

Serveur de sécurité UXP 1.25

Guide de l'utilisateur

UXP-UG-SS

Table des matières

Dernières notes de mise à jour	1
1. Introduction	3
1.1. Public cible	3
1.2. Serveur de sécurité UXP	3
1.3. Concepts UXP	4
1.4. URL importantes	8
1.5. Références	9
2. Gérer mon compte	11
2.1. Affichage de mes rôles	11
2.2. Changer de mot de passe	11
2.3. Réinitialiser un mot de passe oublié	11
2.4. Tentatives de connexion et verrouillage	11
3. Gestion des utilisateurs	12
3.1. Rôles des utilisateurs	12
3.2. Gérer les utilisateurs avec le Gestionnaire des utilisateurs UXP	13
3.2.1. Ajouter un utilisateur	13
3.2.2. Changer les rôles des utilisateurs	14
3.2.3. Supprimer un utilisateur	15
3.2.4. États des utilisateurs	15
3.2.5. Bloquer et débloquer un utilisateur	15
3.2.6. Réinitialiser un mot de passe	16
3.2.7. Ajouter un compte d'administrateur serveur sans accès à l'interface utilisateur	16
3.2.8. Bloquer un utilisateur sans accès à l'interface utilisateur	17
3.2.9. Mécanisme de protection de la connexion	17
3.3. Gérer les utilisateurs avec le Gestionnaire des utilisateurs Ubuntu	17
3.3.1. Commandes du Gestionnaire des utilisateurs Ubuntu	17
3.3.2. Mécanisme de protection de la connexion d'Ubuntu	19
4. Enregistrement du serveur de sécurité	20
4.1. Ajouter une clé de signature et un certificat pour le propriétaire du serveur de sécurité	20
4.2. Ajouter une clé d'authentification et un certificat pour le serveur de sécurité	20

4.3. Enregistrer un serveur de sécurité auprès de l'autorité de gouvernance UXP	21
5. Clients du serveur de sécurité	22
5.1. Ajouter un client de serveur de sécurité	22
5.2. Configurer une clé de signature et un certificat pour un client du serveur de sécurité . .	22
5.3. Enregistrer un client du serveur de sécurité auprès de l'autorité de gouvernance UXP .	23
5.3.1. Enregistrer un client du serveur de sécurité	23
5.4. Supprimer un client du Serveur de sécurité	23
5.4.1. Désenregistrer un client	24
5.4.2. Supprimer un client	24
5.5. États du client du serveur de sécurité	24
6. Architecture mutualisée	26
6.1. Intégration d'un membre	27
6.1.1. Ajouter un membre	27
6.1.2. Ajouter des utilisateurs	27
6.1.3. Choisir le stockage pour les clés de signature des membres	28
6.1.4. Connexion sécurisée entre le système d'information des membres et le serveur de sécurité	29
6.2. Désengagement d'un membre	29
7. Clés de signature	30
7.1. Jetons	30
7.1.1. Jetons logiciels	30
7.1.2. Jetons matériels	31
7.2. Générer une clé et une CSR	32
7.3. Importer un fichier de certificat	32
7.4. Importer un certificat depuis un dispositif	33
7.5. Activer et désactiver les certificats	34
7.6. Supprimer un certificat ou une demande de signature de certificat	34
7.7. Validité d'un certificat	34
7.8. Types de clés	35
8. Clés d'authentification	37
8.1. Générer une clé d'authentification et une CSR	37
8.2. Enregistrer un certificat d'authentification	37
8.3. Annuler l'enregistrement d'un certificat d'authentification	38
8.4. Supprimer une clé d'authentification et un certificat	38

8.5. États d'enregistrement des certificats d'authentification	38
9. Certificat TLS interne du serveur de sécurité	40
9.1. Ajouter une nouvelle clé et un nouveau certificat TLS interne au serveur de sécurité. . .	40
9.2. Activer un certificat TLS interne du serveur de sécurité	41
9.3. Exporter un certificat TLS interne du serveur de sécurité.	41
9.4. Supprimer un certificat TLS interne du serveur de sécurité	41
10. Dispositifs de création de signature	43
10.1. Connexion d'un dispositif de création de signature	43
10.1.1. Dispositif de création de signature (PKCS#11)	43
10.2. Ajouter un jeton matériel	45
10.3. États des jetons matériels	46
10.4. Supprimer un jeton matériel	47
10.5. Supprimer un dispositif de création de signature	47
10.6. Désactiver et activer un dispositif de création de signature	47
10.7. Modification des paramètres d'un dispositif de création de signature.	48
11. Services UXP	49
11.1. Gestion des services SOAP	49
11.1.1. Ajouter un WSDL	49
11.1.2. Actualiser un WSDL	49
11.1.3. Activer et désactiver un WSDL	50
11.1.4. Changer l'adresse d'un WSDL	50
11.1.5. Supprimer un WSDL	51
11.1.6. Changer les paramètres d'un service SOAP	51
11.1.7. Ajouter des en-têtes HTTP aux demandes SOAP	51
11.2. Gestion des API REST	53
11.2.1. Ajouter une API REST	53
11.2.2. Points de terminaison de l'API REST	54
11.2.3. Actualiser une description OpenAPI	55
11.2.4. Activer et désactiver une API REST	55
11.2.5. Changer l'URL de description OpenAPI	56
11.2.6. Paramètres de l'API REST	56
11.2.7. Ajouter des en-têtes HTTP aux demandes REST	57
11.2.8. Supprimer une API REST	59
11.3. Faire des demandes à une API REST	59

11.3.1. Exemple de configuration	59
11.3.2. Format des demandes REST	60
11.3.3. Demande en action	62
11.4. Sécurisation de la connexion au fournisseur de services	62
12. Droits d'accès	64
12.1. Modification des droits d'accès à un service SOAP	64
12.2. Changer les droits d'accès à une API REST	64
13. Limites de débit	66
13.1. Comment fonctionnent les limites de débit	66
13.2. Affichage des limites de débit	67
13.3. Ajouter une limite de débit à un service	67
13.4. Modifier et supprimer une limite de débit	68
14. Groupes de droit d'accès local	69
14.1. Ajouter un groupe local	69
14.2. Affichage et modification des membres d'un groupe local	69
14.3. Supprimer un groupe local	70
15. Communication avec les systèmes d'information des clients	71
15.1. Types de connexion	71
15.2. Certificats TLS internes au système d'information	72
15.3. Certificat TLS interne du serveur de sécurité	72
16. Paramètres du système	73
16.1. Ancre de configuration	73
16.2. Services d'horodatage	73
16.3. Port d'écoute (transport) du serveur de sécurité	73
16.4. Fichiers de configuration	75
16.5. Certificat TLS Nginx	76
17. Journal des messages	79
17.1. Changer la configuration du journal des messages	80
17.1.1. Paramètres communs	80
17.1.2. Paramètres d'horodatage	81
17.1.3. Paramètres d'archivage	83
17.2. Configurer la durée de vie du journal des messages	84
17.3. Transfert des fichiers d'archive à partir du système de fichiers local	85
17.3.1. Exemple : HTTP POST	86

17.4. Désactivation du stockage des signatures du métaservice, de la surveillance et/ou des messages réguliers	87
18. Sauvegarde et restauration	88
18.1. Sauvegarde du serveur de sécurité	89
18.1.1. Sauvegarder la configuration du serveur	89
18.1.2. Sauvegarde du fournisseur d'identité	90
18.2. Restaurer un serveur de sécurité	91
18.2.1. Restaurer une configuration de serveur	91
18.2.2. Restaurer un fournisseur d'identité	92
18.2.3. Après la restauration	93
19. API de gestion	94
19.1. Rest API	94
19.1.1. API d'administration du serveur de sécurité	94
19.1.2. API du fournisseur d'identité	94
19.1.3. API du vérificateur	94
20. Maintenance	95
20.1. Changer l'adresse IP ou le nom DNS du serveur de sécurité	95
21. Journaux et services du système	96
21.1. Journaux	96
21.2. Services du système	97
21.3. Configuration de la journalisation	98
21.3.1. Configuration des paramètres de journalisation des composants	98
21.4. Détail de l'erreur UUID	100
21.5. Journal d'audit	100
21.5.1. Changer la configuration du journal d'audit	101
21.5.2. Archivage du journal d'audit	101
22. Outil de diagnostic	102
22.1. Dépannage des journaux dans l'interface utilisateur	102
22.1.1. Visualisation des journaux	103
22.1.2. Filtrer les journaux	104
22.2. Exporter des journaux	104
22.3. Générer un rapport de diagnostic	104
22.3.1. Générer un rapport à partir de l'interface utilisateur	105
22.3.2. Générer un rapport à partir de l'interface de programmation	106

23. Dépannage de l'échange de messages	107
23.1. Comprendre les messages d'erreur	107
23.2. Erreurs provenant du système d'information du client du service	109
23.3. Erreurs provenant du serveur de sécurité du client du service	111
23.4. Erreurs provenant du serveur de sécurité du fournisseur de services	118
24. Dépannage détaillé	123
24.1. Erreur de mémoire insuffisante du proxy	123
24.2. Erreur de mémoire insuffisante du Vérificateur ou de l'archiveur Messagelog	123
24.2.1. Calcul de la mémoire JVM en fonction des limites de stockage	125
24.2.2. Calcul de la mémoire JVM en fonction de la taille des messages	126
24.2.3. Augmentation progressive de la mémoire JVM	126
Annexe A: Notes de mise à jour	128

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

1.1. Public cible

Ce guide de l'utilisateur s'adresse aux administrateurs de serveurs de sécurité UXP chargés de la gestion quotidienne des serveurs de sécurité UXP.

Les instructions pour l'installation et la configuration initiale du logiciel du serveur de sécurité UXP se trouvent dans le document *Serveur de sécurité UXP : Guide d'installation et de configuration* [\[UXP-IG-SS\]](#).

1.2. 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.

Pour accroître la disponibilité de l'ensemble du système, les serveurs de sécurité de l'utilisateur du service et du fournisseur de services peuvent être configurés de manière redondante comme suit.

- Un consommateur de services peut utiliser plusieurs serveurs de sécurité en parallèle pour effectuer des demandes.
- Si un fournisseur de services connecte plusieurs serveurs de sécurité au réseau afin de fournir les mêmes services, les demandes sont réparties entre les serveurs de sécurité selon un équilibrage de charge.
- Si l'un des serveurs de sécurité du fournisseur de services est hors ligne, les demandes sont automatiquement redirigées vers d'autres serveurs de sécurité disponibles.

