériquement les messages échangés, ou
- une **clé d'authentification** — utilisée par les serveurs de sécurité pour établir des canaux de communication sécurisés.

**Certificats UXP** sont des certificats délivrés par un fournisseur de services de certification agréé par l'autorité de gouvernance UXP.

**Dispositif de création de signature** est un mécanisme externe au serveur de sécurité permettant de protéger les clés cryptographiques que le serveur de sécurité utilise pour signer les messages. Les modules de sécurité matériels (HSM) et les jetons USB sont des exemples de dispositifs de création de signature.

**Jeton** est un espace de stockage destiné à protéger les clés cryptographiques utilisées par le serveur de sécurité. Le serveur de sécurité dispose de deux types de jetons :

- **jeton logiciel** — jeton logiciel intégré au serveur de sécurité,
- **jeton matériel** — jeton situé sur un dispositif de création de signature.

**Services UXP** sont des services fournis via l'infrastructure UXP.

**Message UXP** est un échange de données unidirectionnel entre un client et un fournisseur de services au sein de l'instance UXP. Selon son origine, un message peut être soit une demande, soit une réponse. Les messages UXP doivent être formés selon le protocole de message UXP ([UXP-PR-MESS]) et sont créés par les systèmes d'information des membres UXP.

**Client du service** est le sous-système d'un membre UXP qui a envoyé le message de demande.

**Fournisseur de services** est le sous-système du membre UXP qui a envoyé le message de réponse au client du service en réponse au message de demande.

**Conteneur de signature** est un fichier qui contient le message UXP signé, la signature numérique, l'horodatage et les certificats associés.

**Transaction** est la combinaison d'un message de demande et du message de réponse correspondant.

- **Identifiant de transaction** est un identifiant de transaction que le serveur de sécurité du client du service attribue lors du traitement d'un message de demande provenant du système d'information. L'identifiant de transaction est généré automatiquement par le serveur de sécurité afin de contenir une valeur unique pour chaque message transmis par le serveur de sécurité.

L'identifiant de transaction est également enregistré dans le journal des messages et peut être utilisé pour identifier de manière unique les messages UXP.

**Demande** est un message de demande, les demandes sont initiées par le client du service.

- **Identifiant de demande** est un identifiant de transaction qui fait partie de l'en-tête du message (id dans les en-têtes SOAP ([\[UXP-PR-MESS\]](#)) et Uxp-Queryid dans les en-têtes HTTP). L'identifiant de demande est attribué par le système d'information du client du service.

**En-têtes UXP** ou en-têtes de message sont des en-têtes spécifiques utilisés pour inclure des méta-informations spécifiques UXP dans les messages UXP.

- Pour les services SOAP, voir les en-têtes dans [\[UXP-PR-MESS\]](#).
- Pour les services REST, les en-têtes UXP sont :
  - Uxp-Client
  - Uxp-Service
  - Uxp-Queryid
  - Uxp-Transaction-Id
  - Uxp-Userid
  - Uxp-Consent-Ref
  - Uxp-Issue

## Instance UXP

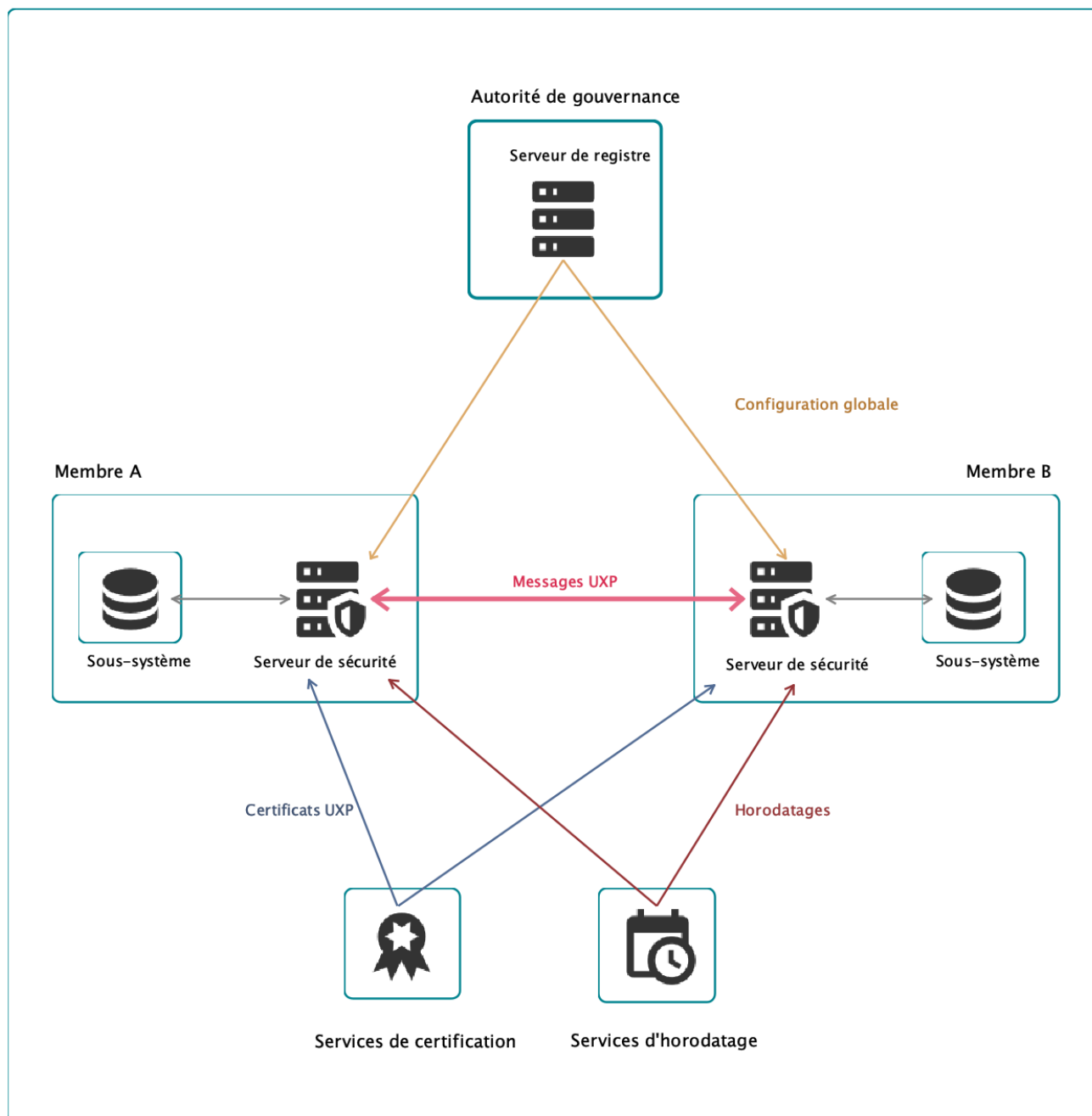


Figure 1. Schéma illustrant les composants d'une instance UXP

## 1.3. URL importantes

La liste suivante contient les URL les plus couramment utilisées pour interagir avec le serveur de sécurité.

Dans tous les URL, `<security-server>` doit être remplacé par l'adresse du serveur de sécurité.

Le type de connexion (HTTP ou HTTPS) dépend de la configuration du serveur de sécurité. Pour plus d'informations, voir la section [Communication avec les systèmes d'information des clients](#).

- Gestion **interface utilisateur** :

```
https://<security-server>:4000/
```

- Télécharger la **liste de tous les membres** et **sous-systèmes** enregistrés dans cette instance UXP :

```
http[s]://<security-server>/listClients
```

Voir [UXP-PR-META] pour plus d'informations sur les services de découverte offerts par UXP.

- URL permettant d'effectuer des **requêtes SOAP** à partir du système d'information :

```
http[s]://<security-server>/
```

- URL permettant d'effectuer des **demandes d'API REST** à partir du système d'information :

```
http[s]://<security-server>/restapi/<rest-api-path>[?<request-parameters>]
```

Les identifiants du client et du service doivent être envoyés sous forme d'en-têtes HTTPS. Pour un exemple détaillé, voir la section [Effectuer des demandes auprès d'une API REST](#).

## 1.4. Références

- [OpenAPI] Qu'est-ce que l'OpenAPI ?, <https://swagger.io/docs/specification/about/>
- [UXP-PR-MESS] Cybernetica AS. UXP: Protocole de message v4.0. Identifiant du document : UXP-PR-MESS
- [UXP-PR-META] Cybernetica AS. UXP: Protocole de métadonnées de service. Identifiant du document : UXP-PR-META
- [UXP-UG-PMA] Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA

## 2. Gérer mon compte

---

### 2.1. Affichage de mes rôles

Pour voir quels rôles votre compte possède, procédez comme suit :

1. Survolez votre nom d'utilisateur dans le coin supérieur droit.
2. Cliquez sur **Mon compte**. Vous pouvez voir quels sont vos rôles.

Si vous ne voyez pas les rôles dont vous avez besoin, contactez votre administrateur.

### 2.2. Changer de mot de passe

Pour changer votre mot de passe, procédez comme suit :

1. Survolez votre nom d'utilisateur dans le coin supérieur droit.
2. Cliquez sur **Changer le mot de passe**.



Si vous ne voyez pas d'option pour changer votre mot de passe dans le menu, cette fonction n'est pas disponible pour votre type de compte. Veuillez contacter votre administrateur pour changer votre mot de passe.

3. Saisissez l'ancien et le nouveau mot de passe et cliquez sur **Changer le mot de passe**.

Après avoir changé votre mot de passe, vous serez déconnecté et devrez vous connecter à nouveau.

### 2.3. Réinitialiser un mot de passe oublié

Si vous avez oublié votre mot de passe, contactez votre administrateur et demandez-lui de réinitialiser votre mot de passe.

### 2.4. Tentatives de connexion et verrouillage

Pour limiter les attaques par force brute lors de la connexion, le compte d'un utilisateur sera temporairement verrouillé après un trop grand nombre d'essais infructueux. Si vous êtes sûr que votre mot de passe est correct mais que vous n'arrivez toujours pas à vous connecter, il se peut que votre compte soit temporairement bloqué en raison d'un trop grand nombre de tentatives infructueuses. Veuillez attendre 10 à 15 minutes et réessayer. Si vous ne parvenez toujours pas à vous connecter, veuillez contacter votre administrateur pour réinitialiser votre mot de passe.

## 3. Sous-systèmes

---

Les sous-systèmes permettent aux membres UXP de distinguer les différents départements ou systèmes d'information au sein de l'organisation.

Les services UXP ne sont pas directement fournis ou consommés par un membre UXP lui-même, mais par ses sous-systèmes. Par conséquent, les services UXP et leurs droits d'accès sont liés à des sous-systèmes spécifiques.

Chaque sous-système de chaque membre UXP possède un identifiant unique au sein de la plate-forme UXP. Il s'agit d'une adresse qu'un message UXP utilise pour trouver le fournisseur de services ou pour vérifier les droits d'accès d'un consommateur de services.

Par exemple, lorsque le National Health Service (NHS) déclare son système d'information sur les dossiers médicaux électroniques (EHR) comme l'un de ses sous-systèmes sur l'instance UXP AA-PROD, l'identifiant unique du système d'information sur les EHR pourrait être AA-PROD/GOV/NHS/ehr.

Un membre UXP peut avoir un ou plusieurs sous-systèmes, en fonction de la taille de l'organisation, du nombre de systèmes d'information et du modèle de gestion utilisé par l'administrateur du serveur de sécurité.

Par exemple, le NHS pourrait avoir un portail pour les patients avec l'identifiant AA-PROD/GOV/NHS/patient-portal.

Lorsqu'un sous-système est enregistré pour utiliser un certain serveur de sécurité, nous appelons ce sous-système un client de ce serveur de sécurité.

## 4. Services UXP

---

Pour que les services du client du serveur de sécurité soient accessibles via l'infrastructure UXP, un Responsable des services doit les enregistrer en tant que services UXP. Un service UXP peut être basé soit sur une opération d'un service SOAP, soit d'une API REST.

- Service SOAP – un fichier WSDL contenant les descriptions des services SOAP est importé sur le serveur de sécurité. Un service SOAP est un ensemble d'opérations invocables. Chaque opération du service SOAP devient un service UXP indépendant.
- API REST – une API REST est encapsulée dans un service UXP. Les utilisateurs peuvent ensuite accéder à l'API REST en adressant une demande au service UXP.

### 4.1. Gestion des services SOAP

Les services SOAP sont gérés à deux niveaux :

- l'ajout, la suppression et la désactivation de services s'effectuent au niveau WSDL ;
- l'adresse du service, le type de connexion et les valeurs du délai d'attente du service sont configurés au niveau du service. Il est cependant facile d'étendre la configuration d'un service à tous les autres services dans le même WSDL.

#### 4.1.1. Ajouter un WSDL

**Droits d'accès :** Responsable des services

Lorsque vous ajoutez un fichier WSDL, le serveur de sécurité lit les informations relatives au service, telles que le code, le titre et l'adresse du service, à partir du fichier.

Pour ajouter un WSDL, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**, sélectionnez un client dans le tableau et cliquez sur l'icône **Services SOAP** de cette ligne.
2. Cliquez sur **Ajouter WSDL**, entrez l'adresse du WSDL dans la fenêtre qui s'ouvre et cliquez sur **Ajouter**.  
Par défaut, le serveur de sécurité ajoute le WSDL à l'état désactivé (voir [Activation et désactivation d'un WSDL](#)).

Pour afficher la liste des services contenus dans le WSDL, cliquez sur le symbole « > » situé devant la ligne WSDL afin de développer la liste.

Le serveur de sécurité vérifie si tous les services du WSDL sont pris en charge. Si le fichier contient des services non pris en charge, le serveur affiche un avertissement et ignore ces services.

#### 4.1.2. Actualiser un WSDL

## Droits d'accès : Responsable des services

Lors de l'actualisation, le serveur de sécurité recharge le fichier WSDL à partir de l'adresse WSDL du serveur de sécurité et vérifie les informations relatives au service dans le fichier rechargé par rapport aux services existants. Si la composition des services dans le nouveau WSDL a changé par rapport à la version actuelle, le serveur affiche un avertissement et vous pouvez soit poursuivre l'actualisation, soit l'annuler.


1. Pour actualiser le WSDL, recherchez le WSDL et cliquez sur **Actualiser**.
2. Si le nouveau WSDL contient des modifications par rapport au WSDL actuel du serveur de sécurité, vous verrez quels services ont été ajoutés ou supprimés. Pour poursuivre l'actualisation, cliquez à nouveau sur **Actualiser**.

Lorsque le WSDL est actualisé, les paramètres des services existants ne sont pas écrasés.

Si un service est supprimé lors de l'actualisation, les droits d'accès à ce service sont également supprimés.

### 4.1.3. Activer et désactiver un WSDL

#### Droits d'accès : Responsable des services

Un WSDL désactivé s'affiche en rouge dans le tableau des services avec une icône .

Les clients du service ne peuvent pas accéder aux services décrits par un WSDL désactivé – les clients du service recevront en retour un message d'erreur contenant le message que le Responsable des services a saisi lorsqu'il a désactivé le WSDL.

Si un WSDL est activé, les services qui y sont décrits deviennent accessibles aux clients des services. Il est donc nécessaire de s'assurer qu'avant d'activer le WSDL, les paramètres de tous ses services sont correctement configurés (voir [Modification des paramètres d'un service SOAP](#)).

Pour **activer** un WSDL, recherchez le WSDL contenant les services que vous souhaitez rendre disponibles et cliquez sur **Activer**.

Pour **désactiver** un WSDL, recherchez le WSDL contenant les services que vous souhaitez rendre indisponibles et cliquez sur **Désactiver**. Saisissez le message qui sera affiché aux clients qui tentent d'accéder aux services de ce WSDL, puis cliquez sur **Désactiver**.

### 4.1.4. Changer l'adresse d'un WSDL

#### Droits d'accès : Responsable des services

Pour changer l'adresse d'un WSDL, recherchez le WSDL, cliquez sur **Modifier** et entrez la nouvelle adresse.

Le serveur de sécurité actualise automatiquement le fichier WSDL (voir la section [Actualiser un WSDL](#)).



### 4.1.5. Supprimer un WSDL

**Droits d'accès :** Responsable des services

Lorsqu'un WSDL est supprimé, toutes les informations relatives aux services décrits dans le WSDL, y compris les droits d'accès, sont supprimées.

Pour supprimer un WSDL, recherchez-le, cliquez sur **Supprimer** et confirmez.

### 4.1.6. Changer les paramètres d'un service SOAP

**Droits d'accès :** Responsable des services

Les paramètres du service sont :

- URL du service — l'URL où le serveur de sécurité dirige les demandes destinées à ce service.
- Type de connexion — détermine si la connexion entre le serveur de sécurité et le serveur fournissant le service est cryptée et authentifiée.
  - Les types de connexion sont expliqués dans la section [Sécurisation de la connexion au fournisseur de services](#).
  - Outre la modification du type de connexion, vous pouvez télécharger le certificat TLS du système d'information fournissant le service et télécharger le certificat du serveur de sécurité sur la page **Détails du service**.
- Délai d'attente du service — délai maximal en secondes pendant lequel le serveur de sécurité attend la réponse du service avant de renvoyer une erreur de délai d'attente à l'utilisateur.

Pour changer les paramètres de service,

1. Recherchez le service et cliquez sur **Modifier**.
2. Sur la page **Détails du service** qui s'ouvre, modifiez les paramètres du service. Pour appliquer le paramètre choisi à tous les services décrits dans le même WSDL, cochez la case adjacente à ce paramètre dans la colonne **Appliquer tout**.
3. Cliquez sur **Enregistrer** pour appliquer les changements.