Pour plus d'informations sur la haute disponibilité des serveurs de sécurité et l'équilibrage des charges, voir [\[UXP-UG-SSHA\]](#).

Le serveur de sécurité dépend également d'un serveur de registre, qui fournit la configuration globale.

1.3. 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.

Ancre de configuration est un fichier nécessaire au téléchargement et à la vérification de la configuration globale.

Services de gestion sont des services UXP spéciaux utilisés par les serveurs de sécurité pour signaler leurs modifications de configuration au serveur de registre. Les serveurs de sécurité utilisent les services de gestion en envoyant des demandes d'enregistrement et de suppression au serveur de sécurité des services de gestion.

Serveur de sécurité des services de gestion est un serveur de sécurité dédié qui assure la médiation des services de gestion vers les serveurs de sécurité.

Demande d'enregistrement est une demande de gestion initiée par le serveur de sécurité ou le serveur de registre pour enregistrer un certificat ou un client du serveur de sécurité.

Demande de suppression est une demande de gestion initiée par le serveur de sécurité ou le serveur de registre pour supprimer un certificat ou un client du serveur de sécurité.

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

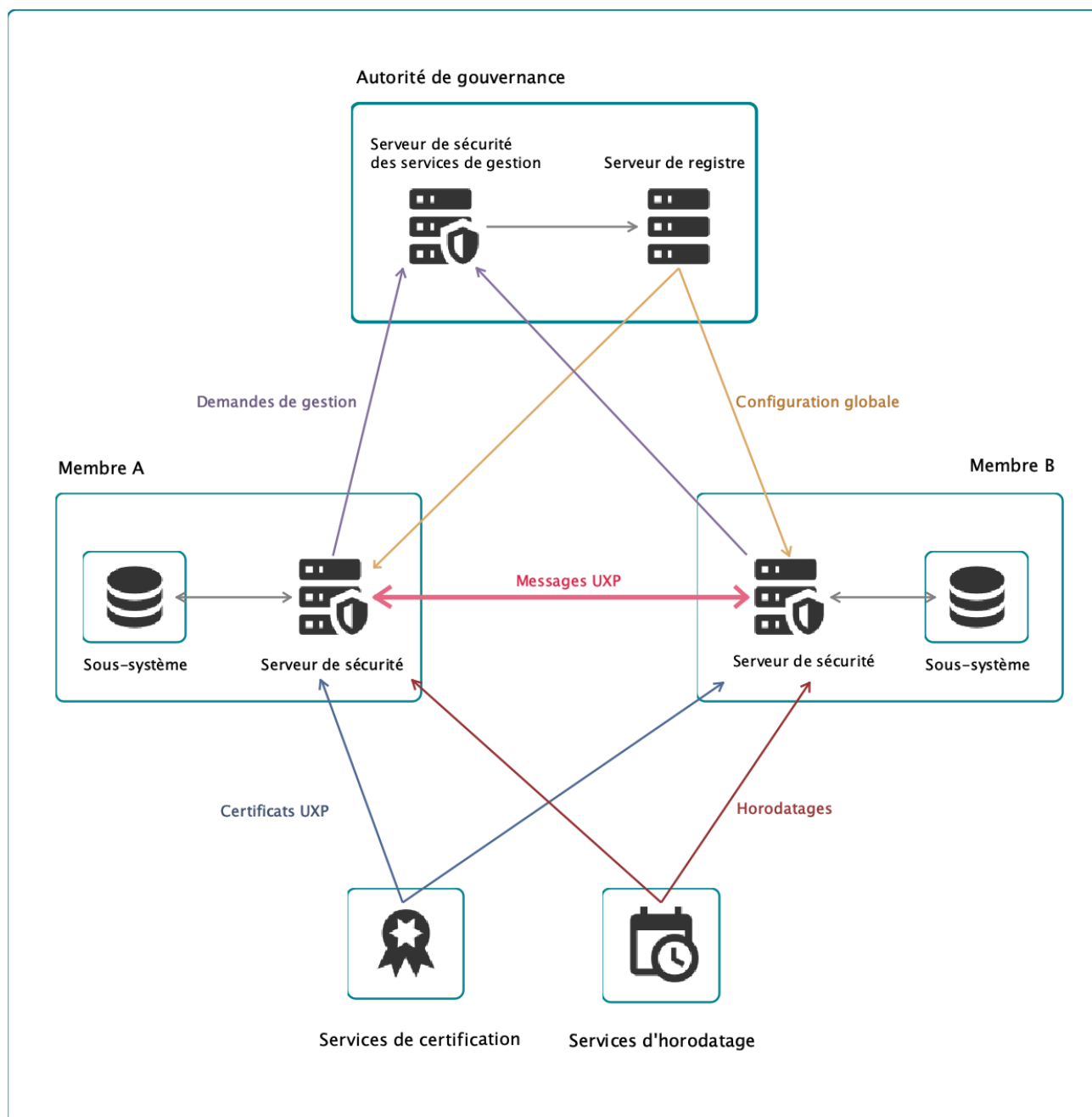


Figure 1. Schéma illustrant les composants d'une instance UXP

1.4. 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/
```

- Téléchargez 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](#).

1.5. Références

- [ASiC] ETSI TS 102 918, Signatures électroniques et infrastructures (ESI) ; Conteneurs de signature associés (ASiC)
- [CRON] Expression CRON de Quartz Scheduler, <http://www.quartz-scheduler.org/documentation/quartz-2.3.0/tutorials/crontrigger.html>
- [INI] Fichier INI, http://en.wikipedia.org/wiki/INI_file
- [LOGBACK-PATTERNS] Documentation de Logback. Chapitre 6 : Layouts — Conversion Word Table, <https://logback.qos.ch/manual/layouts.html#conversionWord>
- [NIST] Recommandation pour la gestion des clés, <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>
- [OpenAPI] Qu'est-ce que l'OpenAPI ?, <https://swagger.io/docs/specification/about/>
- [S3] Amazon S3, <https://aws.amazon.com/s3/>
- [\[UXP-IG-SS\]](#) Cybernetica AS. Serveur de sécurité UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-SS
- [\[UXP-PR-MESS\]](#) 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-SPEC-AL] Cybernetica AS. UXP: Événements du journal d'audit. Identifiant du document : UXP-SPEC-AL
- [UXP-UG-PMA] Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA
- [\[UXP-UG-SSHA\]](#) Cybernetica AS. Serveur de sécurité UXP : Configuration de la haute disponibilité et de l'équilibrage de la charge. Identifiant du document : UXP-UG-SSHA
- [UXP-UPG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide de mise à niveau. Identifiant du document : UXP-UPG-SS

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. Gestion des utilisateurs

3.1. Rôles des utilisateurs

Les activités dans l'interface utilisateur du serveur de sécurité sont regroupées en quatre rôles utilisateur :

- L'**Administrateur serveur** est responsable de
 - connecter le serveur de sécurité à l'instance UXP ;
 - enregistrer les sous-systèmes des membres UXP sur le serveur de sécurité ;
 - gérer les utilisateurs du serveur de sécurité ;
 - assurer le bon fonctionnement du serveur en gérant les paramètres système nécessaires.

En outre, l'Administrateur serveur a besoin du privilège de Responsable des clés pour assurer une configuration et une administration efficaces du serveur.

- Le **Responsable des clés** est chargé de veiller à ce que chaque membre UXP dispose d'une clé de signature fonctionnelle sur le serveur de sécurité.
- Le **Responsable des services** est responsable des services d'un membre UXP :
 - quels services sont fournis par le serveur de sécurité ;
 - qui peut accéder aux services ;
 - la sécurisation de la connexion entre le serveur de sécurité et les systèmes d'information fournissant ou consommant des services.
- L'**Auditeur de transactions** peut visualiser les signatures des messages échangés avec succès, vérifier les signatures et télécharger les conteneurs de messages pour les membres UXP.

Un utilisateur peut avoir plusieurs rôles, et plusieurs utilisateurs peuvent remplir le même rôle. Par défaut, les rôles d'utilisateur s'appliquent à **TOUS LES MEMBRES**, ce qui confère des droits de représentation à tous les membres actuels et futurs du serveur de sécurité.

Si l'architecture mutualisée est activée sur le serveur de sécurité, vous pouvez ajouter des utilisateurs avec les rôles **Responsable des clés**, **Responsable des services** et **Auditeur de transactions** pour des membres spécifiques.



Lorsque l'architecture mutualisée est activée sur le serveur de sécurité puis désactivée, l'accès des utilisateurs au serveur change. Seuls les Administrateurs serveur et les utilisateurs ayant des rôles pour tous les membres peuvent se connecter. Les utilisateurs de membres spécifiques ne peuvent pas se connecter après la désactivation de la mutualisation. Toutes les données des utilisateurs restent dans le système, mais l'administrateur ne peut pas ajouter d'utilisateurs pour des membres spécifiques jusqu'à ce que la mutualisation soit à nouveau activée.

À partir de maintenant, ce guide de l'utilisateur indiquera chaque fois qu'une action utilisateur est limitée à certains rôles utilisateur particuliers. Par exemple :

Droits d'accès : Administrateur serveur

3.2. Gérer les utilisateurs avec le Gestionnaire des utilisateurs UXP

Le gestionnaire des utilisateurs UXP est le principal système de gestion des utilisateurs pour les serveurs de sécurité. Chaque serveur de sécurité dispose de son propre système de gestion des utilisateurs UXP. Cela signifie que si une personne doit accéder à plusieurs serveurs de sécurité, elle doit disposer d'un compte distinct sur chacun des serveurs de sécurité.

Pour afficher tous les utilisateurs dans le gestionnaire des utilisateurs UXP du serveur de sécurité, allez à la page **Comptes d'utilisateurs**.



La page **Comptes d'utilisateurs** ne répertorie que les utilisateurs du gestionnaire des utilisateurs UXP et non les utilisateurs du système Ubuntu qui ont également accès à l'interface utilisateur du serveur de sécurité si le module complémentaire `uxp-addon-identity-provider-pam` est installé et qu'ils disposent des groupes UXP appropriés. Pour gérer les utilisateurs du serveur de sécurité avec le gestionnaire des utilisateurs Ubuntu, voir la section [Gérer les utilisateurs avec le Gestionnaire des utilisateurs Ubuntu](#).

Le rôle **Administrateur serveur** est responsable de la gestion des utilisateurs sur le serveur de sécurité.

3.2.1. Ajouter un utilisateur

Droits d'accès : Administrateur serveur

Pour ajouter un nouvel utilisateur, procédez comme suit.

1. Accédez à la page **Comptes d'utilisateurs**.
2. Cliquez sur **Ajouter un utilisateur**.
3. Saisissez le nom d'utilisateur et le mot de passe.
4. Attribuez des rôles à l'utilisateur.



Lors de l'ajout d'un nouvel Administrateur serveur, le rôle de Responsable des clés est automatiquement sélectionné afin de s'assurer que l'administrateur dispose des privilèges nécessaires pour gérer le serveur. Vous pouvez modifier cela avant de confirmer l'ajout d'un utilisateur.

Vous pouvez également créer un utilisateur sans lui attribuer de rôle, mais celui-ci ne pourra pas se connecter tant qu'au moins un rôle ne lui aura été attribué.



Lorsque la mutualisation est activée, vous pouvez ajouter des utilisateurs qui n'ont accès qu'à des membres spécifiques du serveur.

Bien que vous ne puissiez initialement attribuer qu'un seul membre à l'utilisateur, vous pouvez ajouter d'autres membres ultérieurement en modifiant les rôles de l'utilisateur, voir la section [Changer les rôles des utilisateurs](#).

5. Cliquez sur **Ajouter un utilisateur**.
6. Partagez le nom d'utilisateur et le mot de passe avec l'utilisateur.
Il est important de veiller à la sécurité lors de la distribution des identifiants de connexion. Partagez-les en personne (ou par téléphone) ou par l'intermédiaire d'une application de messagerie ou de courrier électronique cryptée de bout en bout.

Lorsque l'utilisateur se connecte pour la première fois, il est invité à modifier son mot de passe avant de pouvoir accéder au serveur de sécurité.