### 4.1.7. Ajouter des en-têtes HTTP aux demandes SOAP

**Droits d'accès :** Responsable des services

Vous pouvez définir des en-têtes HTTP que le serveur de sécurité ajoutera aux demandes entrantes avant de les transmettre au service SOAP. Par exemple, si vous devez mettre en place une authentification de base entre le serveur de sécurité et un service SOAP, vous pouvez ajouter les informations d'authentification au serveur de sécurité. Le serveur de sécurité inclut les informations d'identification dans chaque demande sous la forme d'un en-tête HTTP, par exemple, `Authorization: Basic dXNlcm5hbWU6VGE1NWYkVGpoJlU=`.

Les en-têtes HTTP sont gérés au niveau du service :

1. Recherchez le service et cliquez sur **Modifier**.
2. Sur la page **Détails du service** qui s'ouvre, trouvez la section **En-têtes HTTP**.
3. Cliquez sur **Ajouter** et saisissez la clé et la valeur de l'en-tête.

Le comportement dans le cas où la demande entrante contient déjà un en-tête avec la même clé est défini sur **Utiliser ceci**, car le serveur de sécurité ne transfère pas les en-têtes HTTP du client aux services SOAP. Ainsi, les en-têtes définis sur le serveur de sécurité sont toujours envoyés au service.



Vous ne pouvez pas écraser les en-têtes UXP et les en-têtes interdits, car ces en-têtes doivent être contrôlés uniquement par le client du service. Voir la liste des en-têtes réservés ci-dessous.

### En-têtes UXP réservés

- Uxp-Client
- Uxp-Service
- Uxp-Queryid
- Uxp-Transaction-Id
- Uxp-Userid
- Uxp-Consent-Ref
- Uxp-Issue

### En-têtes de transport réservés

- Accept-Charset
- Accept-Encoding
- Access-Control-Request-Headers
- Access-Control-Request-Method
- Connection
- Content-Length
- Cookie
- Cookie2
- Date
- DNT
- Expect
- Feature-Policy
- Host
- Keep-Alive

- Origin
- Proxy-Authenticate
- Proxy-Authorization
- Sec-Fetch-Site
- Sec-Fetch-Mode
- Sec-Fetch-User
- Sec-Fetch-Dest
- Referer
- TE
- Trailer
- Transfer-Encoding
- Upgrade
- User-Agent
- Via

## 4.2. Gestion des API REST

### 4.2.1. Ajouter une API REST

**Droits d'accès :** Responsable des services

Lorsque vous ajoutez une nouvelle API REST, le serveur de sécurité l'encapsule dans un service UXP unique et l'affiche dans le tableau des services basés sur l'API REST.

Pour ajouter une API REST, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**, sélectionnez un client dans le tableau et cliquez sur l'icône **API REST** de cette ligne.
2. Cliquez sur **Ajouter API REST**.
3. Choisissez si vous souhaitez ajouter l'API REST à l'aide d'une URL de base ou d'une URL de [description OpenAPI \[OpenAPI\]](#).
4. Saisissez l'URL et le code de service, puis cliquez sur **Ajouter**.  
Par défaut, l'API REST est ajoutée dans un état désactivé (voir [Activer et désactiver une API REST](#)).

### Ajouter une API REST à partir d'une description OpenAPI



Les serveurs de sécurité ne prennent en charge que la version 3.0 d'OpenAPI.

Lorsque vous ajoutez une API REST à partir d'une URL de description OpenAPI, tenez compte

du comportement de l'URL de base. En général, les serveurs de sécurité suivent la [spécification OpenAPI \[OpenAPI\]](#) pour l'URL de base :

- Les URL de base relatives sont résolues par rapport à l'hôte de l'URL de description OpenAPI.
- Plusieurs URL de base sont prises en charge. Choisissez l'URL de base à utiliser par le serveur de sécurité en [modifiant les paramètres de l'API REST](#).

Cependant, les modèles et les remplacements ne sont *pas* pris en charge pour l'URL de base.

## 4.2.2. Points de terminaison de l'API REST

Les droits d'accès à une API REST peuvent être gérés à un niveau plus granulaire si l'API est divisée en points de terminaison. Par exemple, si une API a des `/company` et `/taxreturn` distincts, vous pouvez gérer indépendamment les droits d'accès de ces points de terminaison sur le serveur de sécurité.

Pour chaque API REST, le serveur de sécurité crée automatiquement un point de terminaison faisant référence à l'ensemble de l'API (**ALL ENDPOINTS**) afin que vous puissiez accorder l'accès à toutes les ressources de l'API si vous ne souhaitez pas gérer les droits d'accès au niveau du point de terminaison.

### Diviser une API en points de terminaison

**Droits d'accès :** Responsable des services

Pour les API REST ajoutées manuellement à l'aide de l'URL de base, vous pouvez diviser l'API en points de terminaison sur le serveur de sécurité.



Pour les API REST ajoutées à partir des descriptions OpenAPI, tous les points de terminaison de la description sont automatiquement ajoutés au serveur de sécurité. Vous ne pouvez pas supprimer ces points de terminaison ni en ajouter de nouveaux. Cependant, vous pouvez toujours gérer les droits d'accès de ces points de terminaison à partir du serveur de sécurité.

Il n'est pas nécessaire d'indiquer au serveur de sécurité chaque point de terminaison de votre API REST. Uniquement ceux que vous souhaitez publier auprès des clients.

Pour **ajouter** un point de terminaison à l'API REST, procédez comme suit.

1. Recherchez l'API REST pour laquelle vous souhaitez déclarer un point de terminaison et cliquez sur **Ajouter un point de terminaison**.
2. Saisissez un chemin d'accès à l'API. Par exemple `/taxreturn`. Et cliquez sur **Ajouter**.
  - Pour indiquer un paramètre de chemin d'accès, utilisez des crochets. Par exemple, le point de terminaison `/users/{id}` correspondra aux demandes `/users/1`, `/users/2` et ainsi de suite.
  - Pour autoriser un nombre quelconque de paramètres de chemin, préfixez le nom du

paramètre par un signe plus (+) : `/users/{+params}`. Ce point de terminaison acceptera les demandes comportant un nombre quelconque de paramètres de chemin d'accès, à condition que le chemin d'accès commence par `/users/`.



Le champ point de terminaison n'accepte pas les paramètres de demande (`?name=John&age=20`) car la comparaison entre la demande entrante et la liste des points de terminaison se fait sur la partie paramètres de chemin. Le serveur de sécurité transmet à l'API tous les paramètres de la demande que le système d'information du client a inclus dans celle-ci.

Pour **supprimer** un point de terminaison, cliquez sur l'icône **Supprimer** sur la ligne du point de terminaison.

### 4.2.3. Actualiser une description OpenAPI

**Droits d'accès** : Responsable des services

Pour une API REST ajoutée à partir de son URL de description OpenAPI, une actualisation vérifie l'URL de description OpenAPI pour les mises à jour des points de terminaison de l'API REST et de l'URL de base.

Si l'actualisation détecte des changements dans la description OpenAPI par rapport à l'API REST sur le serveur de sécurité, le serveur de sécurité vous présente une liste des changements et vous pouvez soit poursuivre l'actualisation, soit l'annuler.

Pour actualiser la description OpenAPI, procédez comme suit.

1. Recherchez l'API REST que vous souhaitez actualiser et cliquez sur **Actualiser**.
2. Si la description OpenAPI a changé par rapport à l'API REST enregistrée sur le serveur de sécurité, ce dernier affiche les changements dans les listes des points de terminaison et des URL de base. Pour accepter les modifications et terminer l'actualisation, cliquez à nouveau sur **Actualiser**.

Si un point de terminaison est supprimé pendant l'actualisation, ses droits d'accès sont supprimés du serveur de sécurité.

### 4.2.4. Activer et désactiver une API REST

**Droits d'accès** : Responsable des services

Une API REST désactivée s'affiche en rouge dans le tableau des services avec une icône

Les clients du service ne peuvent pas accéder aux API REST désactivées — les clients du service recevront en retour un message d'erreur contenant le message que le Responsable des services a saisi lorsqu'il a désactivé l'API REST.

Si une API REST est activée, elle devient accessible aux clients du service. Il est donc nécessaire de s'assurer que les paramètres de l'API REST sont correctement configurés avant

de l'activer (voir [Modification des paramètres de l'API REST](#)).

Pour **activer** une API REST, recherchez l'API REST que vous souhaitez rendre disponible et cliquez sur **Activer**.

Pour **désactiver** une API REST, recherchez l'API REST que vous souhaitez rendre indisponible et cliquez sur **Désactiver**. Saisissez le message qui sera affiché aux clients qui tentent d'accéder à l'API REST, puis cliquez sur **Désactiver**.

## 4.2.5. Changer l'URL de description OpenAPI

**Droits d'accès :** Responsable des services

Si une description OpenAPI est déplacée vers une autre URL, vous pouvez modifier l'URL de l'API REST correspondante sur votre serveur de sécurité.

1. Recherchez l'API REST et cliquez sur **Modifier**.
2. Sur la page **Détails du service** qui s'ouvre, modifiez l'URL de description OpenAPI et cliquez sur **Enregistrer**.  
Le serveur de sécurité actualise automatiquement la description OpenAPI (voir la section [Actualiser un description OpenAPI](#)).

## 4.2.6. Paramètres de l'API REST

**Droits d'accès :** Responsable des services

Les paramètres du service sont :

- Code service — le code utilisé pour identifier un service UXP visé par une demande UXP. Le code service est saisi lors de l'ajout de l'API REST au serveur de sécurité et le code ne peut pas être modifié ultérieurement.
- URL de description OpenAPI — l'URL à partir de laquelle la description OpenAPI d'une API REST est récupérée (uniquement applicable aux API REST ajoutées à partir d'une description OpenAPI).
- URL de base — URL vers laquelle le serveur de sécurité dirige les demandes destinées à ce service REST.
- Type de connexion — détermine si la connexion entre le serveur de sécurité et le serveur fournissant le service est cryptée et authentifiée.
  - Les types de connexion sont expliqués dans la section [Sécurisation de la connexion au fournisseur de services](#).
  - Outre la modification du type de connexion, vous pouvez télécharger le certificat TLS du système d'information fournissant le service et télécharger le certificat du serveur de sécurité sur la page **Détails du service**.
- Délai d'attente du service — délai maximal en secondes pendant lequel le serveur de sécurité attend la réponse du service avant de renvoyer une erreur de délai d'attente à l'utilisateur.

Pour les **API REST ajoutées manuellement** à l'aide de l'URL de base, vous pouvez changer :

- l'URL de base ;
- le type de connexion ;
- le délai d'attente du service.

L'URL de description OpenAPI n'existe pas pour les API REST ajoutées manuellement à l'aide de l'URL de base.

Pour les **API REST ajoutées à l'aide de la description OpenAPI**, vous pouvez changer :

- l'URL de description OpenAPI ;
- le type de connexion ;
- le délai d'attente du service.

L'URL de base ne peut pas être modifiée pour les API REST ajoutées à l'aide de la description OpenAPI, car elle est lue directement à partir de la description OpenAPI. Lorsque plusieurs URL de base sont présentes dans la description OpenAPI, vous pouvez choisir celle qui sera utilisée dans la liste déroulante de l'URL de base.

## 4.2.7. Ajouter des en-têtes HTTP aux demandes REST

**Droits d'accès :** Responsable des services

Vous pouvez définir des en-têtes HTTP que le serveur de sécurité ajoutera aux demandes entrantes avant de les transmettre à l'API REST. Par exemple, si vous devez mettre en place une authentification à l'aide d'une clé entre le serveur de sécurité et une API, vous pouvez ajouter la clé de l'API au serveur de sécurité. Le serveur de sécurité inclut la clé API dans chaque demande sous la forme d'un en-tête HTTP, par exemple, `X-API-Key: 9ne323eF49dnC3o4Wf3Dw4gAev3S3fG`.

Les en-têtes HTTP sont gérés au niveau de l'API REST :

1. Recherchez le service et cliquez sur **Modifier**.
2. Sur la page **Détails du service** qui s'ouvre, trouvez la section **En-têtes HTTP**.
3. Cliquez sur **Ajouter** et entrez la clé de l'en-tête, la valeur et le comportement attendu au cas où la demande entrante contiendrait déjà un en-tête avec la même clé.

Les comportements possibles d'une clé dupliquée sont les suivants :

- Utiliser ceci – si le serveur de sécurité détecte dans une demande entrante vers cette API un en-tête HTTP avec la même clé, il remplace la valeur par celle définie sur le serveur de sécurité.
- Utiliser celle du client – si le serveur de sécurité détecte dans une demande entrante vers cette API un en-tête HTTP avec la même clé, il transmet la valeur du client à l'API REST. La valeur du serveur de sécurité n'est pas envoyée à l'API.

La comparaison des clés est insensible à la casse. Cela signifie que `authorization` et

Authorization sont la même clé.



Vous ne pouvez pas écraser les en-têtes UXP et les en-têtes interdits, car ces en-têtes doivent être contrôlés uniquement par le client du service. Voir la liste des en-têtes réservés ci-dessous.

### En-têtes UXP réservés

- Uxp-Client
- Uxp-Service
- Uxp-Queryid
- Uxp-Transaction-Id
- Uxp-Userid
- Uxp-Consent-Ref
- Uxp-Issue

### En-têtes de transport réservés

- Accept-Charset
- Accept-Encoding
- Access-Control-Request-Headers
- Access-Control-Request-Method
- Connection
- Content-Length
- Cookie
- Cookie2
- Date
- DNT
- Expect
- Feature-Policy
- Host
- Keep-Alive
- Origin
- Proxy-Authenticate
- Proxy-Authorization
- Sec-Fetch-Site
- Sec-Fetch-Mode
- Sec-Fetch-User
-



Sec-Fetch-Dest

- Referer
- TE
- Trailer
- Transfer-Encoding
- Upgrade
- User-Agent
- Via

## 4.2.8. Supprimer une API REST

**Droits d'accès :** Responsable des services

Lorsqu'une API REST est supprimée, le service UXP correspondant et ses droits d'accès sont supprimés.

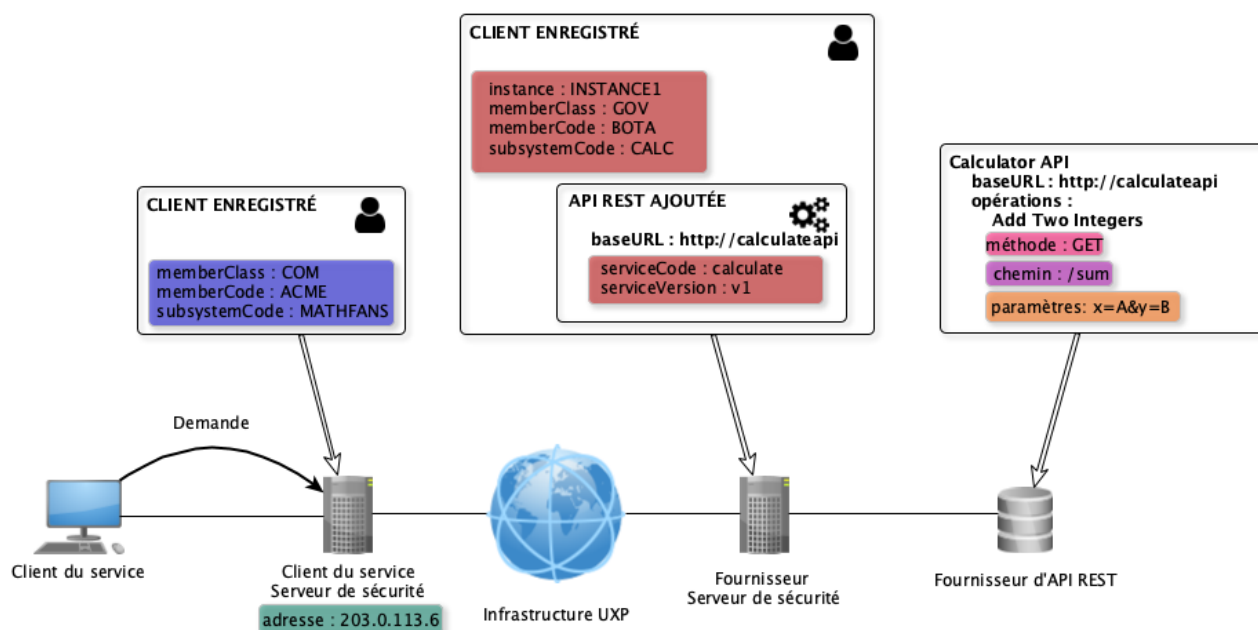
Pour supprimer une API REST, recherchez l'API REST, cliquez sur **Supprimer** et confirmez.

## 4.3. Faire des demandes à une API REST

Après avoir [ajouté une API REST](#) au serveur de sécurité et lui avoir accordé des [droits d'accès](#), l'API devient disponible pour les membres UXP en tant que service UXP. Cette section décrit comment les clients du service peuvent faire des demandes aux API REST via l'infrastructure UXP.

### 4.3.1. Exemple de configuration

Voici un exemple de configuration de l'infrastructure UXP pour illustrer les informations requises pour effectuer des demandes à une API REST. Les informations affichées sur fond coloré sont utilisées pour composer la demande.



### Client du service

Système d'information qui souhaite utiliser une API REST sur l'infrastructure UXP. Ce système d'information doit être enregistré sur un serveur de sécurité.

### SS Client du service

Serveur de sécurité où le client du service est enregistré. Les informations contenues dans la boîte montrent comment le client du service est configuré sur le serveur de sécurité.