3.2.2. Changer les rôles des utilisateurs

Droits d'accès : Administrateur serveur

1. Allez sur la page **Comptes d'utilisateurs**, trouvez l'utilisateur dont vous souhaitez changer les rôles.
2. Cliquez sur **Modifier les rôles**.
3. Sélectionnez et désélectionnez les rôles.
4. Cliquez sur **Enregistrer les changements**. Si vous souhaitez annuler les changements, cliquez plutôt sur **Annuler**.

Lorsque la mutualisation est activée, vous pouvez modifier l'accès des utilisateurs à des membres spécifiques en suivant les étapes ci-dessous :

1. Allez sur la page **Comptes d'utilisateurs**, trouvez l'utilisateur dont vous souhaitez changer les rôles.
2. Cliquez sur **Modifier les rôles**.
 - Pour ajouter un nouveau membre à l'utilisateur :
 - cliquez sur **Ajouter un membre**.
 - sélectionnez des rôles pour le nouveau membre.
 - Pour modifier les rôles d'un utilisateur pour un membre existant :
 - sélectionnez et désélectionnez les rôles du membre.
 - Pour supprimer les rôles de l'utilisateur pour le membre :
 - cliquez sur l'icône **Supprimer** sur la ligne du membre ou désélectionnez toutes les cases des rôles de ce membre.
3. Cliquez sur **Enregistrer les changements**. Si vous souhaitez annuler les changements, cliquez plutôt sur **Annuler**.

Le changement de rôle de l'utilisateur le déconnectera de sa session active, ce qui l'obligera à se reconnecter.

3.2.3. Supprimer un utilisateur

Droits d'accès : Administrateur serveur

Un administrateur serveur peut supprimer des comptes utilisateur du serveur de sécurité, y compris ceux d'autres administrateurs serveur.

Pour supprimer un compte d'utilisateur du serveur de sécurité, procédez comme suit.

1. Allez à la page **Comptes d'utilisateurs**, recherchez l'utilisateur que vous souhaitez supprimer.
2. Cliquez sur **Supprimer** et confirmez.



Les administrateurs serveur ne peuvent pas supprimer leur propre compte afin d'éviter les verrouillages accidentels.

3.2.4. États des utilisateurs

L'état de l'utilisateur dans le système de gestion des utilisateurs indique si l'utilisateur peut accéder au serveur de sécurité ou non. Les états sont les suivants :

- Actif — L'utilisateur peut se connecter et accéder aux fonctionnalités du serveur de sécurité s'il a également des rôles actifs.
- Non activé — L'utilisateur peut se connecter. L'utilisateur doit changer le mot de passe pour activer le compte et accéder aux fonctionnalités du serveur de sécurité.
- Verrouillé — L'utilisateur a saisi son mot de passe de manière incorrecte un trop grand nombre de fois. L'utilisateur est temporairement exclu du serveur de sécurité. Le déverrouillage se fait automatiquement et ne nécessite pas l'intervention de l'administrateur.
- Bloqué — L'administrateur serveur a bloqué l'utilisateur. L'utilisateur ne peut pas accéder au serveur de sécurité jusqu'à ce que l'administrateur le débloque.

3.2.5. Bloquer et débloquer un utilisateur

Droits d'accès : Administrateur serveur

Pour empêcher temporairement un utilisateur d'accéder au serveur de sécurité, vous pouvez le bloquer. Un utilisateur bloqué ne peut pas se connecter ou accéder à l'API du serveur de sécurité.

1. Allez à la page **Comptes d'utilisateurs**, recherchez l'utilisateur que vous souhaitez bloquer ou débloquer.
 - Pour **bloquer** un utilisateur, cliquez sur **Bloquer** et confirmez.

- Pour **débloquer** un utilisateur, cliquez sur **Débloquer** et confirmez.

Le blocage d'un utilisateur le déconnectera de sa session.



Les administrateurs serveur ne peuvent pas bloquer ou débloquent leur propre compte afin d'éviter tout verrouillage accidentel.

3.2.6. Réinitialiser un mot de passe

Droits d'accès : Administrateur serveur

Si un utilisateur a oublié son mot de passe ou si le mot de passe a été divulgué, vous pouvez réinitialiser le mot de passe de l'utilisateur en lui attribuant un mot de passe temporaire.

1. Allez sur la page **Comptes d'utilisateurs**, trouvez l'utilisateur dont vous souhaitez réinitialiser le mot de passe.
2. Cliquez sur **Réinitialiser le mot de passe**.
3. Saisissez le mot de passe temporaire et cliquez sur **Réinitialiser le mot de passe**.
4. Partagez le mot de passe temporaire avec l'utilisateur.
Il est important de veiller à la sécurité lors de la distribution des identifiants de connexion. Partagez-les en personne (ou par téléphone) ou par l'intermédiaire d'une application de messagerie ou de courrier électronique cryptée de bout en bout.

La réinitialisation du mot de passe d'un utilisateur le déconnectera de sa session, l'obligeant à se reconnecter avec le mot de passe temporaire. L'utilisateur est invité à modifier son mot de passe avant de pouvoir accéder au serveur de sécurité.



Pour des raisons de sécurité, les administrateurs serveur ne peuvent pas réinitialiser leur propre mot de passe. Utilisez la fonction [Changer le mot de passe](#) ou contactez un autre administrateur serveur.

3.2.7. Ajouter un compte d'administrateur serveur sans accès à l'interface utilisateur

Droits d'accès : privilèges de l'utilisateur root

Si aucun administrateur serveur ne peut accéder à l'interface utilisateur du serveur de sécurité, il est possible d'ajouter de nouveaux administrateurs serveur à partir de l'interface de ligne de commande du serveur.

Il est recommandé de n'utiliser cette option qu'en cas de verrouillage et non comme méthode principale de gestion des utilisateurs. Utilisez le script pour ajouter un nouvel administrateur serveur qui peut continuer à gérer d'autres comptes dans le gestionnaire des utilisateurs UXP.

Pour ajouter un compte d'administrateur serveur :

```
sudo uxp-idp-usermgmt add-user <username>
```

Le script créera un administrateur serveur avec les rôles de Responsable des clés et de Responsable des services.

3.2.8. Bloquer un utilisateur sans accès à l'interface utilisateur

Droits d'accès : privilèges de l'utilisateur root

Vous pouvez bloquer un utilisateur :

```
sudo uxp-idp-usermgmt block <username>
```

Débloquer un utilisateur :

```
sudo uxp-idp-usermgmt unblock <username>
```

3.2.9. Mécanisme de protection de la connexion

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. Par défaut, après cinq échecs consécutifs, le serveur déconnecte l'utilisateur pendant 15 minutes. Ces valeurs peuvent être modifiées dans les paramètres du système.

3.3. Gérer les utilisateurs avec le Gestionnaire des utilisateurs Ubuntu

3.3.1. Commandes du Gestionnaire des utilisateurs Ubuntu

Droits d'accès : privilèges de l'utilisateur root



Depuis la version 1.24, Serveur de sécurité UXP prend en charge la gestion intégrée des utilisateurs UXP, voir [Gérer les utilisateurs avec le Gestionnaire des utilisateurs UXP](#). La gestion des utilisateurs du serveur de sécurité avec les utilisateurs Ubuntu et l'authentification via l'interface PAM est obsolète et sera progressivement supprimée dans les prochaines versions.

Si vous devez utiliser l'ancienne solution, installez le support d'authentification PAM :

```
sudo apt update
sudo apt install uxp-addon-identity-provider-pam
```

La migration des utilisateurs Ubuntu vers le gestionnaire des utilisateurs UXP est traitée dans le guide de mise à jour du serveur de sécurité [\[UXP-UPG-SS\]](#), voir la section concernant la mise à jour de la version 1.21 à la version 1.24.

Lorsque les gestionnaires des utilisateurs Ubuntu et UXP sont utilisés en parallèle pour accéder au serveur de sécurité, celui-ci donne la priorité au gestionnaire des utilisateurs

UXP lors de l'authentification des utilisateurs. Par conséquent, si le gestionnaire des utilisateurs Ubuntu et UXP ont tous deux un utilisateur avec le même nom d'utilisateur, l'utilisateur Ubuntu ne peut pas se connecter. Gardez cela à l'esprit lorsque vous donnez des noms aux utilisateurs.



Si vous disposez d'un serveur de sécurité mutualisé, toute personne disposant d'un compte utilisateur Responsable des services ou Auditeur de transactions créé dans le gestionnaire des utilisateurs Ubuntu peut accéder aux services et transactions de tous les membres du serveur. Pour voir clairement les autorisations des utilisateurs, n'utilisez pas le gestionnaire des utilisateurs Ubuntu sur un serveur de sécurité mutualisé. Migrez les utilisateurs vers le gestionnaire des utilisateurs UXP.

La gestion des utilisateurs avec les utilisateurs du système Ubuntu s'effectue en ligne de commande avec les privilèges d'utilisateur root.

Pour ajouter un nouvel utilisateur, exécutez la commande suivante :