### Fournisseur d'API REST

Système d'information qui offre un accès à son API REST via l'infrastructure UXP. Dans l'exemple, le fournisseur a ajouté une API REST avec l'URL de base <http://calculateapi> à son serveur de sécurité avec le code de service `calculate` et la version de service `v1`.

### SS Fournisseur

Serveur de sécurité où le fournisseur de l'API REST est enregistré. Les informations contenues dans la boîte montrent comment le fournisseur d'API REST et l'API REST sont configurés sur le serveur de sécurité.

## 4.3.2. Format des demandes REST

Les demandes de services UXP basés sur l'API REST sont envoyées par le client du service au serveur de sécurité du client du service via HTTP(S). HTTPS est utilisé lorsque les messages entre le serveur de sécurité et ses clients sont sécurisés par TLS.

Lors de l'élaboration d'une demande de service, le chemin et les paramètres spécifiques à l'API doivent être inclus dans l'URL de la demande et les informations spécifiques à UXP (détails du client et du service) dans les en-têtes de la demande.

### Format de l'URL de demande

```
<METHOD> http[s]://<security-server>/restapi/<rest-api-path>[?<request-parameters>]
```

Méthode HTTP

Point de terminaison du service client SS

Chemin  
d'accès à l'API REST  
(facultatif)Paramètres  
de la demande  
(facultatif)

## En-têtes de demande requis

```
Uxp-Client: <instance>/<member-class>/<member-code>/<subsystem-code>
```

```
Uxp-Service: <instance>/<member-class>/<member-code>/<subsystem-code>/<service-code>/<service-version>
```

## Autres en-têtes de demande

La demande peut comporter des en-têtes supplémentaires. Les en-têtes supplémentaires seront transmis à l'API REST.

Les couleurs permettent de repérer les informations de l'[exemple de configuration](#) qui sont utilisées dans l'URL et les en-têtes de la demande.

## Méthode HTTP

Les méthodes HTTP prises en charge par les serveurs de sécurité sont les suivantes : HEAD, GET, DELETE, POST, PUT et PATCH. Les informations sur les méthodes HTTP prises en charge par l'API REST doivent être fournies par le fournisseur de l'API REST.

## Point de terminaison du SS du client du service

Point de terminaison où le serveur de sécurité attend les requêtes vers les API REST. L'adresse `<security-server>` doit être remplacée par l'adresse de service du serveur de sécurité du client du service.

## Détails du client du service

Partie qui spécifie l'origine de la demande. (Les détails sont déterminés lors de l'enregistrement du client sur le serveur de sécurité)

Si la demande doit être faite en tant que membre, le sous-système doit être omis. Par exemple, `EXAMPLE/COM/ACME`.

## Chemin de l'API REST (facultatif)

Chemin qui sera ajouté à l'URL de base avant de transmettre la demande à l'API REST. Les informations sur les chemins possibles doivent être fournies par le fournisseur de l'API REST.

## Détails du service

Partie qui spécifie le service UXP visé. Les détails du service (identifiant UXP du service) doivent être fournis au client du service par le fournisseur de l'API REST.

Si le service n'a pas de version, la version du service doit être omise. Par exemple, `EXAMPLE/GOV/BOTA/CALC/calculate`.

## Paramètres de la demande (facultatif)

Les paramètres de demande possibles doivent être fournis par le fournisseur de l'API REST.

## Exemple de demande

Voici un exemple de demande au service `calculate.v1` décrit dans l'exemple de configuration. Les caractères de remplacement des paramètres de demande ont été remplacés par des paramètres réels - 15 et 9.

<b>GET</b> <code>http://203.0.113.6/restapi/sum?x=15&amp;y=9</code>			
Méthode HTTP	Point de terminaison du service client SS	Chemin d'accès à l'API REST	Paramètres de la demande

<b>Uxp-Client:</b>	<code>EXAMPLE/COM/ACME/MATHFANS</code>
<b>Uxp-Service:</b>	<code>EXAMPLE/GOV/BOTA/CALC/calculate/v1</code>

Lisez la section [Demande en action](#) pour voir comment une requête adressée à un service basé sur une API REST est traitée via UXP.

## 4.3.3. Demande en action

1. Le client du service envoie la demande à son serveur de sécurité.
2. Le serveur de sécurité du client détermine le service UXP demandé et transmet la demande au serveur de sécurité du fournisseur.
3. Le serveur de sécurité du fournisseur déterminera l'API REST de destination en fonction du service demandé et élaborera une demande qui sera envoyée à l'API REST.

À la suite de l'exemple de demande, la demande réelle transmise à l'API REST ressemblerait à ceci :

<b>GET</b> <code>http://calculateapi/sum?x=15&amp;y=9</code>			
Méthode HTTP	URL de base	Chemin d'accès à l'API REST	Paramètres de la demande

<b>Uxp-Client:</b>	<code>EXAMPLE/COM/ACME/MATHFANS</code>
<b>Uxp-Service:</b>	<code>EXAMPLE/GOV/BOTA/CALC/calculate/v1</code>

4. La réponse de l'API REST est renvoyée au client du service par l'intermédiaire des serveurs de sécurité.

## 4.4. Sécurisation de la connexion au fournisseur de services

## Droits d'accès : Responsable des services

Le niveau de sécurité entre le serveur de sécurité et le système d'information fournissant le service est déterminé par le choix d'un type de connexion. Vous pouvez modifier le type de connexion pour chaque service séparément sur la page **Détails du service**.

Les types de connexion sont les suivants :

### HTTPS – cryptée avec authentification mutuelle

- **Effet** : Connexion sécurisée où la connexion est cryptée et où le serveur de sécurité et le fournisseur de services s'authentifient à l'aide de certificats TLS.
- **Comment configurer** : Définissez le protocole de l'URL du service ou de l'API de base sur `https://` et choisissez **HTTPS** comme type de connexion. Téléchargez le certificat interne du serveur de sécurité vers le système d'information du fournisseur de services et le certificat TLS du fournisseur de services vers le serveur de sécurité. Vous pouvez le faire sur la page **Détails du service** de celui-ci.



Le serveur de sécurité conserve une liste de certificats TLS internes pour chaque client du serveur de sécurité. Si le système d'information qui fournit des services est également un système de consommation de services, vous pouvez télécharger le certificat une seule fois et il fonctionnera dans les deux cas.

### HTTPS NOAUTH — crypté sans authentification du fournisseur de services

- **Effet** : Connexion sécurisée où la connexion est cryptée mais où le serveur de sécurité n'authentifie pas le fournisseur de services.
- **Comment configurer** : Définissez le protocole de l'URL du service ou de l'API de base sur `https://` et choisissez **HTTPS NOAUTH** comme type de connexion.

### HTTP — connexion non sécurisée entre le serveur de sécurité et le service

- **Effet** : Connexion non sécurisée où la communication n'est pas cryptée et où aucun des partenaires de la communication ne s'authentifie. À n'utiliser que pour l'échange d'informations non sensibles ou si le serveur de sécurité et le fournisseur de services se trouvent dans un environnement de confiance fermé, par exemple un segment de réseau local distinct.
- **Comment configurer** : Définissez le protocole de l'URL du service ou de l'API de base sur `http://` et choisissez **HTTP** comme type de connexion.



Pour les services REST ajoutés à partir d'une description OpenAPI, cette dernière détermine les URL de base possibles et, par conséquent, les types de connexion possibles.

## 5. Droits d'accès

---

Les droits d'accès peuvent être accordés directement à un sous-système ou à un groupe de sous-systèmes et de membres UXP. Si vous accordez un accès à un groupe, l'accès s'étend à tous les membres du groupe.

Il existe deux types de groupes dans UXP. Les groupes globaux sont créés de manière centralisée par l'autorité de gouvernance UXP. Des groupes locaux peuvent être créés sur les serveurs de sécurité (voir la section [Groupes de droits d'accès locaux](#)).

### 5.1. Modification des droits d'accès à un service SOAP

**Droits d'accès :** Responsable des services

Pour ajouter des droits d'accès à un service SOAP, procédez comme suit.

1. Allez à la page **Clients du serveur de sécurité**, choisissez un client dans le tableau et cliquez sur **Services SOAP** sur cette ligne.
2. Choisissez un service et cliquez sur **Droits d'accès**.
3. Sur la page **Détails du service** qui s'ouvre, trouvez la section **Droits d'accès**.
4. Cliquez sur **Ajouter un accès**. Vous pouvez effectuer une recherche parmi tous les sous-systèmes et groupes globaux enregistrés auprès de l'autorité de gouvernance UXP et parmi les groupes locaux du client du serveur de sécurité qui fournit ce service.  
Pour accorder l'accès à tous les membres de l'instance UXP, utilisez le groupe global `all-subsystems`.
5. Sélectionnez les sous-systèmes et les groupes qui auront accès à ce service et cliquez sur **Ajouter la sélection**.

Pour supprimer l'accès aux services, supprimez les sous-systèmes et les groupes du tableau des droits d'accès.

### 5.2. Changer les droits d'accès à une API REST

**Droits d'accès :** Responsable des services

Pour ajouter des droits d'accès à une API REST, procédez comme suit.

1. Allez à la page **Clients du serveur de sécurité**, choisissez un client dans le tableau et cliquez sur **API REST** sur cette ligne.
2. Développez une API REST pour voir les points de terminaison déclarés pour l'API. Chaque API dispose d'un point de terminaison **ALL ENDPOINTS** qui peut être utilisé pour contrôler l'accès à l'ensemble de l'API.
3. Choisissez un point de terminaison et cliquez sur **Droits d'accès**.
4. Sur la page **Détails du service** qui s'ouvre, trouvez la section **Droits d'accès**.

5. Cliquez sur **Ajouter un accès** sur le point de terminaison auquel vous souhaitez accorder l'accès. Vous pouvez effectuer une recherche parmi tous les sous-systèmes et groupes globaux enregistrés auprès de l'autorité de gouvernance UXP et parmi les groupes locaux du client du serveur de sécurité qui fournit ce service.  
Pour accorder l'accès à tous les membres de l'instance UXP, utilisez le groupe global `all-subsystems`.
6. Sélectionnez les sous-systèmes et les groupes qui auront accès à ce service, choisissez les méthodes HTTP que vous souhaitez autoriser pour eux et cliquez sur **Ajouter la sélection**.

Pour modifier les droits d'accès d'un point de terminaison, cliquez sur **Modifier** et supprimez ou ajoutez autant de cases à cocher que nécessaire. Lorsque vous avez terminé, cliquez sur **Enregistrer** pour appliquer les modifications. Si vous avez supprimé toutes les méthodes d'un sous-système ou d'un groupe, celui-ci sera supprimé de la liste des droits d'accès et n'aura plus accès à ce point de terminaison. (Sauf si le sous-système ou le groupe a accès à tous les points de terminaison de cette API ou si le sous-système fait partie d'un groupe qui a accès à ce point de terminaison ou à l'ensemble de l'API)

## 6. Limites de débit

---

Les limites de débit vous permettent de contrôler le nombre de requêtes que les consommateurs peuvent envoyer à un service au cours d'une période donnée.

### 6.1. Comment fonctionnent les limites de débit

Les limites de débit prennent en charge les cas d'utilisation suivants :

- la protection d'un service contre la surcharge ;
- l'application des accords de niveau de service (SLA) pour un ou plusieurs consommateurs.

Chaque limite de débit contrôle la consommation d'un service spécifique. Vous ne pouvez pas appliquer une limite unique à plusieurs services en même temps, ni définir une limite pour un seul point de terminaison API REST.

Les limites de débit régulent la consommation de services pour les sujets concernés, qui peuvent être des sous-systèmes UXP individuels ou des groupes de sous-systèmes. Vous pouvez utiliser des groupes locaux ou globaux pour définir une limite commune à plusieurs sous-systèmes à la fois. L'autorité de gouvernance UXP crée des groupes globaux de manière centralisée. Vous pouvez créer des groupes locaux sur les serveurs de sécurité (voir la section [Groupes de droits d'accès locaux](#)).

Plusieurs limites de débit peuvent s'appliquer à un même service, chaque limite régulant la consommation du service pour un ensemble différent de sujets.

Une fois la limite atteinte, le système cesse de transférer les demandes vers le service provenant des sujets concernés par la limite jusqu'à la fin de la période en cours. L'horloge du système détermine le début de la période suivante. Par exemple, la minute suivante commence lorsque l'horloge atteint la minute suivante.

Un sous-système peut être soumis simultanément à une limite individuelle et à une ou plusieurs limites collectives pour le même service. En tant que membre du groupe, l'utilisation des services du sous-système est prise en compte dans toutes ces limites. Cependant, d'autres membres du groupe peuvent consommer une partie ou même la totalité de la capacité disponible du groupe avant qu'un sous-système individuel ne puisse utiliser sa part. Cela signifie que même si un sous-système n'a pas atteint sa limite individuelle, il peut être incapable d'accéder au service une fois que la limite du groupe est atteinte.

Par exemple, le sous-système A peut être soumis aux limites suivantes :

- Limite 1 - 50 requêtes/minute, sujet : sous-système A ;
- Limite 2 - 100 requêtes/minute, sujet : groupe local B ;
- Limite 3 - 1 000 requêtes/minute, sujet : groupe global `all-subsystems`.

L'utilisation du service du sous-système A est prise en compte dans toutes ces limites et



réduit les demandes restantes pour les deux groupes. Toutefois, il se peut que le sous-système A ne puisse consommer aucune des 50 requêtes qui lui sont attribuées si d'autres membres du groupe local B consomment la totalité des 100 requêtes du groupe.



Les limites de débit sont indépendantes des droits d'accès. L'ajout d'une limite de débit à un sous-système ou à un groupe particulier ne garantit pas à ce sous-système ou à ce groupe l'accès au service. Les droits d'accès doivent être accordés séparément.

## 6.2. Affichage des limites de débit

**Droits d'accès :** Responsable des services

Pour connaître les limites de débit applicables aux services, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**, sélectionnez un client dans le tableau, puis cliquez sur **Services SOAP** ou **API REST** sur cette ligne.
  - a. Dans l'onglet **Services SOAP**, développez une URL WSDL pour voir les limites de débit pour les services SOAP.
  - b. Dans l'onglet **API REST**, consultez les limites de débit pour les API REST.  
Si une seule limite de débit s'applique au service, vous pouvez voir la valeur limite. En cas de limites multiples, vous pouvez voir le nombre de limites appliquées au service. Si aucune limite n'est indiquée, le nombre de demandes transmises au service est illimité.

Pour connaître les limites de débit applicables à un service spécifique, procédez comme suit.

1. Dans la vue précédente, choisissez un service SOAP ou une API REST.
2. Cliquez sur **Modifier**.
3. Sur la page **Détails du service** qui s'ouvre, recherchez la section **Limites de débit**.

## 6.3. Ajouter une limite de débit à un service

**Droits d'accès :** Responsable des services

Pour ajouter une limite de débit à un service SOAP ou à une API REST, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**, sélectionnez un client dans le tableau, puis cliquez sur **Services SOAP** ou **API REST** sur cette ligne.
2. Choisissez un service SOAP sous un WSDL ou une API REST, respectivement, et cliquez sur **Modifier**.
3. Sur la page **Détails du service** qui s'ouvre, recherchez la section **Limites de débit**.
4. Cliquez sur **Ajouter une limite de débit**.
5. Saisissez le nom de la limite de débit.



Plusieurs limites de débit peuvent porter le même nom. Cela permet de gérer de

nombreuses limites, en particulier si vous disposez d'un système de dénomination spécifique pour vos limites, tel que l'utilisation de niveaux de limites.

6. Saisissez le nombre de demandes autorisées et sélectionnez la période de temps appropriée.
7. Par défaut, une limite de débit contrôle la consommation de services pour tous les consommateurs de services (groupe global `all-subsystems`). Pour limiter la consommation pour différents sujets, développez l'entrée **Sujets** et sélectionnez un ou plusieurs sous-systèmes ou groupes. Vous pouvez utiliser le champ de recherche pour filtrer les sujets par identifiants UXP (instance, classe membre, code membre, code sous-système, code groupe).
8. Cliquez sur **Ajouter une limite de débit**.

## 6.4. Modifier et supprimer une limite de débit

**Droits d'accès :** Responsable des services

1. Accédez à la page **Clients du serveur de sécurité**, sélectionnez un client dans le tableau, puis cliquez sur **Services SOAP** ou **API REST** sur cette ligne.
2. Choisissez un service SOAP sous un WSDL ou une API REST, respectivement, et cliquez sur **Modifier**.
3. Sur la page **Détails du service** qui s'ouvre, recherchez la section **Limites de débit** et sélectionnez la limite à modifier.
4. Cliquez sur **Modifier**.
5. Modifiez le nom de la limite de débit, ajustez le nombre de requêtes autorisées, modifiez la période ou modifiez les sujets auxquels cette limite s'applique. Pour limiter la consommation pour différents sujets, développez l'entrée **Sujets** et sélectionnez un ou plusieurs sous-systèmes ou groupes. Vous pouvez utiliser le champ de recherche pour filtrer les sujets par identifiants UXP (instance, classe membre, code membre, code sous-système, code groupe).
6. Cliquez sur **Appliquer les changements**.

Pour supprimer une limite de débit, cliquez sur **Supprimer** dans la vue d'édition des limites de débit et confirmez votre choix.

## 7. Groupes de droit d'accès local

Pour gérer les droits d'accès et les limites de débit de plusieurs sous-systèmes UXP qui utilisent les mêmes services, vous pouvez créer un groupe de droits d'accès local. Les droits d'accès et les limites de débit du groupe s'appliquent à tous les membres du groupe. Les groupes locaux sont basés sur le client du serveur de sécurité, c'est-à-dire qu'un groupe local ne peut être utilisé que pour gérer les droits d'accès aux services et les limites de débit d'un client du serveur de sécurité au sein d'un serveur de sécurité.