```
sudo adduser <username>
```

Pour accorder des privilèges à l'utilisateur que vous avez créé, ajoutez-le aux groupes système correspondants, par exemple :

```
sudo adduser <username> uxp-server-administrator
sudo adduser <username> uxp-service-administrator
sudo adduser <username> uxp-transaction-auditor
```



Le gestionnaire des utilisateurs Ubuntu n'a pas de rôle distinct pour le Responsable des clés. Lorsque le compte Administrateur serveur est créé dans le gestionnaire des utilisateurs Ubuntu, l'Administrateur serveur dispose de privilèges de gestion des clés.



Utilisez uxp-service-administrator pour le rôle de Responsable des services.

Pour afficher les utilisateurs qui peuvent accéder à l'interface utilisateur du serveur de sécurité :

```
getent group | grep '^uxp-'
```

Pour connaître les rôles d'un utilisateur :

```
groups <username>
```

Pour supprimer les privilèges d'un utilisateur, retirez-le du groupe système correspondant, par exemple :

```
sudo deluser <username> uxp-server-administrator
```

Pour supprimer un utilisateur, entrez :

```
sudo deluser <username>
```

3.3.2. Mécanisme de protection de la connexion d'Ubuntu

Droits d'accès : privilèges de l'utilisateur root

Pour limiter les attaques par force brute sur la connexion, le serveur de sécurité restreint les tentatives d'authentification de l'utilisateur après un certain nombre d'échecs consécutifs. Pour les utilisateurs d'Ubuntu, le nombre d'échecs avant le verrouillage et la durée du verrouillage sont contrôlés par les paramètres du système Ubuntu.



Pour les utilisateurs dans le gestionnaire des utilisateurs UXP, les paramètres par défaut du verrouillage sont différents et contrôlés par les paramètres du système UXP (voir la section [Mécanisme de protection de la connexion](#)).

Par défaut, l'utilisateur est bloqué pendant 10 minutes après trois échecs consécutifs d'authentification en l'espace de 15 minutes. Ces paramètres et d'autres peuvent être modifiés dans le fichier `/etc/security/faillock.conf`. Par exemple, pour modifier le nombre de tentatives d'authentification échouées pour déclencher le verrouillage à 5, vous devez décommenter et modifier le paramètre `deny`.

Avant

```
# Deny access if the number of consecutive authentication failures
# for this user during the recent interval exceeds n tries.
# The default is 3.
# deny = 3
```

Après