### 7.1. Ajouter un groupe local

**Droits d'accès :** Responsable des services

Pour créer un groupe local pour un client du serveur de sécurité, procédez comme suit.

1. Allez à la page **Clients du serveur de sécurité**, sélectionnez un client et cliquez sur l'icône **Groupes locaux** sur cette ligne.
2. Pour créer un nouveau groupe, cliquez sur **Ajouter un groupe**. Dans la fenêtre qui s'ouvre, saisissez le code et la description du nouveau groupe et cliquez sur **Ajouter**.



Un code de groupe local est limité au jeu de caractères [a-zA-Z0-9\_-]

### 7.2. Affichage et modification des membres d'un groupe local

**Droits d'accès :** Responsable des services

Pour **afficher les membres** d'un groupe local, procédez comme suit.

1. Allez à la page **Clients du serveur de sécurité**, sélectionnez un client et cliquez sur l'icône **Groupes locaux** sur cette ligne.
2. Sur la page qui s'ouvre, choisissez un groupe dont vous souhaitez afficher ou modifier les membres, puis cliquez sur **Modifier** pour ouvrir la vue détaillée. La vue détaillée contient la liste des membres actuels du groupe.

Pour **ajouter un ou plusieurs membres** à un groupe local, procédez comme suit dans la vue détaillée du groupe.

1. Cliquez sur **Ajouter des membres**.
2. Dans la fenêtre qui s'ouvre, sélectionnez les sous-systèmes que vous souhaitez ajouter au groupe et cliquez sur **Ajouter la sélection**.

Pour **supprimer des membres** d'un groupe local, sélectionnez les membres à supprimer dans la vue détaillée du groupe et cliquez sur **Supprimer la sélection**. Pour supprimer tous les membres du groupe, cliquez sur **Supprimer tout**.

Dans la vue détaillée du groupe, vous pouvez également **modifier la description du groupe**.

## 7.3. Supprimer un groupe local



Lorsqu'un groupe local est supprimé, tous les droits d'accès des membres du groupe, qui ont été accordés du fait de leur appartenance au groupe, sont révoqués. De plus, les limites de débit qui avaient été définies uniquement pour ce groupe local ne limitent plus la consommation du service.

**Droits d'accès :** Responsable des services

Pour supprimer un groupe local, choisissez un groupe dans le tableau des groupes locaux d'un client du serveur de sécurité, cliquez sur **Supprimer** et confirmez.

## 8. Communication avec les systèmes d'information des clients

### 8.1. Types de connexion

**Droits d'accès :** Administrateur serveur, Responsable des services

Le type de connexion détermine la sécurité de la connexion entre un serveur de sécurité et un système d'information qui s'y connecte. Un serveur de sécurité peut utiliser le type de connexion HTTP, HTTPS ou HTTPS NOAUTH pour communiquer avec les systèmes d'information. Cette partie du guide de l'utilisateur se concentre sur la connexion entre le serveur de sécurité et les systèmes d'information qui font des demandes de service.

Les types de connexion sont les suivants :

#### HTTPS – cryptée avec authentification mutuelle

- **Effet :** Connexion sécurisée où la connexion est cryptée et où le serveur de sécurité et le client du service s'authentifient à l'aide de certificats TLS.
- **Comment configurer :** Choisissez **HTTPS** comme type de connexion. Téléchargez le certificat interne du serveur de sécurité sur le système d'information du client du service et le certificat TLS du client du service sur le serveur de sécurité. Vous pouvez le faire sur la page **Systèmes d'information** du client du serveur de sécurité.



Le serveur de sécurité conserve une liste de certificats TLS internes pour chaque client du serveur de sécurité. Si le système d'information qui consomme des services est également un fournisseur de services, vous pouvez télécharger le certificat une seule fois et il fonctionnera dans les deux cas.



Le serveur de sécurité fournit au propriétaire du serveur de sécurité, sur demande, un ensemble complet de données de surveillance. Par conséquent, seul le schéma de connexion HTTPS est utilisé pour communiquer avec le propriétaire du serveur de sécurité. Cela permet d'éviter que d'autres clients du serveur de sécurité se comportent comme le propriétaire du serveur de sécurité et accèdent à des données de surveillance qu'ils ne sont pas autorisés à voir. Seul l'administrateur serveur peut gérer les connexions internes du propriétaire du serveur de sécurité.

#### HTTPS NOAUTH – cryptée sans authentification du client du service

- **Effet :** Connexion sécurisée où la connexion est cryptée mais où le serveur de sécurité n'authentifie pas le client du service.
- **Comment configurer :** Choisissez **HTTPS NOAUTH** comme type de connexion.

#### HTTP – connexion non sécurisée entre le serveur de sécurité et le client du service

- **Effet :** Connexion non sécurisée où la communication n'est pas cryptée et où aucun des partenaires de la communication ne s'authentifie. À n'utiliser que pour l'échange d'informations non sensibles ou si le serveur de sécurité et le client du service se

trouvent dans un environnement de confiance fermé, par exemple un segment de réseau local distinct.

- **Comment configurer** : Choisissez **HTTP** comme type de connexion.



Si le type de connexion HTTP est sélectionné, mais que le système d'information se connecte au serveur de sécurité via HTTPS, alors la connexion est acceptée, les serveurs de sécurité ne vérifient pas le certificat du client (même comportement qu'avec HTTPS NOAUTH).

Selon le type de connexion, l'URL que le système d'information doit utiliser pour envoyer la requête est `http://<security-server>/` ou `https://<security-server>/`. `<security-server>` doit être remplacé par l'adresse réelle du serveur de sécurité.

## 8.2. Certificats TLS internes au système d'information

**Droits d'accès** : Administrateur serveur, Responsable des services

Pour ajouter un certificat TLS interne pour un client du serveur de sécurité (requis pour les connexions HTTPS), procédez comme suit.

1. Sur la page **Clients du serveur de sécurité**, choisissez un client dans le tableau et cliquez sur l'icône **Systèmes d'information** sur cette ligne.
2. Recherchez la section **Certificats TLS internes des systèmes d'information** et cliquez sur **Ajouter**.
3. Sélectionnez un fichier de certificat sur votre ordinateur et cliquez sur **Télécharger**.

Pour supprimer un certificat TLS interne, recherchez le certificat, cliquez sur **Supprimer** et confirmez.

## 8.3. Certificat TLS interne du serveur de sécurité

**Droits d'accès** : Administrateur serveur, Responsable des services

Pour exporter le certificat TLS interne du serveur de sécurité, procédez comme suit.

1. Sur la page **Clients du serveur de sécurité**, choisissez un client dans le tableau et cliquez sur l'icône **Systèmes d'information** sur cette ligne.
2. Recherchez le certificat actuellement utilisé dans la section **Certificats TLS internes du serveur de sécurité**, cliquez sur **Exporter** et enregistrez le fichier sur votre ordinateur.

## 9. Dépannage de l'échange de messages

Pour mieux comprendre les erreurs d'échange de messages, voici un aperçu du fonctionnement de l'échange de messages via UXP.

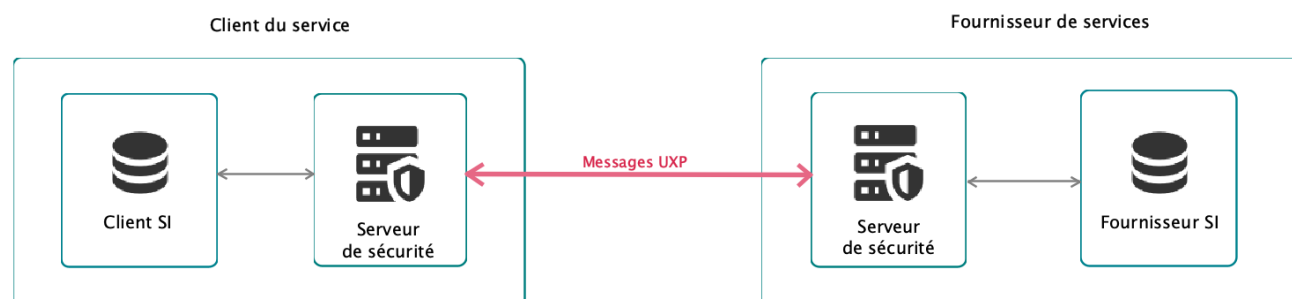


Figure 2. Diagramme montrant l'échange de messages UXP

Des erreurs peuvent se produire dans :

- le système d'information du client du service ;
- le serveur de sécurité du client du service ;
- le serveur de sécurité du fournisseur de services ;
- le système d'information du fournisseur de services.

Ces erreurs sont détectées lors de l'échange de messages. Les erreurs sont également enregistrées sur le serveur de sécurité, ce qui signifie qu'elles peuvent être consultées à partir des journaux du serveur de sécurité. Si la surveillance opérationnelle UXP est configurée pour le serveur de sécurité, les erreurs sont également collectées sur l'Elasticsearch de surveillance (voir le guide de l'utilisateur de la surveillance [\[UXP-UG-PMA\]](#) pour plus d'informations).

### 9.1. Comprendre les messages d'erreur

Les erreurs générées par les serveurs de sécurité ont une structure cohérente et contiennent des informations nécessaires au débogage. Selon que l'erreur a été provoquée par un service REST ou un service SOAP, le message d'erreur généré est présenté et structuré différemment.

#### SOAP

```
<?xml version="1.0" encoding="UTF-8"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
  <SOAP-ENV:Body>
    <SOAP-ENV:Fault>
      <faultcode>Server.ClientProxy.ServiceFailed.MissingBody</faultcode>
      <faultstring>Malformed SOAP message: body missing</faultstring>
      <faultactor />
    </SOAP-ENV:Fault>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

```

    <detail>
      <faultDetail>f31e7451-f0ac-48f6-9f05-1f0459e48eea</faultDetail>
    </detail>
  </SOAP-ENV:Fault>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>

```

- La partie initiale de l'erreur `faultcode` vous dirige vers la source de l'erreur :
  - `Server.ClientProxy` signifie que l'erreur s'est produite du côté du serveur de sécurité du client du service.
  - `Client` signifie que l'erreur s'est produite du côté du serveur de sécurité du client du service.
  - `Server.ServerProxy` signifie que l'erreur s'est produite du côté du serveur de sécurité du fournisseur de services.
- L'erreur complète `faultcode` peut être utilisée pour effectuer des recherches dans les tableaux d'erreurs ci-dessous.
- `faultstring` précise la cause plus spécifique de l'erreur.
- `faultDetail` est un identifiant unique du message d'erreur reçu. Vous pouvez l'utiliser pour trouver les entrées de journal liées au message d'erreur reçu à partir du journal du proxy (`var/log/uxp/proxy.log`).

## REST

La réponse contient le message d'erreur en texte clair :

```
Service client security server has no valid authentication certificate
```

Les en-têtes HTTP contiennent le code d'erreur (`Uxp-FaultCode`), le message d'erreur (`Uxp-FaultString`) et le détail (`Uxp-FaultDetail`).

```

Uxp-FaultCode: Server.ClientProxy.SslAuthenticationFailed
Uxp-FaultString: Service client security server has no valid authentication certificate
Uxp-FaultDetail: f31e7451-f0ac-48f6-9f05-1f0459e48eea

```

- La partie initiale de l'erreur `Uxp-FaultCode` vous dirige vers la source de l'erreur :
  - `Server.ClientProxy` signifie que l'erreur s'est produite du côté du serveur de sécurité du client du service.
  - `Client` signifie que l'erreur s'est produite du côté du serveur de sécurité du client du service.
  - `Server.ServerProxy` signifie que l'erreur s'est produite du côté du serveur de sécurité du fournisseur de services.
- L'erreur complète `Uxp-FaultCode` peut être utilisée pour effectuer des recherches dans les tableaux d'erreurs ci-dessous.
- `Uxp-FaultString` précise la cause plus spécifique de l'erreur.



- `Uxp-FaultDetail` est un identifiant unique du message d'erreur reçu. Vous pouvez l'utiliser pour trouver les entrées de journal liées au message d'erreur reçu à partir du journal du proxy (`var/log/uxp/proxy.log`).



Si vous recevez un message d'erreur qui n'utilise pas les structures de message ci-dessus, l'erreur doit provenir du système d'information du fournisseur de services. UXP renvoie tous les messages d'erreur provenant du système d'information du fournisseur de services, à condition que ces messages comportent les en-têtes UXP requis [\[UXP-PR-MESS\]](#).

## 9.2. Erreurs provenant du système d'information du client du service

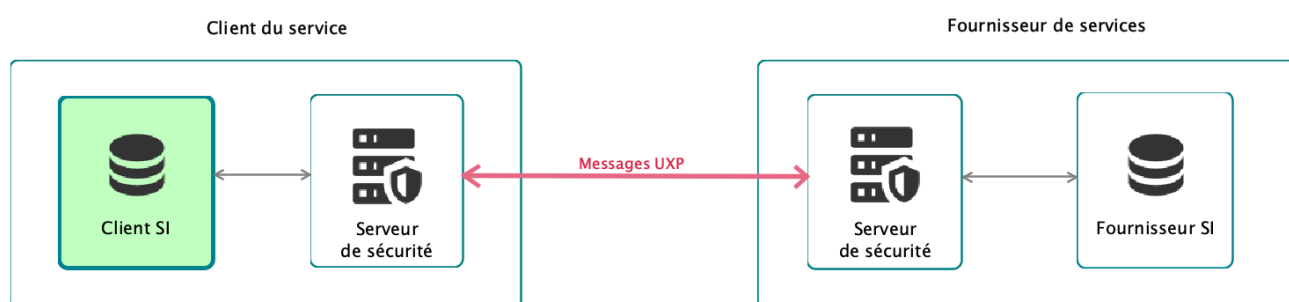


Figure 3. Cette section couvre les codes d'erreur provenant du système d'information du client du service (mis en évidence).

Toutes les erreurs suivantes proviennent du système d'information du client du service. En général, cela signifie qu'il y a un problème avec le message de demande envoyé par le système d'information du client.



Dans tous les cas suivants, l'abréviation « SS » est utilisée pour « serveur de sécurité ». Tous les codes d'erreur et messages possibles ne sont pas répertoriés ici, mais une sélection des plus courants est présentée.

### Client.InternalError

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Différents messages d'erreur possibles. Par exemple : Unexpected SOAP message	Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a> ). Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service ( <code>/var/log/uxp/proxy.log</code> ).	

### Client.InvalidContentType

Le type de contenu du message SOAP n'est pas `text/xml`, `xop/xml`, `soap/xml` ou `multipart/related`.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Invalid content type: <content-type>	Le type de contenu du message SOAP doit être text/xml, xop/xml, soap/xml ou multipart/related. Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a> ).	

### Client.InvalidHttpMethod

Le serveur de sécurité du client du service a reçu une requête utilisant une méthode HTTP non prise en charge.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Must use POST request method instead of <HTTP-method-used>	Le système d'information du client du service doit envoyer des messages de requête SOAP en utilisant la méthode HTTP POST.	
Unsupported HTTP method <HTTP-method-used>	Le système d'information du client du service doit envoyer des messages de demande REST en utilisant les méthodes HTTP HEAD, GET, DELETE, POST, PUT ou PATCH.	

### Client.InvalidSOAP

Le serveur de sécurité du client du service a reçu un message SOAP non valide.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Plusieurs messages d'erreur différents en fonction de la cause de l'erreur. Par exemple : org.xml.sax.SAXParseException; Premature end of file.	Le système d'information du client du service a envoyé un message SOAP malformé. Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a> ). Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).	

### Client.MissingBody

Le serveur de sécurité du client du service a reçu un message SOAP sans corps.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Malformed SOAP message: body missing	<p>Le système d'information du client du service a envoyé un message SOAP sans corps. Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a>).</p> <p>Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).</p>	

#### Client.MissingHeader

Le serveur de sécurité du client du service a reçu un message SOAP sans en-tête.

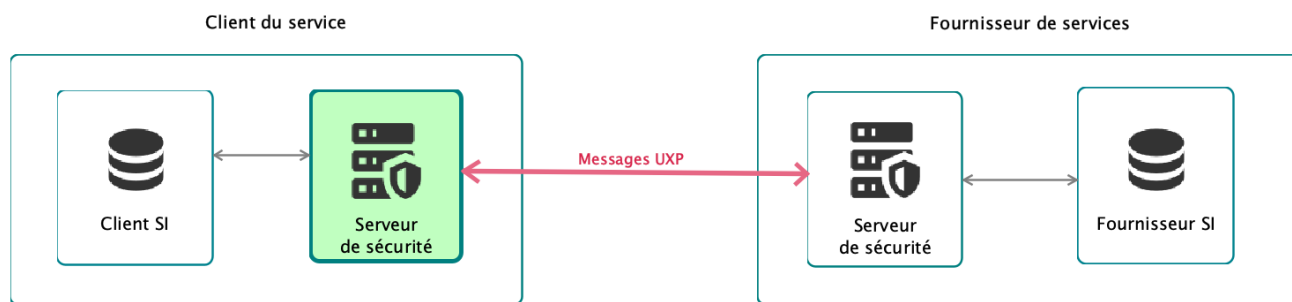
Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Malformed SOAP message: header missing	<p>Le système d'information du client du service a envoyé un message SOAP sans en-tête. Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a>).</p> <p>Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).</p>	

#### Client.MissingSOAP

Le serveur de sécurité du client du service a reçu une demande multipart, mais le premier composant de l'enveloppe MIME multipart n'est pas un message SOAP.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Request does not have SOAP message	<p>Le système d'information du client du service a envoyé une enveloppe MIME multipart dont le premier composant n'est pas un message SOAP. Assurez-vous que le message est correctement formaté (pour plus d'informations, voir <a href="#">[UXP-PR-MESS]</a>).</p> <p>Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).</p>	

## 9.3. Erreurs provenant du serveur de sécurité du client du service



**Figure 4.** Cette section couvre les codes d'erreur provenant du serveur de sécurité du client du service (mis en évidence).

Toutes les erreurs suivantes proviennent du serveur de sécurité du client du service, dans le proxy du client. Cela signifie que la plupart de ces erreurs peuvent être résolues par l'administrateur du serveur de sécurité ou le Responsable des services du client du service.



Dans tous les cas suivants, l'abréviation « SS » est utilisée pour « serveur de sécurité ». Tous les codes d'erreur et messages possibles ne sont pas répertoriés ici, mais une sélection des plus courants est présentée.

## Server.ClientProxy.BadRequest

La requête REST n'a pas d'en-tête de requête spécifique à UXP (Uxp-Client et Uxp-Service) ou les valeurs de l'en-tête sont invalides.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Différents messages d'erreur possibles. Par exemple : Uxp-Service header value 'SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/' does not contain all required service identifier parts	Lors de la construction d'une demande de service, assurez-vous que les six (ou cinq lorsque le service n'a pas de version) parties de l'identifiant du service sont incluses dans l'en-tête de la demande Uxp-Service (par exemple, EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE/SERVICE_VERSION) (voir UG-SS Section <a href="#">Envoi de demandes à une API REST</a> ).	

## Server.ClientProxy.UnknownMember

La demande est adressée à un sous-système ou à un service UXP inconnu.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Could not find addresses for service provider 'SERVICE:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT/EXAMPLE_SERVICE'	Le service n'est pas enregistré sur le SS du fournisseur de services. Vérifiez que le code de service figurant dans le message de demande est le même que le code enregistré sur le SS du fournisseur de services.	
Client 'SUBSYSTEM:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT' not found	Contactez l'administrateur SS du client du service	Le sous-système n'est pas enregistré dans le SS du client du service. Enregistrez le sous-système (voir la section UG-SS <a href="#">Ajouter un client au serveur de sécurité</a> )

### Server.ClientProxy.ServiceFailed.InternalError

Le SS du client du service a connu une erreur interne qui a entraîné l'échec de la demande.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Plusieurs messages d'erreur différents en fonction de la cause de l'erreur.	Les causes peuvent être diverses. Consultez le journal du proxy pour plus de détails ( <code>var/log/uxp/proxy.log</code> ).	

### Server.ClientProxy.SslAuthenticationFailed

Il y a un problème avec l'authentification SSL.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Service client security server has no valid authentication certificate	Contactez l'administrateur SS du client du service	<p>Le système de sécurité du client du service n'a pas de certificat d'authentification valide. Assurez-vous que toutes les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Le SS possède au moins un certificat d'authentification (voir la section UG-SS <a href="#">Ajouter une clé et un certificat d'authentification pour le serveur de sécurité</a>).</li> <li>• Le certificat se trouve sur un jeton qui est connecté.</li> <li>• Le certificat est enregistré (voir UG-SS Section <a href="#">États d'enregistrement des certificats d'authentification</a>).</li> <li>• Le certificat est actif (voir section UG-SS <a href="#">Activer et désactiver des certificats</a>).</li> <li>• La réponse OCSP du certificat est bonne (voir UG-SS Section <a href="#">Validité du certificat</a>).</li> </ul>

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Service provider security server has no valid authentication certificate	Contactez l'administrateur SS du <b>fournisseur de services</b>	<p>Le SS du fournisseur de services n'a pas de certificat d'authentification valide. Assurez-vous que toutes les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Le SS possède au moins un certificat d'authentification (voir la section <a href="#">UG-SS Configurer une clé et un certificat d'authentification pour le serveur de sécurité</a>).</li> <li>• Le certificat se trouve sur un jeton qui est connecté.</li> <li>• Le certificat est enregistré (voir UG-SS Section <a href="#">États d'enregistrement des certificats d'authentification</a>).</li> <li>• Le certificat est actif (voir section UG-SS <a href="#">Activer et désactiver des certificats</a>).</li> <li>• La réponse OCSP du certificat est bonne (voir UG-SS Section <a href="#">Validité du certificat</a>).</li> </ul>
Client <SUBSYSTEM:EE_DEV/GOV/EXAMPLE_ORGANIZATION/EXAMPLE_DEPARTMENT> specifies HTTPS but did not supply TLS certificate	Le certificat TLS du système d'information du client du service doit être téléchargé sur le serveur SS du client du service (voir la section <a href="#">Communication avec les systèmes d'information des clients</a> ).	

## Server.ClientProxy.CannotCreateSignature

La signature du message au nom du client du service échoue.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Failed to get client signing context for member 'EE_DEV/GOV/EXAMPLE_ORGANIZATION': Member has no usable certificates	Contactez l'administrateur SS du client du service	<p>Le sous-système du client du service ne dispose pas d'un certificat de signature valide. Assurez-vous que les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Il existe au moins un certificat de signature pour le membre auquel appartient le sous-système (voir la section UG-SS <a href="#">Configurer une clé et un certificat de signature pour un client du serveur de sécurité</a>).</li> <li>• Le certificat se trouve sur un jeton qui est connecté.</li> <li>• Le certificat est actif (voir section UG-SS <a href="#">Activer et désactiver des certificats</a>).</li> <li>• La réponse OCSP du certificat est bonne (voir UG-SS Section <a href="#">Validité du certificat</a>).</li> </ul>

### Server.ClientProxy.IOError

Les erreurs d'E/S peuvent se produire dans différentes situations liées à la lecture ou à l'écriture dans le système de fichiers.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
No space left on device	Contactez l'administrateur SS du client du service	Assurez-vous que le SS du client du service dispose d'un espace disque libre. Si le disque est partitionné, assurez-vous que les partitions concernées disposent d'espace libre.

### Server.ClientProxy.LoggingFailed.TimestamperFailed

L'horodatage échoue dans le journal des messages du SS du client du service.



Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Cannot timestamp messages: no timestamping services configured	Contactez l'administrateur SS du client du service	<p>Assurez-vous que les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Le SS du client du service peut se connecter au service d'horodatage. Vérifiez que tous les pare-feu sont correctement configurés.</li> <li>• Le service d'horodatage est disponible. Consultez le journal du proxy (/var/log/uxp/proxy.log) pour plus de détails.</li> </ul>

### Server.ClientProxy.OutdatedGlobalConf

La configuration globale a expiré.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Global configuration is expired	Contactez l'administrateur SS du client du service	<p>Le SS du client du service ne peut pas télécharger la configuration globale à partir du serveur de registre. Consultez le journal de configuration du client (/var/log/uxp/configuration_client.log) pour plus de détails.</p>

### Server.ClientProxy.NetworkError

Il y a un problème de connexion au réseau.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Could not connect to target host (https://<service-provider-security-server>:5500)	Contactez l'administrateur SS du client du service	Le SS du client du service ne peut pas se connecter au SS du fournisseur de services. Assurez-vous que le pare-feu est correctement configuré des deux côtés : le SS du client du service doit autoriser le trafic sortant vers le port 5500 du SS du fournisseur de services, et le SS du fournisseur de services doit autoriser le trafic entrant vers les ports 5500.
Name or service not known. No address associated with hostname.	Contactez l'administrateur SS du <b>fournisseur de services</b>	Le SS du fournisseur de services est introuvable parce qu'il est enregistré avec le mauvais FQDN.

## 9.4. Erreurs provenant du serveur de sécurité du fournisseur de services

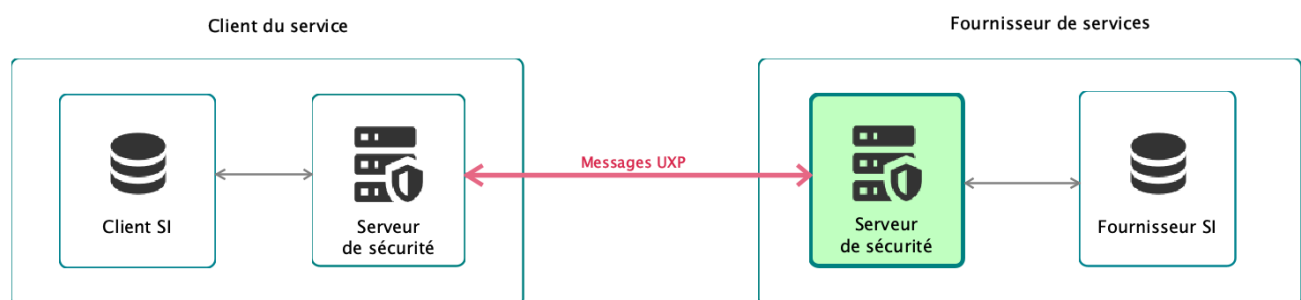


Figure 5. Cette section couvre les codes d'erreur provenant du serveur de sécurité du fournisseur de services (mis en évidence).

Tous les codes d'erreur suivants proviennent du serveur de sécurité du fournisseur de services, dans le processus de proxy du serveur. Cela signifie que ces erreurs peuvent être résolues par l'administrateur du serveur de sécurité ou le Responsable des services du fournisseur de services.



Dans tous les cas suivants, l'abréviation « SS » est utilisée pour « serveur de sécurité ». Tous les codes d'erreur et messages possibles ne sont pas répertoriés ici, mais une sélection des plus courants est présentée.

### Server.ServerProxy.AccessDenied

Le sous-système client du service n'a pas le droit d'accéder au service UXP.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Request is not allowed: SERVICE:EE_DEV/GOV/EXAM PLE_ORGANIZATION/EXAMPL E_DEPARTMENT/EXAMPLE_SE RVICE	Le SS du fournisseur de services doit accorder des droits d'accès au service au sous-système client du service. Voir la section <a href="#">Droits d'accès</a> .	

### Server.ServerProxy.ServiceFailed.MissingHeaderField

Un en-tête UXP obligatoire est manquant dans le message SOAP renvoyé par le système d'information du fournisseur de services.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Malformed SOAP message: header missing	Le système d'information du fournisseur de services doit renvoyer tous les en-têtes UXP obligatoires. Voir <a href="#">[UXP-PR-MESS]</a> pour plus de détails.	

### Server.ServerProxy.ServiceFailed.InvalidSoap

Le serveur de sécurité du fournisseur de services a reçu un message SOAP non valide.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Plusieurs messages d'erreur différents en fonction de la cause de l'erreur. Par exemple : org.xml.sax.SAXParseException; Premature end of file.	Le système d'information du fournisseur de services a renvoyé un message SOAP malformé. Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du fournisseur de services (/var/log/uxp/proxy.log).	

### Server.ServerProxy.UnknownService

Le SS du fournisseur de services ne dispose pas d'un service avec le code de service fourni par le client du service dans le message de demande.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Unknown service: SERVICE:EE_DEV/GOV/EXAM PLE_ORGANIZATION/EXAMPL E_DEPARTMENT/EXAMPLE_SE RVICE	Assurez-vous que le code de service dans le message de demande correspond à un service du côté du fournisseur de services.	

## Server.ServerProxy.ServiceFailed.HttpError

Le SS du fournisseur de services n'a pas pu se connecter au système d'information du fournisseur de services.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Raison pour laquelle la connexion a échoué. Par exemple : Server responded with error 403: Forbidden	Assurez-vous que le SS du fournisseur de services est autorisé à se connecter au système d'information du fournisseur de services et que la connexion est correctement configurée. Pour plus d'informations sur la configuration de la connexion, voir la section <a href="#">Communication avec les systèmes d'information des clients</a> . Pour plus d'informations sur l'erreur, consultez le journal proxy SS du fournisseur de services (/var/log/uxp/proxy.log).	

## Server.ServerProxy.SslAuthenticationFailed

L'authentification SSL a échoué entre le SS du fournisseur de services et le système d'information du fournisseur.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Server certificate is not trusted	L'option « Vérifier le certificat TLS » est sélectionnée dans la configuration du service, mais le certificat du système d'information du fournisseur de services n'a pas été téléchargé sur le SS du fournisseur de services. Téléchargez le certificat du système d'information du fournisseur de services sur le SS (voir la section <a href="#">Communication avec les systèmes d'information des clients</a> ).	

## Server.ServerProxy.ServiceFailed.InternalError

Le SS du fournisseur de services a connu une erreur interne qui a entraîné l'échec du traitement des messages.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Connection pool shut down	Contactez l'administrateur SS du fournisseur de services	Le SS du fournisseur de services ne peut pas accéder à sa base de données. Consultez le journal du proxy (/var/log/uxp/proxy.log) et le journal Postgres (/var/log/postgresql/) pour plus de détails.

## Server.ServerProxy.CannotCreateSignature

La signature du message au nom du fournisseur de services échoue.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Failed to get client signing context for member 'EE_DEV/GOV/EXAMPLE_ORGANIZATION': Member has no usable certificates	Contactez l'administrateur SS du fournisseur de services	<p>Le sous-système du fournisseur de services n'a pas de certificat de signature valide. Assurez-vous que les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> <li>• Il existe au moins un certificat de signature pour le membre auquel appartient le sous-système (voir la section UG-SS <a href="#">Configurer une clé et un certificat de signature pour un client du serveur de sécurité</a>).</li> <li>• Le certificat se trouve sur un jeton qui est connecté.</li> <li>• Le certificat est actif (voir section UG-SS <a href="#">Activer et désactiver des certificats</a>).</li> <li>• La réponse OCSP du certificat est bonne (voir UG-SS Section <a href="#">Validité du certificat</a>).</li> </ul>

`Server.ServerProxy.LoggingFailed.TimestamperFailed`

L'horodatage est défaillant dans le journal des messages du SS du fournisseur de services.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Cannot timestamp messages: no timestamping services configured	Contactez l'administrateur SS du fournisseur de services	Vous devez configurer un service d'horodatage pour le SS du fournisseur de service (voir section UG-SS <a href="#">Services d'horodatage</a> ).

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Cannot timestamp messages	Contactez l'administrateur SS du fournisseur de services	<p>Même si un service d'horodatage est configuré (voir le message d'erreur précédent), l'horodatage peut toujours échouer. Les problèmes suivants peuvent survenir :</p> <ul style="list-style-type: none"> <li>• Il y a un problème du côté du service d'horodatage et le service n'est pas disponible. Consultez le journal du proxy (<code>var/log/uxp/proxy.log</code>) pour plus de détails.</li> <li>• Le SS du fournisseur de services ne peut pas se connecter au service d'horodatage. Assurez-vous que les pare-feu et les ports sont correctement configurés pour le service SS et le service d'horodatage.</li> </ul>

## Server.ServerProxy.OutdatedGlobalConf

La configuration globale du SS du fournisseur de services a expiré et le SS ne peut pas en télécharger une nouvelle.

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Global configuration is expired	Contactez l'administrateur SS du fournisseur de services	<p>Essayez de redémarrer le processus du client de configuration <code>\$ systemctl restart uxp-confclient</code>. Il est possible que le SS du fournisseur de services ne puisse pas se connecter au serveur de registre pour télécharger la configuration globale. Assurez-vous que la configuration du pare-feu est correcte des deux côtés. Voir le journal du client de configuration pour plus de détails (<code>/var/log/uxp/configuration_client.log</code>).</p>

# 10. API de gestion

---

## 10.1. Rest API

Le logiciel Serveur de sécurité vous permet de récupérer et de modifier la configuration du serveur par programmation via une API REST.

### 10.1.1. API d'administration du serveur de sécurité

L'API d'administration est utilisée pour la configuration et la gestion générale du serveur de sécurité. La documentation de l'API est disponible à l'adresse suivante :

```
https://<security-server>:4000/api/v1/openapi-ui
```

### 10.1.2. API du fournisseur d'identité

L'API du fournisseur d'identité est utilisée pour gérer et authentifier/autoriser les utilisateurs du serveur de sécurité. La documentation de l'API est disponible à l'adresse suivante :