```
# Deny access if the number of consecutive authentication failures
# for this user during the recent interval exceeds n tries.
# The default is 3.
deny = 5
```

De même, pour modifier l'intervalle pendant lequel les échecs sont comptés, modifiez le paramètre `fail_interval`. Le paramètre `unlock_time` détermine la durée du verrouillage.

4. Enregistrement du serveur de sécurité

Pour utiliser un serveur de sécurité pour l'échange de messages, vous devez connecter le serveur de sécurité à l'instance UXP.

La configuration initiale du serveur de sécurité couvrait tout ce qui était nécessaire à l'enregistrement du serveur, mais si l'une des étapes a été ignorée, vous pouvez terminer l'enregistrement en suivant les instructions des sections suivantes.

L'enregistrement du serveur nécessite une communication avec deux institutions :

1. Un service de certification approuvé par l'autorité de gouvernance UXP doit certifier le serveur de sécurité et son propriétaire, ce qui inclut :
 - ajouter une clé de signature et un certificat pour le propriétaire du serveur de sécurité ;
 - ajouter une clé d'authentification et un certificat pour le serveur de sécurité.
2. Vous devez enregistrer le serveur de sécurité auprès de l'autorité de gouvernance UXP.

Les étapes sont expliquées dans les sections suivantes.

4.1. Ajouter une clé de signature et un certificat pour le propriétaire du serveur de sécurité

Droits d'accès : Responsable des clés du propriétaire du serveur



Lorsque vous devez stocker la clé de signature du propriétaire sur un dispositif de création de signature, assurez-vous que vous avez connecté le dispositif et ajouté un jeton matériel au serveur de sécurité. Suivez les instructions de la section [Dispositifs de création de signature](#).



Vous pouvez générer les fichiers CSR et les transmettre immédiatement au service de certification.

1. Allez sur la page **Clés et certificats** ou sur la page **Clés du membre** du propriétaire du serveur et [générez une clé et une CSR](#) : sélectionnez **Signature** pour l'utilisation de la clé et le propriétaire du serveur de sécurité en tant que membre qui possèdera le certificat.
2. Transmettez le fichier CSR au service de certification et attendez le certificat.
3. [Importez le certificat de signature reçu](#) sur le serveur de sécurité.

4.2. Ajouter une clé d'authentification et un certificat pour le serveur de sécurité

Droits d'accès : Responsable des clés du propriétaire du serveur

1. Allez sur la page **Clés et certificats** ou sur la page **Clés du membre** du propriétaire du serveur, puis [générez une clé et une CSR](#) sur le jeton logiciel : sélectionnez **Authentification** pour l'utilisation de la clé.
2. Transmettez le fichier CSR au service de certification et attendez le certificat.
3. [Importez le certificat d'authentification reçu](#) sur le serveur de sécurité.

4.3. Enregistrer un serveur de sécurité auprès de l'autorité de gouvernance UXP



La demande d'enregistrement du serveur de sécurité est signée avec la clé de signature du propriétaire du serveur et la clé d'authentification du serveur. Il faut donc s'assurer que les certificats correspondants sont importés sur le serveur de sécurité et qu'ils fonctionnent :

- le jeton détenant les clés est connecté ;
- les réponses OCSP des certificats sont `good` ;
- les certificats sont actifs.

Pour enregistrer le serveur de sécurité auprès de l'autorité de gouvernance UXP, vous devez :

1. [Envoyer une demande d'enregistrement de certificat d'authentification](#) depuis le serveur de sécurité.
2. Soumettre une demande d'enregistrement du serveur de sécurité à l'autorité de gouvernance UXP conformément aux procédures organisationnelles de votre instance UXP. Vous devez transmettre le certificat d'authentification et le code du serveur.
3. Attendre que l'autorité de gouvernance UXP approuve la demande d'enregistrement.

Une fois que l'autorité de gouvernance UXP a approuvé l'enregistrement, l'état d'enregistrement du certificat passe à « Enregistré » et le processus d'enregistrement du serveur de sécurité est terminé.

Si l'autorité de gouvernance UXP rejette la demande d'enregistrement du certificat, le certificat restera dans l'état « Enregistrement en cours » et l'autorité de gouvernance vous informera du rejet par des moyens indépendants d'UXP.

5. Clients du serveur de sécurité

Les services UXP sont liés aux sous-systèmes des membres UXP. Pour qu'un sous-système puisse se connecter à UXP par l'intermédiaire d'un serveur de sécurité, le sous-système doit être ajouté en tant que client du serveur de sécurité. Pour ajouter un sous-système en tant que client sur un serveur de sécurité :

- Vous devez ajouter l'identifiant du sous-système au serveur de sécurité et enregistrer l'association entre le sous-système et le serveur de sécurité auprès de l'autorité de gouvernance UXP.
- Un fournisseur de services de certification, agréé par l'autorité de gouvernance, doit certifier le propriétaire du sous-système. Cela signifie que chaque membre UXP qui a des sous-systèmes sur un serveur de sécurité doit avoir un certificat de signature sur ce même serveur de sécurité.

5.1. Ajouter un client de serveur de sécurité

Droits d'accès : Administrateur serveur

Pour ajouter un client au serveur de sécurité, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**.
2. Cliquez sur **Ajouter un client**. Dans la fenêtre qui s'ouvre, entrez manuellement l'identifiant du client ou cliquez sur **Sélectionner le client dans la liste globale** et recherchez le client parmi tous les membres UXP et leurs sous-systèmes.



Le code membre et le code sous-système sont limités au jeu de caractères [a-zA-Z0-9_-].

3. Cliquez sur **Ajouter** une fois les informations du client saisies.

Le nouveau client est enregistré en tant que client du serveur de sécurité, mais cela n'est pas encore visible pour les autres membres UXP. Pour que les autres membres de UXP sachent que ce sous-système utilise ce serveur de sécurité, vous devez [enregistrer le client](#).

5.2. Configurer une clé de signature et un certificat pour un client du serveur de sécurité

Pour signer les messages sortants au nom d'un client du serveur de sécurité, le serveur de sécurité doit disposer d'une clé de signature et d'un certificat pour le client (sous-système).

Les certificats ne sont pas délivrés aux sous-systèmes eux-mêmes : un certificat de signature est attribué à un membre UXP et est utilisé pour tous ses sous-systèmes. Par conséquent, il n'est pas nécessaire d'ajouter un nouveau certificat de signature lors de l'ajout d'un client pour un membre qui dispose déjà d'un certificat de signature et d'une clé sur ce

serveur de sécurité.

Vous pouvez voir si chaque membre UXP dispose d'un certificat de signature fonctionnel sur la page **Clients du serveur de sécurité**. Si vous devez ajouter une nouvelle clé de signature et un nouveau certificat (il n'y a pas de certificat ou il a expiré), [commencez par générer une clé et une CSR](#).

5.3. Enregistrer un client du serveur de sécurité auprès de l'autorité de gouvernance UXP

Pour enregistrer un client de serveur de sécurité auprès de l'autorité de gouvernance UXP, vous devez suivre les étapes suivantes :

1. [Soumettez une demande d'enregistrement de client de serveur de sécurité](#) à partir du serveur de sécurité.
2. Soumettez une demande d'enregistrement du client à l'autorité de gouvernance UXP conformément aux procédures organisationnelles de votre instance UXP. Vous devez indiquer qui est le propriétaire et quel est le code du serveur de sécurité, ainsi que le code du sous-système du nouveau client.
3. Attendez que l'autorité de gouvernance UXP approuve la demande d'enregistrement.

5.3.1. Enregistrer un client du serveur de sécurité

Droits d'accès : Administrateur serveur

Pour soumettre une demande d'enregistrement de client, suivez les étapes suivantes :

1. Accédez à la page **Clients du serveur de sécurité**.
2. Recherchez un client que vous souhaitez enregistrer (il doit être dans l'état « Sauvegardé ») et cliquez sur l'icône **Détails**.
3. Sur la page **Détails du client** qui s'ouvre, cliquez sur **Enregistrer** et confirmer.
L'état du client passe à « Enregistrement en cours ».

Une fois que l'autorité de gouvernance UXP a approuvé l'enregistrement du client, le client passe à l'état « Enregistré » sur le serveur de sécurité et le processus d'enregistrement est terminé.

Si l'autorité de gouvernance UXP rejette la demande d'enregistrement du client, le client restera dans l'état « Enregistrement en cours » et l'autorité de gouvernance vous informera du rejet par des moyens indépendants d'UXP.

5.4. Supprimer un client du Serveur de sécurité

Si un client est supprimé du serveur de sécurité, toutes les informations relatives à ce client sont également supprimées du serveur, c'est-à-dire tous les services, les droits d'accès et, le cas échéant, les certificats.

Pour supprimer un client enregistré ou en cours d'enregistrement, vous devez le désenregistrer avant de pouvoir le supprimer.

5.4.1. Désenregistrer un client

Droits d'accès : Administrateur serveur

Pour désenregistrer un client, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**.
2. Sélectionnez le client que vous souhaitez désenregistrer du serveur et cliquez sur l'icône **Détails** sur la ligne du client.
3. Sur la page **Détails du client** qui s'ouvre, cliquez sur **Désenregistrer** et confirmez. Le serveur de sécurité envoie au serveur de registre une demande de désenregistrement du client et le serveur de registre désenregistre automatiquement le client.
4. Le serveur de sécurité vous demandera si vous souhaitez supprimer le client et toutes ses informations du serveur de sécurité. Vous pouvez soit supprimer le client maintenant, soit le conserver (par exemple, pour migrer les informations relatives au service), mais vous ne pouvez pas réenregistrer le client avant de l'avoir supprimé et ajouté à nouveau.



Si vous ne pouvez pas envoyer une demande de désenregistrement d'un client à partir du serveur de sécurité (par exemple, si vous ne disposez pas d'un certificat d'authentification fonctionnel), vous pouvez demander à l'autorité de gouvernance UXP de désenregistrer le client sur le serveur de registre. Si le client a été désenregistré du serveur de registre sans demande du serveur de sécurité, le serveur de sécurité affiche le client dans l'état « Erreur globale ».

5.4.2. Supprimer un client

Droits d'accès : Administrateur serveur



Vous devez désenregistrer les clients enregistrés ou en cours d'enregistrement avant de pouvoir les supprimer (voir la section [Désenregistrer un client](#)).