```
https://<security-server>:4000/auth-api/v1/openapi-ui
```

# Annexe A: Notes de mise à jour

---

## 1.25.0 (11.2025)

- Ajout de la prise en charge de la mutualisation, qui permet à plusieurs membres UXP de partager un serveur de sécurité. Les utilisateurs peuvent désormais voir leur accès limité aux données de leur membre spécifique. Par défaut, la mutualisation est désactivée et peut être activée par le biais d'un indicateur de fonctionnalité. Contactez l'Autorité de gouvernance pour plus de détails.
- Présentation de l'Outil de diagnostic, une fonction conçue pour aider les administrateurs de serveurs de sécurité à identifier rapidement les problèmes potentiels en analysant les journaux du système à la recherche d'avertissements et d'erreurs. L'outil :
  - Affiche une liste concise des problèmes détectés dans l'interface utilisateur du serveur de sécurité.
  - Fournit un rapport système détaillé comprenant des informations sur le serveur, la configuration Nginx et UXP, et les fichiers journaux. Ce rapport peut être envoyé au service d'assistance en cas de besoin.
  - Examine les journaux pour y trouver des modèles d'avertissement et d'erreur courants.
  - Aide les administrateurs à identifier les problèmes sans avoir recours à SSH ou à des outils externes.
- Ajout d'un script de vérification post-installation (`uxp-installation-verification`) qui vérifie l'installation des paquets, l'état des services, la connectivité de la base de données et les rôles des utilisateurs, en fournissant des informations claires sur les réussites et les échecs. Le script répertorie également les adresses accessibles de l'interface utilisateur du serveur de sécurité et valide les connexions PostgreSQL, garantissant ainsi un bilan de santé complet après l'installation. Cela permet d'améliorer la validation post-déploiement et de réduire le dépannage manuel.
- Ajout de la prise en charge des clés EdDSA (Ed25519 et Ed448) sur les jetons logiciels et matériels qui prennent en charge le mécanisme CKM\_EDDSA\_PH. Notez que les versions 1.24 et 1.25 du Serveur de sécurité UXP sont incompatibles avec l'utilisation de clés EdDSA. Veillez à ce que les versions soient cohérentes ou évitez d'utiliser des clés EdDSA dans des environnements mixtes.
- Ajout d'une fonctionnalité de recherche à la boîte de dialogue de limitation du débit. Afin d'améliorer la convivialité dans les instances de grande taille, la boîte de dialogue de limitation du débit prend désormais en charge la recherche dynamique lors de la sélection de sous-systèmes ou de groupes. Les utilisateurs peuvent filtrer par nom ou par numéro d'identification pour trouver et sélectionner rapidement le bon sujet.
- Changements liés à la surveillance locale :
  - Les versions 9.x d'Elasticsearch et de Kibana sont désormais prises en charge.
  - La prise en charge d'Elasticsearch et de Kibana 7.x a été entièrement supprimée.
  - Un nouveau paramètre de configuration, `enable_update_existing_triggers`, a



été ajouté à `monitor-agent.ini`. Cela permet d'activer ou de désactiver les mises à jour des déclencheurs existants dans le modèle Zabbix UXP, ce qui permet d'éviter les écrasements involontaires.

- Changements liés à la gestion des utilisateurs :
  - Les exigences suivantes relatives aux noms d'utilisateur aux serveurs de sécurité ont été appliquées. Les utilisateurs existants peuvent continuer à accéder au système.
    - Les noms d'utilisateur sont désormais limités à 30 caractères.
    - Caractères autorisés dans les noms d'utilisateur : lettres (a-z), chiffres, caractères de soulignement (`_`), tirets (`-`), points (`.`) et le symbole at (`@`).
- Augmentation de la RAM minimale recommandée de 4 Go à 6 Go.
- La fonction d'authentification automatique du jeton logiciel permet désormais de se connecter automatiquement au jeton après le démarrage de Serveur de sécurité UXP et de Serveur de registre UXP, ce qui permet un fonctionnement ininterrompu après les redémarrages. Cette fonction n'est disponible que lorsqu'elle est fournie par le service d'assistance sur demande et installée explicitement, car elle implique des considérations qui doivent être prises en compte au préalable.
- Java Runtime Environment est mis à jour vers la version 21. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Diverses corrections et améliorations mineures ont été apportées.

### 1.24.0 (09.2025)

- La mise à jour du serveur de sécurité vers une version plus récente fait désormais l'objet d'un document distinct : Guide de mise à jour de Serveur de sécurité UXP (UXP-UPG-SS).
  - Veuillez à lire le guide de mise à jour pour savoir comment passer de la version 1.21 à la version 1.24, car beaucoup de choses ont changé depuis la version 1.21 (lisez également les notes de mise à jour de la version 1.22.7). L'administrateur doit effectuer certains changements pendant la mise à jour, par exemple migrer les utilisateurs vers le nouveau système de gestion des utilisateurs et éventuellement résoudre des conflits dans la configuration de la surveillance.
  - Le guide de mise à jour explique également comment passer d'une ancienne version à la dernière version du serveur de sécurité.
- Ubuntu 24.04 LTS est désormais une plate-forme prise en charge (et recommandée). Ubuntu 22.04 LTS est désormais une plate-forme minimale prise en charge. Mettez d'abord votre serveur à jour vers la version 1.24 comme décrit dans le guide de mise à jour du Serveur de sécurité (UXP-UPG-SS) et suivez ensuite le guide de mise à jour d'Ubuntu 24.04 (UXP-UPG-UB24) pour savoir comment mettre à jour la version d'Ubuntu.
- Zabbix 7.0 LTS est maintenant prise en charge. La prise en charge de Zabbix 6.0 LTS est obsolète et sera supprimée dans une prochaine version.
- La prise en charge de la version 7.x d'Elasticsearch/Kibana est obsolète et sera supprimée dans une prochaine version.

- Changements liés à la gestion des utilisateurs :
  - Ajout de l'option permettant d'utiliser les utilisateurs Ubuntu et l'authentification via l'interface PAM pour assurer la compatibilité ascendante. L'interface PAM sera prise en charge dans plusieurs versions à venir pour des raisons de compatibilité ascendante, mais elle sera finalement supprimée lorsque le gestionnaire des utilisateurs UXP évoluera.
  - Le serveur de sécurité bloque désormais temporairement les utilisateurs du gestionnaire des utilisateurs Ubuntu après un trop grand nombre de tentatives de connexion infructueuses, afin de prévenir les attaques par force brute. Vous pouvez configurer le nombre de tentatives autorisées et le temps de verrouillage. Consultez la section « Mécanisme de protection de connexion Ubuntu » dans le guide d'utilisation.
  - Application d'un nombre minimum de caractères au mot de passe de l'administrateur du serveur ajouté lors de l'installation du serveur. Le mot de passe doit comporter au moins 12 caractères.
  - Si tous les administrateurs serveur sont bloqués hors de l'interface utilisateur du serveur, les scripts de gestion des utilisateurs de l'interface de gestion peuvent être utilisés pour ajouter de nouveaux administrateurs de serveur et bloquer les utilisateurs existants. Les événements sont enregistrés dans le journal d'audit.
  - Amélioration des messages de fin de session.
  - Pour des raisons de sécurité, interdiction faite à l'administrateur serveur de réinitialiser son propre mot de passe.
  - Ajout de scripts pour la sauvegarde et la restauration de la base de données des utilisateurs, en plus de la sauvegarde de la configuration du serveur. Consultez la section « Sauvegarde et restauration » du guide d'utilisation.
- Ajout d'une option de cryptage pour la sauvegarde de la configuration du serveur.
- Changements liés à la surveillance locale :
  - Paramètres de configuration unifiée pour l'agent de surveillance du proxy :
    - Paramètres suivants dans les sections [proxy-monitoring-agent] et [op-monitor]] de proxy-monitor-agent.ini renommés :
      - port → listen-port,
      - params-collecting-interval-seconds → data-collection-interval-seconds,
      - sending-interval-seconds → zabbix-send-interval-seconds,
      - keep-records-for-days → retain-records-for-days.
    - Déplacement du paramètre send\_interval\_seconds de la section [elasticsearch] de la section monitor-agent.ini vers la section [proxy-monitoring-agent] de la section proxy-monitor-agent.ini et renommé elasticsearch-send-interval-seconds.
    - Ajout de la valeur par défaut uxp-security-servers au groupe d'hôtes des serveurs de sécurité (host\_group) dans Zabbix.

- Amélioration du modèle Zabbix UXP Security Server by PMA par l'ajout d'un nouveau service UXP `uxp-messagelog-timestamper`.
- Par défaut, le client HTTP Elasticsearch vérifie désormais le nom d'hôte du serveur Elasticsearch pendant l'établissement de la connexion TLS (lors de l'utilisation du schéma `https`).
- L'horodatage par lots est désormais effectué par un service système UXP distinct `uxp-messagelog-timestamper`.
  - Zabbix dispose désormais d'un déclencheur en cas de panne de `uxp-messagelog-timestamper`.
- La rétrocompatibilité du répondeur OCSP avec les serveurs de sécurité fonctionnant avec les versions 1.17 ou inférieures a été supprimée. Le répondeur OCSP n'accepte plus de demandes extérieures et le port 5577 doit être fermé aux connexions entrantes. Tous les serveurs de sécurité de la version 1.17 ou inférieure doivent être mis à jour vers une version plus récente.
- Mise à jour des bibliothèques et des composants tiers pour garantir la sécurité du système.
- Diverses corrections et améliorations mineures ont été apportées.

### 1.22.7 (05.2025)

- Un système de gestion des utilisateurs basé sur le Web a été ajouté au serveur de sécurité pour remplacer la gestion des utilisateurs basée sur Ubuntu. Le système de gestion des utilisateurs UXP sera le système par défaut pour tous les nouveaux serveurs de sécurité. Pour en savoir plus, consultez la section sur la mise à jour de la version 1.21 à la version 1.24 dans le guide de mise à jour du serveur de sécurité UXP (UXP-UPG-SS).
- Le Gestionnaire des utilisateurs UXP introduit les changements suivants dans la gestion des utilisateurs :
  - L'Administrateur serveur est maintenant responsable de la gestion des utilisateurs.
  - Les mots de passe doivent comporter au moins 12 caractères.
  - Les utilisateurs doivent changer leur mot de passe lors de leur première connexion pour accéder au serveur de sécurité.
  - Les utilisateurs peuvent modifier leur propre mot de passe.
  - Les utilisateurs peuvent consulter leurs propres rôles.
  - L'Administrateur serveur peut bloquer des utilisateurs.
  - Le serveur de sécurité bloque désormais temporairement les utilisateurs après un trop grand nombre de tentatives de connexion infructueuses afin d'empêcher les attaques par force brute.
    - La valeur par défaut est de 5 tentatives et le verrouillage dure 15 minutes.
    - Vous pouvez configurer le nombre de tentatives autorisées et la durée du verrouillage. Consultez la section « Mécanisme de protection de la connexion » dans le guide d'utilisation.

- Le rôle de Responsable des clés a été ajouté afin d'accorder des privilèges uniquement pour la gestion des clés et des certificats, indépendamment de l'administration générale du serveur.
  - Le rôle d'Administrateur de services a été renommé en Responsable des services pour s'aligner sur le nom du rôle de Responsable des clés.
- Vérificateur UXP fait désormais partie du serveur de sécurité et a été visuellement mis à jour pour correspondre au langage de conception du serveur de sécurité.
  - Suivez le lien « Messages » dans le menu latéral. Le lien apparaît lorsque l'utilisateur dispose des privilèges d'Auditeur de transactions.
  - Le vérificateur permet désormais de télécharger les certificats CA et TSA à partir de la signature.
  - Pour en savoir plus sur Vérificateur UXP, consultez le guide de l'Auditeur de transactions (UXP-UG-SSAUDIT).
  - Si des problèmes de mémoire surviennent lors de la vérification et de l'archivage des messages, consultez la section « Erreur de mémoire insuffisante du vérificateur ou de l'archiveur de journaux de messages » du guide d'utilisation pour savoir comment calculer et allouer de la mémoire supplémentaire pour les services système.
- Changements relatifs aux clés et aux certificats :
  - Les pages Certificats de serveur et Certificats de signature ont été fusionnées en une seule page Clés et certificats.
  - Les clés et certificats du membre ont été déplacés de la page Détails du sous-système vers une nouvelle page Clés du membre.
  - Ajout d'une option permettant d'ajouter des jetons logiciels supplémentaires. Les jetons logiciels supplémentaires ne peuvent être utilisés que pour stocker les clés de signature. Les clés d'authentification doivent être conservées sur le jeton logiciel 0.
  - Chaque jeton doit maintenant avoir un membre propriétaire. Tous les jetons existant avant la version 1.22.7 seront attribués au propriétaire du serveur après la mise à jour.
  - En plus d'alerter sur les certificats expirés, le serveur de sécurité affiche désormais un avertissement sur les certificats qui sont sur le point d'expirer.
    - L'avertissement apparaît un mois avant l'expiration.
    - Le seuil est configurable à l'aide du paramètre système `common.expiration-warning-threshold-days`.
  - Lors du téléchargement de certificats à partir du serveur, l'extension du certificat est désormais `.cer` au lieu de `.pem`.
  - Lors du téléchargement des CSR à partir du serveur, le format de fichier par défaut est désormais DER avec l'extension `.p10`.
  - Lors de la génération d'un certificat TLS interne de serveur de sécurité, le serveur ajoute ses adresses à l'extension `subjectAlternativeName`.
  - Lors de la génération des CSR, les champs DN de l'Objet sont désormais limités à 64 caractères chacun, conformément à la norme.

- Le serveur de sécurité affiche désormais dans l'interface utilisateur les clés de configuration qui n'ont pas de certificats ou de CSR.
- Changements liés à l'échange de messages :
  - Ajout d'une option permettant d'activer la suppression automatique des métadonnées afin de libérer de l'espace sur le disque.
    - Pour en savoir plus, consultez la section « Configurer la durée de vie du journal des messages » du guide d'utilisation.
  - Ajout d'une méthode alternative pour choisir les services d'horodatage pendant le processus d'horodatage : `round-robin`.
    - La stratégie `round-robin` répartit les demandes d'horodatage du serveur de sécurité entre tous les fournisseurs de services choisis.
    - Par défaut, la stratégie basée sur l'ancien ordre est utilisée. Utilisez le paramètre système `message-log.timestamp-provider-round-robin` pour activer la stratégie `round-robin`.
  - Ajout d'un nouveau paramètre système `proxy.signature-timestamp-required` pour activer la vérification sur le serveur de sécurité du destinataire du message que le serveur de sécurité de l'expéditeur a utilisé l'horodatage immédiat. La vérification ne doit être utilisée que lorsque l'horodatage immédiat est une pratique convenue avec les partenaires de communication ou dans l'ensemble de l'instance UXP.
  - Ajout d'un nouveau paramètre système `proxy.max-retained-soap-message-size-bytes` — permettant de définir la taille maximale en octets des messages SOAP conservés pour l'enregistrement (la valeur par défaut est de 5 Mo).
  - Lorsque la stratégie `round-robin` est utilisée pour choisir entre plusieurs serveurs de sécurité d'un fournisseur de services, le serveur de sécurité du client ignore désormais le serveur de sécurité d'un fournisseur qui ne répond pas pendant un court laps de temps. Cela permet d'éviter de contacter un serveur probablement indisponible.
- Changements liés à la surveillance locale :
  - Ajout de la prise en charge de la grappe HA native de Zabbix.
  - Ajout de la prise en charge de la découverte automatique Zabbix.
  - Suppression de la prise en charge de la version 5.0 LTS de Zabbix.
  - Amélioration du modèle UXP Security Server by PMA Zabbix :
    - Nouveaux éléments ajoutés :
      - `uxp.certs.auth.expire_timestamp`
      - `uxp.certs.auth.ocsp_not_good`
      - `uxp.certs.sign.expire_timestamp`
      - `uxp.certs.sign.ocsp_not_good`
      - `uxp.gc.download_timestamp`
      - `uxp.proc.uxp_identity_provider_rest_api.status`

- `uxp.proc.uxp_identity_provider_rest_api.uptime`
- `uxp.proc.uxp_verifier_rest_api.status`
- `uxp.proc.uxp_verifier_rest_api.uptime`
- `uxp.system.jvm.operable`
- `uxp.system.sw.uxp_identity_provider_rest_api.version`
- De nouveaux déclencheurs ont été ajoutés :
  - Le certificat d'authentification expire dans moins de 30 jours
  - L'état de la réponse OCSP du certificat d'authentification n'est pas « Bon »
  - Le certificat de signature expire dans moins de 30 jours
  - L'état de la réponse OCSP du certificat de signature n'est pas « Bon »
  - La dernière CG valide a été téléchargée il y a plus d'une heure
  - [nginx | postgresql] est en panne
  - [uxp-confclient | uxp-identity-provider-rest-api | uxp-messagelog-archiver | uxp-monitor | uxp-ocsp-cache | uxp-proxy | uxp-securityserver-rest-api | uxp-verifier-rest-api] is down
  - Le taux de messages UXP dépasse le seuil
- Mise à jour des valeurs par défaut des paramètres de configuration de Zabbix :
  - `conf_api_path` : est passé de `/zabbix/api_jsonrpc.php` à `/api_jsonrpc.php`
  - `conf_api_port` : est passé de 80 à 8080
- Amélioration des données de surveillance opérationnelle en faisant la distinction entre les messages SOAP et REST.
- Ajout d'une nouvelle demande de surveillance `getSecurityServerOperationalDataStats` pour interroger les statistiques des données de surveillance opérationnelle.
- Le Guide de haute disponibilité du serveur de sécurité (UXP-UG-SSHA) comprend désormais un guide d'exportation et d'importation de la configuration étape par étape, une vue d'ensemble de l'ajout et de la suppression des nœuds de la grappe, ainsi qu'une section de dépannage.
- Changements liés à l'API de gestion :
  - Les clés API sont désormais obsolètes. Utilisez plutôt le flux d'informations d'identification client machine-à-machine OAuth. Les étapes sont décrites dans la documentation de l'API du fournisseur d'identité.
  - La documentation de l'API de gestion du serveur de sécurité inclut désormais les codes d'erreur.
  - Une nouvelle méthode d'autorisation est désormais disponible dans Swagger UI : Flux de codes d'autorisation OAuth 2.0 avec clé de preuve pour l'échange de codes (PKCE).