Pour supprimer un client, procédez comme suit.

1. Accédez à la page **Clients du serveur de sécurité**.
2. Sélectionnez un client que vous souhaitez supprimer du serveur de sécurité et cliquez sur l'icône **Détails** de cette ligne.
3. Sur la page **Détails du client** qui s'ouvre, cliquez sur **Supprimer** et confirmez.
4. S'il s'agissait du dernier client de ce membre, le serveur de sécurité proposera également de supprimer les certificats associés à ce membre.

5.5. États du client du serveur de sécurité

Le serveur de sécurité distingue les états suivants pour les clients.

○ **Sauvegardé** – les informations du client ont été saisies sur le serveur de sécurité, mais l'association entre le client et le serveur de sécurité n'est pas enregistrée par l'autorité de gouvernance UXP. (Si l'association est enregistrée sur le serveur de registre avant l'ajout du client au serveur de sécurité, le client passera à l'état « Enregistré » juste après son ajout) Lorsqu'un client est sauvegardé :

- Vous pouvez envoyer une demande d'enregistrement du client depuis le serveur de sécurité vers le serveur de registre (voir [Enregistrement d'un client du serveur de sécurité](#)). Le nouvel état sera « Enregistrement en cours ».
- Vous pouvez supprimer le client.

● **Enregistrement en cours** – une demande d'enregistrement du client a été envoyée au serveur de registre, mais l'autorité de gouvernance UXP n'a pas encore approuvé l'association entre le client et le serveur de sécurité. Lorsqu'un enregistrement client est en cours :

- Vous pouvez attendre que l'autorité de gouvernance UXP approuve l'association entre le client et le serveur de sécurité. Une fois cette opération effectuée, le nouvel état sera « Enregistré ».
- Vous pouvez envoyer une demande de désenregistrement du client du serveur de sécurité au serveur de registre (voir [Désenregistrement d'un client](#)). Le nouvel état sera « Suppression en cours ».

● **Enregistré** – l'autorité de gouvernance UXP a approuvé l'association entre le client et le serveur de sécurité. Dans cet état, le client peut fournir et utiliser les services UXP (en supposant que toutes les autres conditions préalables soient remplies). Lorsqu'un client est enregistré :

- L'autorité de gouvernance UXP peut révoquer l'association entre le client et le serveur de sécurité sur le serveur de registre. Le nouvel état sera « Erreur globale ».
- Vous pouvez envoyer une demande de désenregistrement du client du serveur de sécurité au serveur de registre (voir [Désenregistrement d'un client](#)). Le nouvel état sera « Suppression en cours ».

○ **Erreur globale** – l'autorité de gouvernance a révoqué l'association entre le client et le serveur de sécurité. Lorsqu'un client présente une erreur globale :

- L'autorité de gouvernance UXP peut restaurer l'association entre le client et le serveur de sécurité. L'état sera à nouveau « Enregistré ».
- Vous pouvez supprimer le client.

● **Suppression en cours** – une demande de désenregistrement du client a été envoyée par le serveur de sécurité au serveur de registre. Lorsqu'une suppression de client est en cours :

- Vous pouvez supprimer le client.

6. Architecture mutualisée



Les directives de cette section ne s'appliquent que si la mutualisation est activée sur le serveur de sécurité. Pour vérifier si votre licence autorise la mutualisation, rendez-vous sur la page Licence.

Cette section explique comment gérer plusieurs membres UXP au sein d'un seul serveur de sécurité à l'aide de la fonctionnalité de mutualisation. Elle couvre la mise en place et l'administration des membres, qu'ils gèrent leurs propres ressources ou qu'ils délèguent des responsabilités à l'opérateur du serveur. Vous apprendrez à intégrer de nouveaux membres, à attribuer des rôles, à configurer le stockage sécurisé des clés, à établir des connexions de confiance et à exclure correctement des membres lorsque cela est nécessaire. Des instructions détaillées étape par étape pour chaque tâche sont toutefois disponibles dans les sections dédiées de ce guide.

Le modèle de fonctionnement du serveur de sécurité le plus simple est celui où un seul membre UXP utilise le serveur. Le membre est également le propriétaire du serveur de sécurité.

Afin de partager les frais d'administration du serveur entre les membres, le serveur de sécurité dispose d'une fonction de mutualisation qui permet d'héberger plusieurs membres UXP sur un seul serveur de sécurité sans que ces membres aient accès aux informations des autres. Lorsque la mutualisation est activée, chaque membre peut avoir ses propres Responsables des clés, Responsables des services et Auditeurs de transactions. Les membres peuvent également décider de déléguer une partie de la gestion à l'opérateur du serveur.

- Opérateur – l'organisation responsable de l'administration du serveur de sécurité, y compris de la maintenance du matériel et des logiciels, ainsi que du rôle d'Administrateur serveur.
- Locataire – membre UXP qui utilise le serveur de sécurité administré par l'opérateur. Le locataire peut gérer ses propres tâches au niveau des membres (gestion des services et signature des clés), mais il peut choisir de laisser l'opérateur se charger de ces tâches.

Les locataires sont indépendants au niveau des membres UXP. Lorsqu'un utilisateur est affecté à un membre, il peut consulter et gérer (dans le cadre de son rôle) toutes les informations de tous les sous-systèmes de ce membre sur le serveur de sécurité.

Lorsque vous placez plusieurs membres UXP sur un serveur de sécurité, n'oubliez pas que les ressources de traitement des messages du serveur sont partagées. Le trafic de tous les membres réunis ne doit pas dépasser la charge que le serveur peut supporter.

Lors de la mise en place de plusieurs serveurs de sécurité identiques pour la haute disponibilité (décrite dans le guide de la haute disponibilité et de l'équilibrage des charges [\[UXP-UG-SSHA\]](#)), chaque serveur dispose de sa propre base de données d'utilisateurs. Par conséquent, chaque utilisateur doit disposer d'un compte distinct sur chaque serveur.

6.1. Intégration d'un membre

6.1.1. Ajouter un membre

Ajoutez un sous-système du membre en tant que client du serveur de sécurité. Enregistrez le client sur le serveur de sécurité. L'enregistrement du client n'a pas encore besoin d'être confirmé par l'autorité compétente. Vous pouvez poursuivre avec les autres étapes de l'intégration.

6.1.2. Ajouter des utilisateurs

Déterminez si les employés du membre ont besoin d'accéder à l'interface utilisateur du serveur de sécurité. Cela dépend si le membre gère sa propre clé de signature et ses propres services, ou s'il délègue tout ou partie de cette responsabilité à l'opérateur du serveur.

Autogestion par le membre

- Si le membre doit gérer ses propres clés de signature, créez un compte d'utilisateur pour ce membre avec le rôle de Responsable des clés.
- Si le membre doit fournir des services et gérer ses propres services, ajoutez également un compte avec le rôle de Responsable des services. Ce rôle peut être attribué au même compte que le Responsable des clés.
- Si nécessaire, ajoutez un rôle d'Auditeur de transactions pour le membre. L'Auditeur de transactions pourra consulter les messages échangés avec succès par le membre. L'Auditeur des transactions pourra également télécharger l'intégralité du message. Il convient donc de garder à l'esprit la sécurité des informations lors de l'attribution de ce rôle.

Vous pouvez attribuer les rôles à un seul compte d'utilisateur ou les répartir entre plusieurs utilisateurs, en fonction de la manière dont le membre envisage de distribuer les responsabilités entre différentes personnes.

Le membre délègue la gestion à l'opérateur

Les membres peuvent également décider de déléguer une partie de la gestion à l'opérateur du serveur de sécurité. Si le membre a délégué la gestion des clés ou des services à l'opérateur, assurez-vous qu'un utilisateur dispose des privilèges de Responsable des clés et de Responsable des services pour ce membre. Cette tâche peut être accomplie par un utilisateur disposant des privilèges de Responsable des clés, de Responsable des services ou d'Auditeur de transactions pour tous les membres du serveur. Vous pouvez également attribuer le membre à un utilisateur existant qui gère déjà un autre membre, ce qui lui permet de gérer les deux.



Lorsque vous utilisez la gestion des utilisateurs Ubuntu pour le serveur de sécurité, gardez à l'esprit que tous les utilisateurs Ubuntu qui ont les rôles Responsable des services et Auditeur de transactions peuvent accéder aux services et aux transactions de tous les membres du serveur de sécurité. Ainsi, sur un serveur de sécurité mutualisé, pour avoir une vision claire des privilèges des utilisateurs, il n'est pas recommandé d'utiliser la gestion des utilisateurs Ubuntu en parallèle avec le gestionnaire des

utilisateurs UXP.

6.1.3. Choisir le stockage pour les clés de signature des membres

Déterminez l'endroit où la clé de signature du membre sera stockée. La législation ou le membre UXP lui-même peut exiger que la clé de signature soit stockée sur un dispositif externe de création de signature afin d'assurer une protection supplémentaire de la clé privée.

Le membre s'autogère sur le dispositif de création de signature externe

Si le membre dispose de son propre dispositif externe de création de signature pour la clé de signature, connectez le dispositif au serveur et associez un jeton du dispositif au membre UXP. Si le dispositif dispose déjà d'une clé de signature avec certificat, déterminez le jeton du dispositif qui possède la clé. L'ajout du jeton au serveur le rendra disponible au Responsable des clés du membre, qui pourra alors importer le certificat du jeton vers le serveur.

Si le membre ne dispose pas de son propre dispositif externe, mais que l'opérateur du serveur de sécurité lui en fournit un, attribuez-lui un jeton à partir de ce dispositif.

Le membre s'autogère grâce à un jeton logiciel intégré

Si le membre n'utilise pas de dispositif externe de création de signature, attribuez-lui un nouveau jeton logiciel. Allez dans **Clés et certificats**, puis choisissez **Ajouter un jeton**. Le serveur de sécurité est livré avec neuf jetons logiciels intégrés supplémentaires. Attribuez l'un d'entre eux au membre. Avant que le Responsable des clés ne puisse utiliser le nouveau jeton logiciel, il doit définir le code PIN du jeton.

Si les neuf jetons logiciels supplémentaires ne suffisent pas, vous pouvez créer d'autres jetons logiciels en ajoutant de nouveaux dossiers dans le dossier `/etc/uxp/signer/`.

Par exemple :