- Changements liés aux dispositifs de création de signatures externes :
  - Ajout d'une option permettant d'utiliser les clés existantes sur les dispositifs de création de signature avec le serveur de sécurité. Vous pouvez soit importer la référence de la clé et le certificat d'un dispositif vers le serveur de sécurité, soit importer uniquement la référence de la clé et télécharger le certificat à partir d'un fichier.
  - Suppression de l'option permettant de modifier, après la création d'un dispositif, les paramètres de celui-ci qui peuvent interrompre la connexion avec ce périphérique.
  - Il est désormais possible de supprimer des jetons matériels avec des clés du serveur de sécurité. Les clés et les certificats qui se trouvent sur le dispositif physique restent sur celui-ci. Les certificats et les CSR qui se trouvent uniquement dans la configuration du serveur seront supprimés.
  - Lors de la connexion d'un dispositif de création de signature PKCS#11, il est possible de choisir la source de l'identité du jeton : l'identifiant de l'emplacement ou le numéro de série. Choisissez la valeur stable sur le dispositif afin que le serveur sache quel jeton physique correspond au jeton sur le serveur.
- La période de validité des certificats TLS internes générés est passée de 20 à 100 ans.
- Il est désormais possible de fermer les erreurs affichées en haut de l'interface utilisateur (par exemple, les avertissements relatifs à l'expiration des certificats) pour une session d'utilisateur.
- Ajout d'un nouveau paramètre système, `rsa-allowed`, qui peut être utilisé pour interdire l'utilisation de clés RSA sur le serveur de sécurité.
- Les journaux d'audit du serveur de sécurité enregistrent désormais les tentatives d'accès non autorisé aux ressources, en plus des tentatives de modification.
- La plate-forme minimale prise en charge est désormais Ubuntu 22.04 LTS.
- Mise à jour des bibliothèques et des composants tiers pour garantir la sécurité du système.
- Diverses corrections et améliorations mineures ont été apportées.

### 1.21.9 (05.2025)

- Les modules PKCS#11 sont réinitialisés en cas de certaines erreurs dans les opérations sur les jetons afin de corriger les pilotes qui ne répondent pas.

### 1.21.8 (04.2025)

- Correction d'un problème de double encodage des espaces blancs dans les segments de chemin d'appel de l'API REST transférés.
- Ajout de la possibilité de définir des limites de débit pour les services SOAP et les API REST.

### 1.21.7 (09.2024)

- Correction de l'échec de la vérification de la chaîne de certificats d'authentification lorsque l'autorité de certification intermédiaire est utilisée comme service de certification approuvé de premier niveau.



- Correction d'un problème lié à l'absence de nom alternatif du sujet dans le certificat d'authentification interne du serveur de sécurité.

### 1.21.6 (08.2024)

- Validation plus souple de l'exactitude des URL WSDL dans l'API du serveur de sécurité
- Meilleure gestion de l'erreur CKR\_KEY\_HANDLE\_INVALID pour les jetons PKCS11
- La langue du sélecteur de date du vérificateur dépend désormais de la langue du navigateur
- Correction des demandes simultanées provenant du proxy vers l'agent de surveillance qui s'interrompait de manière inattendue.

### 1.21.5 (07.2024)

- Utilisation de l'en-tête HTTP « content-length » au lieu de « transfer-encoding: chunked » lors du transfert des demandes API REST.
- Correction de l'épuisement du pool de connexions HTTP du serveur de sécurité dans certaines circonstances
- Autorisation du caractère « & » dans les chemins de base de l'API REST
- Problème de compatibilité ascendante résolu entre les anciens et les nouveaux serveurs de sécurité lié à l'en-tête HTTP « x-original-content-type ».
- Autorisation du caractère « . » dans la version et le nom du service pour une compatibilité ascendante

### 1.21.4 (05.2024)

- Ajout de la prise en charge de la localisation.

### 1.21.3 (04.2024)

- Les valeurs d'en-tête HTTP en XML sont désormais envoyées en tant que CDATA.
- Mise à jour de la liste des en-têtes HTTP (en-têtes HTTP réservés et saut par saut) à filtrer lors du transfert des messages REST.
- Aucune imposition de restrictions à la taille de la valeur de l'en-tête HTTP configuré que le serveur de sécurité ajoutera aux demandes entrantes.

### 1.21.2 (02.2024)

- Correction des profils de certificats `SkKlass3CertificateProfileInfoProvider`, `UxpCertificateProfileInfoProvider`, et `UxpOrgIdCertificateProfileInfoProvider`.

### 1.21.1 (01.2024)

- Par défaut, la prise en charge de la signature par lots est activée pour les dispositifs de création de signature nouvellement ajoutés.
- Transfert de l'en-tête d'autorisation du client au service.
- Ajout des dépendances de bibliothèque manquantes qui causaient le dysfonctionnement de l'interface CLI de configuration du serveur.



## 1.21.0 (11.2023)

- Après une interruption de la version 1.18 à la version 1.20, le serveur de sécurité prend à nouveau en charge les dispositifs externes de création de signature (tels que les HSM de réseau et les clés USB) pour le stockage des clés de signature.
  - La configuration de l'emplacement du pilote et des paramètres avancés du dispositif a été déplacée du fichier `devices.ini` vers l'interface utilisateur du serveur de sécurité.
  - Le dispositif de création de signature doit toujours disposer d'une interface PKCS#11.
  - Le serveur de sécurité a été testé et confirmé pour fonctionner avec le HSM *nShield Connect* d'Entrust.  
Pour en savoir plus sur l'utilisation des dispositifs de création de signature, consultez le guide de l'utilisateur du serveur de sécurité.
- Amélioration de l'expérience utilisateur de l'interface utilisateur.
  - Les certificats de serveur ont été déplacés sur une page distincte de la page Paramètres du système.
  - Les réponses OCSP pour les certificats sont désormais chargées de manière asynchrone afin d'éviter que des répondeurs OCSP lents ou défectueux ne ralentissent l'interface utilisateur du serveur de sécurité.
- Amélioration des performances de l'échange de messages.
- Lorsque la génération de CSR échoue, le serveur de sécurité supprime désormais la clé afin d'éviter de rassembler des clés inutilisables dans la base de données.
- Correction d'un bogue qui empêchait l'envoi d'une demande de service REST avec plus d'un paramètre de demande.
- Le guide de l'utilisateur contient désormais une recommandation sur l'attention à porter au niveau de journalisation, en particulier dans les installations de production. Après avoir modifié le niveau de journalisation pour enregistrer plus de détails à des fins de dépannage, il est recommandé, une fois le problème résolu, de rétablir le niveau par défaut afin d'économiser les ressources du serveur.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

## 1.20.1 (07.2023)

- Changement de version.

## 1.20.0 (06.2023)



Consultez la section Migration du guide d'installation (UXP-IG-SS) avant la mise à jour.

- Le serveur de sécurité utilise désormais la stratégie `round-robin` pour envoyer des demandes aux serveurs de sécurité du fournisseur de services lorsque ce dernier a mis en place plusieurs serveurs de sécurité. La stratégie `round-robin` répartit la charge entre plusieurs serveurs de sécurité et peut donc améliorer les performances de

l'échange de messages. L'ancienne stratégie (`fastest-connected`), selon laquelle le serveur le plus rapide à répondre obtenait la connexion, peut être réactivée en utilisant le paramètre `proxy.client-httpclient-target-selection-strategy`.

- Ajout de nouveaux paramètres de configuration pour le serveur de sécurité :
  - `proxy.client-httpclient-target-selection-strategy` — permet de définir la stratégie HTTP du proxy client pour choisir le proxy du serveur cible (la valeur par défaut est `round-robin`).
  - `proxy.max-retained-soap-attachment-size-bytes` — permet de définir la taille maximale en octets des pièces jointes SOAP qui sont conservées pour la journalisation (la valeur par défaut est 0).  
Le paramètre analogue pour la charge utile REST a été renommé de `proxy.max-retained-attachment-size-bytes` à `proxy.max-retained-rest-payload-size-bytes`.
  - `proxy.batch-signatures-enabled` — permet d'activer/désactiver les signatures de lots (valeur par défaut : `true`).
  - `proxy.log-signatures` — permet d'activer/désactiver le stockage des signatures des demandes et réponses régulières dans le journal des messages (la valeur par défaut est `true`).
- Limitation à 5 Mo de la taille des fichiers pouvant être téléchargés sur le serveur de sécurité.
- Amélioration de la prise en charge d'Elasticsearch.
  - La version 8.x des outils Elasticsearch et Kibana est désormais prise en charge.
  - Remplacement du client Java High Level REST d'Elasticsearch obsolète par le client Java API.
- Amélioration de la prise en charge de Zabbix.
  - La version 6.0 LTS de Zabbix est désormais prise en charge.
  - L'ancienne version 4.0 LTS de Zabbix n'est plus officiellement prise en charge.
  - Les modèles Zabbix sont désormais utilisés pour configurer les serveurs de sécurité vers Zabbix.
    - Ajout du modèle `Template App UXP Security Server by PMA` pour Zabbix 5.0 et `UXP Security Server by PMA` pour Zabbix 6.0.
    - Anciennes clés d'objets et certains noms d'objets renommés.
    - Anciens éléments pour les progiciels UXP, statuts de processus et temps de fonctionnement divisés pour une meilleure convivialité.
    - Ajout d'un nouvel élément calculé `Disk free in %`.
    - Ajout de quelques déclencheurs aux modèles.
  - Ajout d'un mode de coexistence avec le serveur de surveillance UXP. Si cette option est activée, le nom d'hôte du serveur de sécurité configuré dans Zabbix reçoit le suffixe `(local)`.

- Correction des délais de connexion et de lecture infinis du client de configuration.
- L'historique des journaux système est désormais conservé pendant 60 jours au lieu de 30.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

### **1.19.2 (03.2023)**

- Amélioration du basculement de l'horodatage en cas de configuration de plusieurs TSP dans le serveur de sécurité.

### **1.19.1 (11.2022)**

- Correction de l'importation d'un magasin de clés TLS interne sur le serveur de sécurité dans le cas où un certificat n'est pas auto-signé.

### **1.19.0 (11.2022)**

- L'assistant d'initialisation du serveur de sécurité a été étendu au reste des étapes nécessaires pour qu'un serveur de sécurité soit prêt à échanger des messages avec d'autres serveurs. L'assistant comprend maintenant la sélection d'un service d'horodatage, la configuration d'une clé d'authentification et de signature et l'enregistrement du serveur sur une instance UXP.
- Ajout de la prise en charge de la notation CIDR pour la configuration des adresses autorisées à demander des informations sur l'état du serveur de sécurité.
- L'état du serveur de sécurité est désormais considéré comme DOWN si le jeton stockant la clé d'authentification (jeton logiciel) n'est pas connecté.
- Ubuntu 22.04 LTS est désormais une plate-forme prise en charge (et recommandée). Ubuntu 20.04 LTS est désormais une plate-forme minimale prise en charge. Consultez le guide de mise à jour Ubuntu UXP-UPG-UB22.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

### **1.18.4 (11.2022)**

- Correction d'une procédure anormale d'établissement de connexion TLS lors de la connexion à la grappe HA du serveur de sécurité.

### **1.18.3 (10.2022)**

- Correction des délais de connexion et de lecture infinis du client de configuration.

### **1.18.2 (09.2022)**

- Correction du problème de démarrage de l'agent de surveillance du proxy lorsque le serveur de sécurité n'a pas encore été initialisé.

### **1.18.1 (09.2022)**

- Correction du métaservice WSDL définissant une adresse de serveur de sécurité incorrecte dans le WSDL renvoyé.

## 1.18.0 (06.2022)



L'agent de surveillance du proxy n'est plus compatible avec l'ancienne version 6.x d'Elasticsearch.

- Réécriture complète de l'interface utilisateur Serveur de sécurité UXP en utilisant les dernières technologies.
  - Omission de certaines fonctionnalités à la suite de la réécriture :
    - Les jetons matériels, Azure Key Vault et AWS CloudHSM ne sont pas pris en charge. Lorsque l'on utilise l'un de ces jetons pour stocker des clés, celles-ci doivent être remplacées par de nouvelles clés sur le jeton logiciel.
    - Les clés de chiffrement séparées ne sont plus prises en charge. La communication entre les serveurs de sécurité est toujours cryptée car les serveurs de sécurité utilisent intrinsèquement le protocole TLS pour communiquer entre eux. Seule la possibilité d'utiliser un cryptage supplémentaire au niveau du message a été supprimée.
    - La vue d'ensemble de l'état du système n'est plus disponible dans l'interface utilisateur. L'état du serveur peut toujours être surveillé à l'aide d'une installation locale de Zabbix. Consultez le guide de surveillance du serveur de sécurité (UXP-UG-PMA) pour obtenir des instructions.
    - Les statistiques sur les demandes ne sont plus disponibles dans l'interface utilisateur. Les demandes traitées par le serveur de sécurité peuvent toujours être surveillées à l'aide d'une configuration locale Elasticsearch et Kibana. Consultez le guide de surveillance du serveur de sécurité (UXP-UG-PMA) pour obtenir des instructions.
    - La création de sauvegardes et la restauration à partir de sauvegardes ne sont plus disponibles dans l'interface utilisateur. Le serveur de sécurité peut toujours être sauvegardé et restauré à l'aide de l'interface de ligne de commande.
    - Le téléchargement des journaux à partir de l'interface utilisateur n'est plus disponible dans l'interface utilisateur. Les journaux sont toujours accessibles via l'interface de ligne de commande.
    - L'exportation et l'importation de la configuration des services pour la grappe ne sont plus disponibles dans l'interface utilisateur. La configuration peut toujours être exportée et importée à l'aide de l'interface de ligne de commande.
    - L'onglet Clients du service a été supprimé. Les droits d'accès au service peuvent être contrôlés dans la vue détaillée du service.
    - La console Signer n'est plus prise en charge. Les clés et les certificats peuvent être gérés à l'aide de l'interface utilisateur du serveur de sécurité.
  - Refonte de certaines parties de l'interface utilisateur du serveur de sécurité et ajout de nouvelles fonctionnalités :
    - Les certificats importants pour le fonctionnement du serveur de sécurité sont désormais regroupés.
    - Il existe une page séparée pour tous les certificats de signature.

- La génération de clés et de CSR se fait désormais en une seule étape.
  - Le tableau des clients indique le nombre de services fournis par chaque client.
  - Le tableau des clients indique si chaque membre dispose d'un certificat de signature opérationnel.
  - Les certificats de signature peuvent être gérés dans les détails de chaque client.
  - Les certificats TLS du client peuvent également être gérés dans les détails du service.
  - Les certificats et les CSR peuvent maintenant être téléchargés.
  - L'interface utilisateur contient davantage de textes d'aide pour guider les utilisateurs dans leurs tâches.
  - Le serveur de sécurité effectue des contrôles avant d'envoyer une demande de gestion pour s'assurer que les conditions préalables sont remplies.
  - Les heures affichées dans l'interface utilisateur sont calculées en fonction de l'heure locale de l'utilisateur (sauf indication contraire). Les utilisateurs peuvent vérifier leur fuseau horaire dans le menu utilisateur.
- Le serveur de sécurité comprend désormais une API de gestion. La description OpenAPI peut être consultée à l'adresse : <https://<security-server>:4000/api/v1/openapi-ui>. L'API est encore en cours de développement et susceptible d'être modifiée.
  - La session utilisateur du serveur de sécurité est fixée à 3 heures. Après ce délai, l'utilisateur sera automatiquement déconnecté.
  - Réécriture de l'enregistrement des audits du serveur de sécurité. Le journal d'audit a un nouveau format d'événement.
  - Fusion de trois rôles de serveur de sécurité — *uxp-security-officer*, *uxp-registration-officer*, *uxp-system-administrator* — en un nouveau rôle *uxp-server-administrator*. Les utilisateurs ayant les trois rôles mentionnés se verront attribuer le nouveau rôle automatiquement après la mise à jour. Pour les autres, le nouveau rôle doit être attribué manuellement.
  - Lors de l'ajout du propriétaire ou d'un client, le serveur de sécurité valide désormais également les symboles dans les identifiants des membres UXP et des sous-systèmes qui figurent déjà dans la configuration globale. Seuls les lettres A à Z, les chiffres, les traits de soulignement ( \_ ) et les traits d'union ( - ) sont autorisés.
  - Le serveur de sécurité limite désormais les caractères dans les codes et les versions des services SOAP. Seuls les lettres, les chiffres, les traits de soulignement ( \_ ) et les traits d'union ( - ) sont autorisés.
  - Lors du calcul des limitations de licence, le serveur de sécurité ne compte plus le propriétaire comme un client.
  - Les serveurs de sécurité du client ne demandent pas les réponses OCSP du certificat d'authentification du serveur de sécurité du fournisseur de services avant d'initier une connexion, la fonction d'agrafage OCSP de TLS 1.3 est utilisée pendant l'établissement de la connexion. Lors de la communication avec des serveurs plus anciens, l'ancien

mode de fourniture de réponses OCSP est utilisé à des fins de compatibilité ascendante (il sera supprimé à l'avenir).

- Le serveur de sécurité stocke désormais ses clés et certificats internes sur le jeton logiciel, de la même manière que les autres clés du serveur.
- Ajout d'un nouveau paramètre système (`timestamp-immediately` dans la section `[message-log]` du fichier de configuration `message-log.ini`) au serveur de sécurité qui active le mode d'horodatage immédiat. Par défaut, l'horodatage est effectué périodiquement pour un lot de messages réunis comme précédemment.
- L'agent de surveillance proxy prend désormais en charge la connexion TLS et l'authentification de base avec Elasticsearch.
  - De nouveaux paramètres ont été ajoutés pour configurer l'agent de surveillance proxy de manière sécurisée pour Elasticsearch. Les nouveaux paramètres du fichier `monitor-agent.ini` sont `scheme`, `username`, `password`, `ca-cert-file`, et `verify-hostname`.