```
sudo mkdir /etc/uxp/signer/10
```

Donnez ensuite à l'utilisateur système `uxp` l'accès au nouveau dossier :

```
sudo chown uxp:uxp /etc/uxp/signer/10
```

Redémarrer les services :

```
sudo systemctl restart uxp-securityserver-rest-api
```

Le membre délègue la gestion des clés à l'opérateur

En tant qu'opérateur, vous pouvez choisir sur quel jeton gérer la clé du membre. Le jeton ne doit pas nécessairement appartenir au membre, mais vous devez avoir le rôle de Responsable des clés pour ce membre. S'il est possible que le membre commence à gérer sa clé de signature à l'avenir, il est préférable de créer un jeton distinct pour ce membre.

Utilisez un jeton matériel ou logiciel, comme convenu avec le membre.

6.1.4. Connexion sécurisée entre le système d'information des membres et le serveur de sécurité

Lorsque le serveur de sécurité est utilisé par une organisation, il peut partager le segment de réseau interne avec les systèmes d'information et une connexion HTTP non sécurisée peut alors suffire pour tester et développer les services. Lorsque le serveur est hébergé par l'opérateur et que les systèmes d'information du locataire se trouvent sur un autre réseau, éventuellement accessible via Internet, il est essentiel d'établir une connexion TLS sécurisée entre le serveur de sécurité et les systèmes d'information.

Lorsque les locataires disposent de leurs propres Responsable des services, ils peuvent activer la connexion HTTPS et échanger les certificats du système d'information et du serveur de sécurité, afin que les deux systèmes puissent s'authentifier mutuellement.

Par ailleurs, lorsque le locataire n'est qu'un client du service et n'a donc pas besoin d'un Responsable des services, ou lorsque le locataire a délégué la gestion du service à l'opérateur, ce dernier est chargé de sécuriser la connexion entre le serveur de sécurité et le système d'information.

6.2. Désengagement d'un membre

Pour désengager un membre du serveur, vous devez supprimer manuellement tous les objets membres UXP :

- désenregistrez et supprimez les sous-systèmes du membre ;
- supprimez le membre des rôles des utilisateurs ;
- supprimez les comptes utilisateurs qui disposaient de privilèges uniquement pour ce membre ;
- supprimez tous les jetons appartenant au membre ;
- supprimez les dispositifs du membre.

7. Clés de signature

Chaque membre UXP a besoin d'une clé de signature avec un certificat sur le serveur de sécurité. Le serveur utilise la clé de signature pour émettre des signatures numériques aux messages du membre UXP.

Pour voir les clés de signature et les certificats du membre, accédez à sa page **Clés du membre**. Vous verrez les clés sur les jetons correspondants. Si le membre dispose de clés sur des jetons auxquels vous n'avez pas accès, vous verrez uniquement ces clés.

7.1. Jetons

Les jetons sont des supports permettant de protéger les clés cryptographiques utilisées par le serveur de sécurité. Les clés sur les jetons sont protégées par un code PIN. Le serveur de sécurité ne peut utiliser les clés d'un jeton que lorsque le code PIN est saisi (le jeton est connecté). Lorsque le jeton est déconnecté, par exemple lors du redémarrage du serveur, il est important de le reconnecter dès que possible pour rétablir l'échange de messages.

Le serveur de sécurité distingue deux types de jetons en fonction de leur emplacement physique :

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

Chaque jeton du serveur de sécurité appartient à un membre UXP.



Le Responsable des clés du propriétaire du jeton peut créer de nouvelles clés sur le jeton et importer des certificats. Les clés et les certificats ne doivent pas nécessairement appartenir au propriétaire du jeton, mais le Responsable des clés doit avoir des privilèges pour le membre dont il veut gérer les clés.

Dans les détails du jeton, vous pouvez :

- renommer le jeton ;
- afficher le type de jeton (jeton logiciel ou matériel) ;
- si le jeton est un jeton matériel, afficher le nom du dispositif sur lequel se trouve le jeton ;
- afficher si le jeton est en lecture seule (dans ce cas, il n'est pas possible de créer de nouvelles clés sur le jeton, le jeton doit déjà avoir une clé et un certificat et vous devez [importer le certificat sur le serveur de sécurité](#)) ;
- afficher les [algorithmes de clés](#) pris en charge par le jeton.

7.1.1. Jetons logiciels

Un jeton logiciel peut être utilisé lorsqu'il n'est pas nécessaire d'utiliser un dispositif externe pour protéger la clé de signature. L'Administrateur serveur attribue des jetons logiciels aux

membres.

Pour commencer à utiliser le jeton logiciel :

1. Définissez le code PIN du jeton s'il n'en a pas encore.
2. [Générez une clé et une CSR.](#)
3. Demandez un certificat à une autorité de certification.
4. [Importez le fichier de certificat sur le serveur.](#)

Il est important de se souvenir du code PIN du jeton ou de le conserver en toute sécurité dans un gestionnaire de mots de passe. Lorsque le PIN est oublié et que le jeton est déconnecté (ce qui se produit lors du redémarrage du serveur), les clés du jeton ne peuvent pas être utilisées ou restaurées sans le PIN.

7.1.2. Jetons matériels

Les jetons matériels sont utilisés lorsque la clé de signature se trouve sur un dispositif externe (HSM, jeton USB). L'Administrateur serveur connecte le dispositif de création de signature au serveur de sécurité et attribue un jeton du dispositif au membre.

Le Responsable des clés doit connaître le code PIN du jeton.

Il existe différents scénarios d'utilisation d'un jeton matériel, selon que la clé et le certificat sont déjà préparés ou que le jeton est vide.

Clé sur le dispositif et certificat sous forme de fichier

Si la clé se trouve sur le dispositif mais que le certificat a été remis sous forme de fichier, le Responsable des clés doit :

1. S'assurer que le jeton matériel est connecté et disponible.
2. [Importer le fichier de certificat sur le serveur.](#) Le serveur de sécurité recherche la clé sur le dispositif. S'il est trouvé, le serveur stocke le certificat et la référence à la clé sur le serveur de sécurité.

Clé et certificat sur le dispositif

Le dispositif peut être livré avec une clé et un certificat pré-générés. Dans ce cas, le Responsable des clés doit [importer le certificat depuis le dispositif vers le serveur.](#)

Pas de clé sur le dispositif

Si le jeton matériel ne dispose pas d'une clé et d'un certificat pré-générés, le Responsable des clés doit :

1. [Générer une clé et une CSR.](#)
2. Demander un certificat à une autorité de certification.
3. [Importer le fichier de certificat sur le serveur.](#)

7.2. Générer une clé et une CSR

Droits d'accès : Responsable des clés

La première étape de l'obtention d'un certificat de signature pour le serveur ou un membre UXP consiste à générer une clé et une demande de signature de certificat (CSR) correspondante à envoyer au service de certification.

Pour générer une clé et une CSR, procédez comme suit.

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre**.
2. Choisissez un jeton pour la clé. **Connectez-vous** au jeton si nécessaire.



Dans le cas d'un jeton matériel indisponible, verrouillé ou non initialisé, ce problème doit être résolu avant de pouvoir générer une clé.

3. Cliquez sur **Générer une clé et une CSR**.
4. Choisissez le type de clé (voir les options à la section [Types de clés](#)).
5. Choisissez le membre UXP qui sera le propriétaire de cette clé de signature.
6. Choisissez le service de certification qui délivrera le certificat.
7. Vous pouvez éventuellement attribuer un nom à la clé afin de la distinguer ultérieurement des autres clés.
8. Choisissez le format dans lequel vous souhaitez obtenir le fichier CSR (le service de certification peut exiger un format spécifique).
9. Si le nom distinctif de l'objet nécessite une entrée, remplissez le formulaire. En général, les valeurs sont saisies d'avance.
10. Cliquez sur **Générer**.
Le fichier CSR sera téléchargé automatiquement. Le CSR apparaîtra sous le jeton et vous pourrez télécharger le fichier à nouveau si nécessaire.

Transmettez le fichier CSR au fournisseur de services de certification. Après avoir reçu le certificat, [importez-le sur le serveur de sécurité](#).

7.3. Importer un fichier de certificat

Droits d'accès : Responsable des clés

Pour importer un fichier de certificat sur le serveur de sécurité, procédez comme suit.

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre**.
2. Recherchez le jeton où se trouve la clé (éventuellement aussi une CSR si vous en avez généré une). Assurez-vous que le jeton est connecté.
3. Cliquez sur **Importer un certificat**.
4. Choisissez **Importer un fichier**.

5. Recherchez le fichier de certificat sur votre ordinateur et cliquez sur **Importer**.



Si le serveur de sécurité ne peut pas trouver de clé pour le certificat téléchargé, assurez-vous que :

- vous avez téléchargé le bon fichier de certificat (vous pouvez ouvrir le fichier avec les outils de votre système d'exploitation et en lire le contenu) ;
- le dispositif et le jeton avec la clé sont ajoutés au serveur de sécurité, connectés et disponibles ;
- que le serveur de sécurité peut détecter la clé du dispositif (vous pouvez vérifier les clés sans certificat à l'aide du flux [Importation d'un certificat à partir d'un dispositif](#)). Recherchez la clé dont l'alias comprend l'identifiant de clé sujet du certificat.

Après l'importation du certificat, celui-ci apparaît sous le jeton. Si vous aviez une CSR, elle sera supprimée.

La clé de signature est prête à être utilisée dès l'importation du certificat. Aucune étape supplémentaire n'est nécessaire.



Les certificats ont une date d'expiration, après laquelle la clé associée devient inutilisable. Lorsqu'un certificat expire, vous devez obtenir une nouvelle clé et un nouveau certificat. Le serveur de sécurité affichera une alerte un mois avant l'expiration d'un certificat.

7.4. Importer un certificat depuis un dispositif

Droits d'accès : Responsable des clés

Si vous disposez déjà d'une paire de clés et de certificats que vous souhaitez utiliser sur le dispositif de création de signature, vous devez importer le certificat sur le serveur avant que ce dernier ne puisse utiliser la clé pour la signature.

Pour importer un certificat sur le serveur de sécurité à partir d'un dispositif, procédez comme suit.

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre**.
2. Recherchez le jeton matériel contenant la clé et le certificat. Si vous ne trouvez pas le jeton, l'Administrateur serveur doit d'abord ajouter le dispositif et le jeton au serveur de sécurité.
3. Assurez-vous que le jeton est connecté.
4. Cliquez sur **Importer un certificat**.
5. Choisissez **Importer à partir d'un dispositif**.
6. Recherchez le certificat et cliquez sur **Importer**.
Le certificat doit être un certificat de signature délivré à un membre du serveur de sécurité.

Une fois l'importation réussie, le certificat apparaît sous le jeton. La clé de signature est prête à être utilisée dès l'importation du certificat. Aucune étape supplémentaire n'est nécessaire.



Les certificats ont une date d'expiration, après laquelle la clé associée devient inutilisable. Lorsqu'un certificat expire, vous devez obtenir une nouvelle clé et un nouveau certificat. Le serveur de sécurité affichera une alerte un mois avant l'expiration d'un certificat.

7.5. Activer et désactiver les certificats

Droits d'accès : Responsable des clés

Le serveur de sécurité ne peut pas utiliser de certificats inactifs.

Si le serveur de sécurité dispose de plusieurs certificats actifs pour le même usage, il choisira l'un des certificats actifs.

Pour activer ou désactiver un certificat, recherchez le certificat que vous souhaitez activer ou désactiver et faites basculer le bouton sur la ligne du certificat.

7.6. Supprimer un certificat ou une demande de signature de certificat

Droits d'accès : Responsable des clés

Si le certificat ou la CSR était le seul certificat ou CSR associé à la clé, la clé est également supprimée.



Lors de la suppression de certificats ou de CSR avec des clés sur des jetons matériels, le serveur de sécurité essaiera de supprimer la clé du dispositif de création de signature. Lorsque le serveur de sécurité ne peut pas supprimer la clé du dispositif (par exemple, lorsque le serveur de sécurité ne peut pas accéder à la clé sur le dispositif ou que la clé est déjà supprimée du dispositif), vous pouvez continuer à supprimer le certificat/CSR et sa clé uniquement à partir du serveur de sécurité. La clé restera sur le dispositif (sauf si elle a déjà été supprimée).

Pour supprimer un certificat ou une CSR, recherchez le certificat ou la CSR que vous souhaitez supprimer et cliquez sur **Supprimer** et confirmer.

7.7. Validité d'un certificat

Les deux autres attributs qui déterminent si le serveur de sécurité peut utiliser un certificat sont la période de validité et la réponse OCSP.

La période de validité du certificat est déterminée par la date de délivrance et la date d'expiration. Un certificat est périmé lorsque la date d'expiration est dépassée.

La réponse OCSP indique si le certificat est toujours approuvé par le service de certification.

Un certificat de serveur de sécurité peut avoir l'une des réponses OCSP suivantes :

- **Inconnu** (informations de validité manquantes) – la dernière réponse OCSP était soit `unknown` (le répondeur ne connaît pas le certificat demandé), soit une erreur.
- **Suspendu** – la dernière réponse OCSP concernant le certificat était `suspended`.
- **Bon** (valide) – la dernière réponse OCSP concernant le certificat était `good`. Seuls les certificats à l'état `good` (valide) peuvent être utilisés pour signer des messages ou établir une connexion entre des serveurs de sécurité.
- **Révoqué** – la dernière réponse OCSP concernant le certificat était `revoked`. Le certificat n'est pas actif et aucune requête OCSP n'est effectuée à son sujet.
- **Périmé** – la dernière réponse OCSP est plus ancienne que la période de validité autorisée pour les réponses OCSP.
- **Non vérifié** – le serveur de sécurité n'interroge pas la réponse OCSP du certificat parce que celui-ci n'est pas utilisé (par exemple, le certificat est inactif ou n'est pas enregistré).

7.8. Types de clés