- Le serveur de sécurité ne dépend plus des paquets `uxp-jetty` et `uxp-signer`.
- Le serveur de sécurité dépend désormais des paquets `uxp-securityserver-ui` et `uxp-securityserver-rest-api`.
- Java Runtime Environment est mis à jour vers la version 17. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

### 1.17.2 (10.2022)

- Correction des délais de connexion et de lecture infinis du client de configuration.

### 1.17.1 (12.2021)

- Correction de la gestion de la valeur de l'en-tête HTTP Accept pour les métaservices.

### 1.17.0 (10.2021)

- Nouveau guide de dépannage pour l'échange de messages UXP. Aperçu général de l'interprétation des codes d'erreur et instructions détaillées pour certaines erreurs plus courantes.
  - Consultez la section « Dépannage de l'échange de messages » dans UXP-UG-SS.
- Meilleure prise en charge de l'archivage S3 pour le journal des messages.
  - Configuration plus facile de l'archivage AWS S3 et S3-like et compatibilité totale avec Vérificateur UXP.
  - Tous les scripts d'archivage S3 précédemment configurés doivent maintenant être remplacés. Pour plus de détails, voir la section « Journal des messages » dans UXP-UG-SS.
- Les données utiles des messages REST sont désormais enregistrées dans le journal des messages afin de permettre le même niveau d'audit que pour les messages SOAP.
- Interface utilisateur et guide d'utilisation du serveur de sécurité spécialisés pour le rôle d'Administrateur service (`uxp-service-administrator`).

- Interface utilisateur simplifiée pour les utilisateurs qui ne font que rendre les services Web disponibles sur UXP et ne gèrent pas la configuration du serveur de sécurité.
- Le guide d'administration des services (UXP-UG-SSSERVICE) fournit une vue d'ensemble des tâches pour le rôle.
- Certains journaux peuvent désormais être téléchargés directement à partir de l'interface utilisateur du serveur de sécurité.
  - Les 5 derniers Mo de `audit.log`, `proxy.log` et `jetty.log` peuvent être téléchargés à partir de l'interface utilisateur, ce qui simplifie le dépannage et l'audit pour les utilisateurs qui n'ont pas d'accès SSH au serveur de sécurité.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

### 1.16.0 (07.2021)

- Lorsqu'un certificat est importé sur un serveur de sécurité et qu'il n'existe pas d'autres certificats ayant le même usage (authentification, cryptage), le certificat est automatiquement activé après l'importation.
- Le serveur de sécurité se connecte désormais automatiquement au jeton logiciel après l'initialisation du serveur.
- Préparatifs pour le développement de l'API de gestion des serveurs de sécurité. Ces préparatifs comprennent principalement des modifications de l'architecture interne.
- Quelques corrections mineures.

### 1.15.2 (07.2021)

- Les enregistrements du journal du proxy relatifs à l'échange de messages UXP comprennent désormais l'identifiant de la transaction et les identifiants UXP du client et du fournisseur de services, ce qui facilite le débogage.
- Tous les journaux sont désormais affichés par défaut dans le fuseau horaire local.
- Autres corrections mineures.

### 1.15.1 (06.2021)

- Correction d'un bogue dans la gestion du journal des messages dans des situations exceptionnelles (coupure de courant).
- Autres corrections mineures.

### 1.15.0 (04.2021)



Pour mettre à jour les serveurs de sécurité vers la version 1.15, vous devez suivre les instructions de l'annonce « Mise à jour du serveur de sécurité et migration du journal des messages ».

- Le journal des messages du serveur de sécurité a été réécrit, ce qui améliore les performances de l'échange de messages.
  - Il y a maintenant un exemple de script pour déplacer des archives de journaux de messages vers Amazon S3. Voir la section UXP-UG-SS « Transfert des fichiers



d'archive depuis le serveur de sécurité ».

- Les fournisseurs de services peuvent désormais ajouter des API REST à partir de descriptions OpenAPI hébergées. Voir la section « Gestion des API REST » de l'UXP-UG-SS.
  - La version 3.0 d'OpenAPI est prise en charge.
  - Le serveur de sécurité prend en charge les URL de base relatives et multiples.
  - La fonctionnalité d'actualisation permet de rester informé des modifications apportées à la description OpenAPI tout en préservant les droits d'accès existants.
- Les niveaux de journalisation peuvent désormais être modifiés sans redémarrer les services UXP.
  - Cela permet de déboguer dans des environnements réels sans causer de temps d'arrêt.
- Les anciennes versions de Zabbix 2.2 - 2.4, et 3.0 - 3.4 ne sont plus officiellement prises en charge.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

#### 1.14.1 (02.2021)

- Changement de version.

#### 1.14.0 (12.2020)

- Les fournisseurs de services peuvent désormais ajouter des droits d'accès aux API REST à un niveau plus granulaire. Voir la section « Division d'une API REST en points de terminaison » d'UXP-UG-SS.
  - Le serveur de sécurité prend en charge la définition de points de terminaison spécifiques pour les API REST, y compris les points de terminaison dynamiques tels que `/posts/{id}`.
  - Les administrateurs de services peuvent contrôler les droits d'accès au niveau des points de terminaison de l'API.
  - Les administrateurs de services peuvent contrôler les opérations HTTP (GET, DELETE, etc.) que chaque client de service peut effectuer sur un point de terminaison.
- Les fournisseurs de services peuvent ajouter des en-têtes HTTP pour les services REST et SOAP. Les en-têtes peuvent être utilisés pour configurer l'authentification entre le serveur de sécurité et l'API.
- Les serveurs de sécurité n'acceptent pas les demandes REST qui incluent des identifiants de client et de service dans l'URL. Les identifiants doivent être placés dans les en-têtes HTTP. Pour connaître le format accepté, consultez la section « Format de demande REST » d'UXP-UG-SS.
- Les serveurs de sécurité disposent désormais d'un service d'information sur l'état qui peut être utilisé par des répartiteurs de charge tiers pour choisir un serveur de sécurité cible sain dans une configuration en grappe.



- Le serveur de sécurité peut être configuré pour utiliser ses informations d'état afin de décider d'accepter ou non les demandes entrantes (désactivé par défaut). Si cette option est activée, un serveur de sécurité ayant le statut DOWN cesse de répondre aux demandes HTTP(S) afin que d'autres serveurs de la grappe ayant le statut UP puissent répondre à la demande. Cela améliore la fiabilité d'une grappe de serveurs de sécurité.
- Pour aider les administrateurs de serveurs de sécurité à maintenir la synchronisation de tous les serveurs de sécurité d'une grappe, nous avons ajouté une fonctionnalité permettant d'exporter les informations pertinentes sur les clients et les services dans un fichier. Les fichiers de configuration peuvent être importés vers d'autres serveurs de sécurité.
- Nouveau guide de l'utilisateur Serveur de sécurité : Configuration de la haute disponibilité et de l'équilibrage de la charge. Voir UXP-UG-SSHA.
- Les services de métadonnées UXP permettant de découvrir les fournisseurs de services et leurs services sont désormais disponibles via des demandes REST. Voir UXP-PR-META.
- Amélioration des performances en cas de forte charge de messages.
- La présentation de l'interface utilisateur a été modifiée dans le dialogue entre le serveur de sécurité et le client.
- Le serveur de sécurité est désormais incompatible avec les versions 1.x du Serveur de surveillance UXP. Les serveurs de sécurité ne transmettent pas les informations de surveillance à l'ancien serveur de surveillance.
- Le serveur de sécurité est désormais incompatible avec la version 2.2 et celles antérieures de Répertoire UXP. Avant de mettre à jour le serveur de sécurité, Répertoire UXP doit être mis à jour à la version 2.3 ou supérieure.
- Ajout de scripts qui aident les administrateurs de serveurs UXP à recueillir des informations pertinentes sur l'état actuel d'un serveur.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Plusieurs corrections et améliorations mineures.

### 1.13.1 (09.2020)

- Document UXP-UG-SS amélioré.
- Document UXP-UPG-UB20 amélioré.
- Plusieurs corrections et améliorations mineures.

### 1.13.0 (08.2020)

- Ajout de la prise en charge des clés à courbe elliptique (EC) pour les jetons logiciels et matériels (les clés EC en tant que clés de chiffrement du serveur de sécurité ne sont actuellement pas prises en charge).



Les clés EC ne peuvent être utilisées comme clés de configuration sur le serveur de registre qu'une fois que tous les serveurs de sécurité (et le paquet `uxp-confclient` sur les serveurs de surveillance) de l'instance UXP ont été mis à

jour vers la version actuelle.

- Ajout de la prise en charge des clés EC pour Nginx et les certificats TLS internes.
- Ajout de la prise en charge de clés RSA plus longues (3072 et 4096 bits).
- Amélioration de la communication TLS.
  - Ajout de la prise en charge de TLS 1.3 (désormais protocole par défaut). TLS 1.2 est toujours pris en charge par défaut pour des raisons de compatibilité ascendante.
  - Ajout de suites de chiffrement TLS plus puissantes activées par défaut.
  - Il est désormais possible de configurer les suites de chiffrement activées pour la communication TLS entre le serveur de sécurité et le système d'information.
- Le serveur de sécurité utilise désormais une connexion de bouclage lorsque la demande du client de service est traitée par le même serveur de sécurité.
- Amélioration de la procédure de modification du certificat TLS interne du serveur de sécurité.
  - Il est désormais possible de modifier le certificat en toute simplicité.
  - Il est désormais possible d'importer un certificat (généré par une autorité de certification externe) et la clé privée correspondante sous la forme d'un magasin de clés PKCS#12.
- Le port d'écoute côté serveur entre les serveurs de sécurité est désormais distribué avec l'adresse du serveur de sécurité via la configuration globale. Il permet de modifier le port d'écoute du serveur de sécurité sans interrompre les connexions avec d'autres serveurs de sécurité.



Cette fonctionnalité ne peut être utilisée que lorsque tous les serveurs de registre et les serveurs de sécurité de l'instance UXP ont été mis à jour vers la version actuelle.

- Le type de connexion du propriétaire du serveur de sécurité pour les serveurs dans le rôle de consommateur de services est maintenant fixé à HTTPS pour améliorer la sécurité.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Ubuntu 20.04 LTS est désormais une plate-forme supportée (et recommandée). Consultez le guide de mise à jour Ubuntu UXP-UPG-UB20.
- Plusieurs corrections et améliorations mineures.

### 1.12.2 (04.2020)

- Ajout d'un profil de certificat.

### 1.12.1 (03.2020)

- Plusieurs corrections et améliorations mineures.

### 1.12.0 (02.2020)

- Il y a un nouveau composant Vérificateur UXP. Il permet de consulter le contenu du journal des messages stocké sur le serveur de sécurité, ainsi que de télécharger et de vérifier des messages individuels signés.
- L'API pour le téléchargement de documents signés (ASiC) exige désormais l'utilisation du protocole HTTPS afin d'éviter toute violation de la confidentialité dans le réseau interne.
- Il y a un nouvel en-tête HTTP `Uxp-Transaction-ID`. Il est généré automatiquement par le serveur de sécurité et contient une valeur unique pour chaque message traité par le serveur de sécurité. L'identifiant de la transaction est également enregistré dans le journal des messages et peut être utilisé pour identifier de manière unique les messages UXP.
- Une nouvelle option de configuration permet de désactiver l'enregistrement des messages techniques (services de surveillance et metainfo) dans le journal des messages. Cela peut permettre d'économiser de l'espace disque s'il n'est pas nécessaire de créer une valeur probante pour les échanges qui n'impliquent pas de données commerciales.
- La version 7.x des outils Elasticsearch et Kibana est désormais prise en charge pour la surveillance locale.
- La grappe multi-nœuds Elasticsearch est désormais pris en charge.
- L'ancien document de statistiques sur les demandes (l'ancien format pour les statistiques UXP) n'est plus pris en charge dans le suivi local.
- Ubuntu 18.04 est désormais la plus ancienne plate-forme prise en charge.
- Java Runtime Environment est mis à jour vers la version 11. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

#### 1.11.4 (12.2019)

- Correction de la création de signature avec Azure Key Vault.

#### 1.11.3 (12.2019)

- Ajout de la prise en charge du mécanisme de signature PKCS#11 CKM\_RSA\_PKCS\_PSS et configuration du modèle de création de clé.

#### 1.11.2 (10.2019)

- Correction des dépendances des bibliothèques communes dans Serveur de surveillance UXP.
- Correction d'un comportement incorrect lors du transfert d'appels API REST avec des chaînes de demande URL vides.
- Correction des segments de chemin inutiles lors de la transmission des appels à l'API REST.

#### 1.11 (08.2019)

- Ajout d'une prise en charge complète de l'IPv6.
- Ajout de la prise en charge de Zabbix 4.0.

- Ajout de la prise en charge de AWS CloudHSM (module de sécurité matérielle basé sur le cloud).
- Ajout de la prise en charge d'une large gamme de jetons matériels basés sur la norme PKCS#11.
- Suppression de la fonction de services centraux qui n'était pas utilisée dans la pratique.
- Amélioration de l'emballage des composants UXP. L'emballage est désormais plus modulaire et seuls les modules essentiels sont installés pour chaque composant UXP.
- Ajout d'un nouveau profil de certificat UXP par défaut `ee.cyber.uxp.common.certificateprofile.impl.UxpCertificateProfileInfoProvider`.
- Le jeu de caractères des identifiants UXP est désormais limité à `[a-zA-Z0-9_-]`. Ceci s'applique à l'identificateur d'instance, à la classe de membre, au code de membre, au code de sous-système, au code de groupe et au code de serveur.
- Correction de l'horodatage du type de média dans le manifeste des conteneurs ASiC produits par les serveurs de sécurité UXP.
- Mise en œuvre de diverses améliorations mineures et corrections de bogues.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Documentation améliorée (UXP-UG-RS, UXP-IG-SS, UXP-IG-SS, UXP-UG-SS, UXP-UG-PMA, UXP-IG-MS). Ajout de l'aide en ligne UXP-UG-PMA sur le serveur de sécurité.

## 1.10 (12.2018)

- La série de versions 1.x du Serveur de surveillance UXP est obsolète. La version 2.0 du Serveur de surveillance est une réécriture de l'ancienne version et utilise un modèle de données différent. Voir UXP-IG-MS (version 2.0) pour plus de détails.
- Le même protocole de surveillance peut être utilisé pour récupérer les informations de surveillance du serveur de sécurité.
- Note : Le type de connexion HTTPS doit être configuré pour le propriétaire du serveur dans le rôle de consommateur de services. Cela permettra d'éviter tout abus des dispositifs de surveillance. Pour plus de détails, consultez UXP-UG-PMA, section Surveillance des serveurs de sécurité UXP.
- Ubuntu 18.04 LTS est désormais une plate-forme prise en charge (et recommandée).
- Amélioration de la gestion des erreurs SOAP.
- Corrections de bogues et améliorations mineures.

## 1.9 (06.2018)

- Le système de gestion des licences est amélioré.
  - Il est possible de déléguer la signature des licences à une autre entité.
  - Différents produits installés sur la même machine peuvent utiliser des licences distinctes.
  - Les licences peuvent être visualisées et gérées dans l'interface utilisateur.

- Le système de surveillance prend en charge la version 6.x des outils Elasticsearch et Kibana.
- La surveillance locale permet d'obtenir des statistiques plus détaillées sur les transactions.
- Ubuntu 14.04 n'est plus une plate-forme prise en charge.
- Les guides d'utilisation et d'installation contiennent des informations plus détaillées et sont restructurés pour une meilleure lisibilité.
- Le guide de l'utilisateur est également accessible à partir de l'interface utilisateur en tant qu'aide en ligne.
- Les bibliothèques et frameworks tiers sont mis à jour.
- Plusieurs améliorations mineures de la convivialité, des performances et de la sécurité.

## **1.8 (10.2017)**

- UXP prend désormais en charge Microsoft Azure Key Vault.
- UXP prend en charge le chiffrement supplémentaire des messages (il peut utiliser des algorithmes de chiffrement qui ne sont pas pris en charge par TLS).

## **1.7 (06.2017)**

- Les API REST peuvent désormais être fournies et consommées via l'infrastructure UXP.
- Les WSDL contenant des déclarations d'importation sont désormais pris en charge.

## **1.6 (05.2017)**

- Mise à jour vers la nouvelle version d'Elasticsearch pour la collecte d'analyses de surveillance.
- Amélioration de la sécurité et des performances.
- Amélioration de la solution de haute disponibilité du serveur de registre.

## **1.5 (03.2017)**

- UXP peut maintenant être installé sur Ubuntu 16.04 LTS.
- Les WSDL qui ne décrivent pas les messages de réponse (services « push ») sont désormais pris en charge.

## **1.4 (10.2016)**

- UXP prend désormais en charge les messages SOAP 1.2.
- La gestion du WSDL UXP prend désormais en charge les services sans en-tête UXP/X-Road. Cela permet de fournir des services SOAP existants via UXP sans aucune modification.

## **1.3 (07.2016)**

- UXP prend en charge la traduction des interfaces utilisateur.
- Plusieurs améliorations de la sécurité.

## **1.2 (04.2016)**

- Le Serveur de surveillance UXP est introduit.  
Les serveurs de sécurité envoient des informations de surveillance au Serveur de

surveillance UXP qui les met à la disposition de Zabbix. Aide à la collecte et à l'analyse des statistiques sur les transactions. Des informations statistiques sur les transactions sont collectées, analysées et visualisées.

### **1.1 (03.2016)**

- UXP prend en charge le mode de fonctionnement mutliconnexion.  
UXP peut être installé dans un environnement composé de plusieurs réseaux déconnectés (par exemple, réseau privé et internet). Les serveurs de sécurité peuvent être connectés à plusieurs réseaux et ils sélectionnent automatiquement le bon réseau pour envoyer les données au partenaire de communication.
- Ajout d'une vue de l'état du système sur le serveur de sécurité.
- Plusieurs corrections de bogues et améliorations.

### **1.0 (12.2015)**

- Première publication des composants principaux UXP.