Vous pouvez générer huit types de clés différents sur le serveur de sécurité. Vous avez à votre disposition : trois courbes NIST standard pour les clés de l'algorithme de signature numérique à courbe elliptique (ECDSA), deux courbes Edwards standard pour les clés de l'algorithme de signature numérique à courbe d'Edwards (EdDSA), et trois longueurs de clés différentes pour les clés de l'algorithme de signature numérique RSA :

- NIST P-256 (également connue sous le nom de `secp256r1` ou `prime256v1`) ;
- NIST P-384 (également connue sous le nom de `secp384r1` ou `prime384v1`) ;
- NIST P-521 (également connue sous le nom de `secp521r1` ou `prime521v1`) ;
- Edwards 25519 (également connue sous le nom de `Ed25519`) ;
- Edwards 448 (également connue sous le nom de `Ed448`) ;
- RSA (2048) ;
- RSA (3072) ;
- RSA (4096) ;



Pour les jetons matériels, la liste des algorithmes pris en charge peut être plus courte en fonction des algorithmes pris en charge par le dispositif spécifique de création de signature.

Pour tous les types de clés, la taille de la clé publique détermine à la fois la sécurité des clés et la rapidité des opérations effectuées avec la clé. Les clés plus longues sont plus sûres mais plus lentes à effectuer des opérations.

Le National Institute of Standards and Technology (NIST) approuve les clés RSA (2048)

comme étant sûres jusqu'en 2030, et approuve toutes les autres clés utilisées par le serveur de sécurité [même au-delà de 2030 \[NIST\]](#).

Lorsque vous choisissez un type de clé pour une nouvelle clé, tenez compte des conseils donnés par l'autorité de gouvernance de votre UXP. Assurez-vous également que le type de clé choisi est pris en charge par votre autorité de certification.

8. Clés d'authentification

Le serveur de sécurité utilise une clé d'authentification et un certificat pour établir une connexion sécurisée, cryptée et mutuellement authentifiée avec d'autres serveurs de sécurité.

8.1. Générer une clé d'authentification et une CSR

Droits d'accès : Responsable des clés du propriétaire du serveur

Les clés d'authentification ne peuvent être stockées que sur le jeton logiciel intégré avec l'ID 0. Pour en générer, recherchez le jeton logiciel 0, [générez une nouvelle clé](#) et choisissez **authentification** pour l'utilisation de la clé. À l'aide du fichier CSR, demandez un certificat pour votre clé auprès d'un fournisseur de services de certification. [Importez le certificat reçu](#) sur le serveur.

Vous devez [enregistrer le certificat d'authentification](#) sur l'instance UXP avant que le serveur de sécurité puisse l'utiliser. L'enregistrement associera le certificat à votre serveur et publiera cette information aux autres membres UXP.

8.2. Enregistrer un certificat d'authentification

Droits d'accès : Administrateur serveur, Responsable des clés du propriétaire du serveur

Pour enregistrer un certificat d'authentification, vous devez envoyer une demande d'enregistrement de certificat à partir du serveur de sécurité :

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre** du propriétaire du serveur.
2. Sélectionnez un certificat à enregistrer (il doit être dans l'état « Sauvegardé ») et cliquez sur **Enregistrer**.
3. Saisissez le nom DNS public ou l'adresse IP du serveur de sécurité. La boîte de dialogue affiche également le port d'écoute du serveur de sécurité (voir [Port d'écoute \(transport\) du serveur de sécurité](#) pour plus d'informations).
4. Cliquez sur **Enregistrer**.
L'état du certificat est défini sur « Enregistrement en cours ».

Une fois que l'autorité de gouvernance UXP a approuvé l'enregistrement du certificat, le serveur de sécurité définit l'état du certificat sur « Enregistré » et peut commencer à utiliser le certificat (le certificat doit être actif).

Si l'autorité de gouvernance UXP rejette la demande d'enregistrement du certificat, le certificat restera dans l'état « Enregistrement en cours » et l'autorité de gouvernance vous informera du rejet par des moyens indépendants d'UXP. Vous pouvez ensuite supprimer le certificat.

8.3. Annuler l'enregistrement d'un certificat d'authentification

Droits d'accès : Administrateur serveur, Responsable des clés du propriétaire du serveur



Vous ne pouvez annuler que l'enregistrement des certificats d'authentification qui sont dans les états « Enregistré » ou « Enregistrement en cours ».

Pour annuler l'enregistrement d'un certificat d'authentification, recherchez le certificat que vous souhaitez annuler et cliquez sur **Annuler l'enregistrement**.

Ensuite, le serveur de sécurité envoie une demande au serveur de registre UXP et le serveur de registre annule automatiquement l'enregistrement du certificat. Le serveur de sécurité fait passer le certificat à l'état « Suppression en cours » et vous pouvez supprimer le certificat du serveur de sécurité.



Pour annuler l'enregistrement d'un certificat, il faut que le certificat d'authentification fonctionne (c'est-à-dire qu'il soit enregistré, que l'OCSP soit bon et qu'il soit actif).

Vous pouvez supprimer un certificat enregistré sur le serveur de registre sans envoyer de demande via le serveur de sécurité. Dans ce cas, vous devez informer l'administration du serveur de registre du certificat que vous souhaitez supprimer. Si l'administrateur du serveur de registre a supprimé le certificat du serveur de registre sans que le serveur de sécurité en ait fait la demande, le serveur de sécurité affiche le certificat dans l'état « Erreur globale ».

Si vous essayez d'annuler l'enregistrement d'un certificat alors qu'il n'y a pas de certificat d'authentification fonctionnel, le serveur de sécurité renvoie un message d'erreur et demande s'il faut continuer à supprimer le certificat du serveur de sécurité. Dans ce cas, le certificat reste connu sur le serveur de registre mais ne peut plus être utilisé.

8.4. Supprimer une clé d'authentification et un certificat

Droits d'accès : Responsable des clés du propriétaire du serveur

Lorsque le certificat est enregistré ou en cours d'enregistrement, vous devez [le désenregistrer du serveur de registre](#) avant de pouvoir supprimer la clé et le certificat du serveur de sécurité.

8.5. États d'enregistrement des certificats d'authentification

Les états d'enregistrement indiquent où se trouve un certificat d'authentification dans son cycle de vie d'enregistrement.

Les différents états sont les suivants :

○ **Sauvegardé** – le certificat a été importé sur le serveur de sécurité, mais il n'a pas encore été soumis pour enregistrement au serveur de registre. Lorsqu'un certificat est sauvegardé :

- Vous pouvez envoyer une demande d'enregistrement de certificat depuis le serveur de sécurité vers le serveur d'enregistrement (voir [Enregistrement d'un certificat d'authentification](#)). Le nouvel état sera « Enregistrement en cours ».

- Vous pouvez supprimer le certificat.

● **Enregistrement en cours** – une demande d'enregistrement de certificat a été envoyée au serveur de registre, mais l'autorité de gouvernance UXP n'a pas encore approuvé l'association entre le certificat et le serveur de sécurité. Lorsqu'un enregistrement de certificat est en cours :

- Vous pouvez attendre que l'autorité de gouvernance UXP approuve l'association entre le certificat et le serveur de sécurité. Une fois cette opération effectuée, le nouvel état sera « Enregistré ».
- Vous pouvez envoyer une demande pour annuler l'enregistrement du certificat depuis le serveur de sécurité au serveur de registre (voir [Annuler l'enregistrement d'un certificat d'authentification](#)). Vous pouvez forcer cette transition d'état même si l'annulation de l'enregistrement échoue. Le nouvel état sera « Suppression en cours ».

● **Enregistré** – l'autorité de gouvernance UXP a approuvé l'association entre le certificat et le serveur de sécurité. Les serveurs de sécurité ne peuvent utiliser que des certificats enregistrés pour effectuer l'authentification. Lorsqu'un certificat est enregistré :

- L'autorité de gouvernance UXP peut révoquer l'association entre le certificat et le serveur de sécurité sur le serveur de registre. Le nouvel état sera « Erreur globale ».
- Vous pouvez envoyer une demande pour annuler l'enregistrement du certificat depuis le serveur de sécurité au serveur de registre (voir [Annuler l'enregistrement d'un certificat d'authentification](#)). Vous pouvez forcer cette transition d'état même si l'annulation de l'enregistrement échoue. Le nouvel état sera « Suppression en cours ».

○ **Erreur globale** – l'autorité de gouvernance a révoqué l'association entre le certificat et le serveur de sécurité. Lorsqu'un certificat présente une erreur globale :

- L'autorité de gouvernance UXP peut restaurer l'association entre le certificat et le serveur de sécurité. L'état sera à nouveau « Enregistré ».
- Vous pouvez supprimer le certificat.

● **Suppression en cours** – une demande d'annulation de l'enregistrement du certificat a été envoyée par le serveur de sécurité au serveur d'enregistrement. Lorsqu'une suppression de certificat est en cours :

- Vous pouvez supprimer le certificat.

9. Certificat TLS interne du serveur de sécurité

Le serveur de sécurité utilise son certificat TLS interne pour établir une connexion sécurisée avec les systèmes d'information qui y sont connectés.

9.1. Ajouter une nouvelle clé et un nouveau certificat TLS interne au serveur de sécurité

Droits d'accès : Responsable des clés du propriétaire du serveur

Sur le serveur de sécurité, exportez le certificat TLS interne du serveur de sécurité.

Il existe deux options différentes pour ajouter une nouvelle paire de clés et de certificats TLS internes au serveur de sécurité.

Générer une nouvelle clé et un nouveau certificat

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre** du propriétaire du serveur.
2. Recherchez les **Certificats TLS internes**.
3. Cliquez sur **Générer une clé et un certificat**.
4. Choisissez le type de clé et cliquez sur **Générer**. Pour plus d'informations sur les différents types de clés, voir la section [Types de clés](#).

Dans cette option, le serveur de sécurité génère une nouvelle clé TLS et le certificat auto-signé correspondant.

Importer un magasin de clés existant

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre** du propriétaire du serveur.
2. Recherchez les **Certificats TLS internes**.
3. Cliquez sur **Importer un magasin de clés**.
4. Choisissez une base de données PKCS#12 sur votre ordinateur.
5. Si le magasin de clés contient plus d'une clé, entrez l'alias de la clé que vous souhaitez importer.
6. Si le magasin de clés est protégé par un mot de passe, saisissez celui-ci.
7. Cliquez sur **Importer**.

Dans cette option, vous avez généré la clé TLS et le certificat correspondant à l'aide d'une méthode externe. Pour les importer sur le serveur de sécurité, vous devez disposer de la clé et du certificat TLS sous la forme d'un magasin de clés PKCS#12. La clé TLS téléchargée et le certificat correspondant sont ajoutés à la liste des certificats TLS internes du serveur de

sécurité.

9.2. Activer un certificat TLS interne du serveur de sécurité

Droits d'accès : Responsable des clés du propriétaire du serveur

Pour garantir un processus fluide de changement du certificat TLS interne du serveur de sécurité, plusieurs certificats peuvent être ajoutés au serveur de sécurité, mais seul le certificat actif est utilisé lors de la communication avec d'autres systèmes d'information.



Avant d'activer un certificat, confirmez avec les administrateurs de tous les systèmes d'information se connectant au serveur de sécurité qu'ils ont commencé à utiliser le nouveau certificat. Les connexions entre le serveur de sécurité utilisant le nouveau certificat et les systèmes d'information utilisant l'ancien certificat échoueront.

Pour activer un certificat TLS interne de serveur de sécurité, recherchez le certificat TLS interne du serveur de sécurité inactif, cliquez sur **Utiliser ceci** et confirmez.

Après avoir activé un nouveau certificat, l'ancien certificat ne sera pas supprimé automatiquement. Vous pouvez réactiver l'ancien certificat ultérieurement si nécessaire.

9.3. Exporter un certificat TLS interne du serveur de sécurité

Droits d'accès : Administrateur serveur, Responsable des clés du propriétaire du serveur (les Responsables des services peuvent exporter les certificats TLS internes du serveur de sécurité sur la page **Systèmes d'information**)

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

1. Accédez à la page **Clés et certificats** ou à la page **Clés du membre** du propriétaire du serveur.
2. Recherchez les **Certificats TLS internes**.
3. Choisissez un certificat et cliquez sur **Exporter**.
4. Choisissez si vous souhaitez exporter le certificat au format PEM ou DER.
5. Cliquez sur **Exporter** et enregistrez le fichier demandé sur votre ordinateur.

9.4. Supprimer un certificat TLS interne du serveur de sécurité

Droits d'accès : Responsable des clés du propriétaire du serveur

Si un certificat TLS interne de serveur de sécurité inactif n'est plus nécessaire, vous pouvez le supprimer du serveur de sécurité.



Un serveur de sécurité a toujours besoin d'un certificat TLS interne actif, vous ne pouvez donc pas supprimer le certificat qui est actuellement actif. Si vous souhaitez supprimer un ancien certificat pendant le processus de changement de certificats, veuillez à d'abord

activer un autre certificat TLS interne du serveur de sécurité.

Pour supprimer un certificat TLS interne du serveur de sécurité, recherchez le certificat TLS interne inactif du serveur de sécurité, cliquez sur **Supprimer** et confirmez.

10. Dispositifs de création de signature

10.1. Connexion d'un dispositif de création de signature

Par défaut, les serveurs de sécurité stockent les clés cryptographiques sur des jetons de sécurité logiciels (jeton logiciel dans UXP).

Certaines autorités de gouvernance UXP exigent que les clés de signature soient stockées sur un périphérique externe afin d'ajouter un niveau de protection supplémentaire. Ce besoin découle souvent de lois qui exigent que les dispositifs de création de signature pour les signatures électroniques aient un certain degré de valeur juridique. Les modules de sécurité matériels (HSM), les jetons USB et les HSM en nuage sont des exemples de dispositifs de création de signature. Dans ce cas, les serveurs de sécurité prennent en charge les dispositifs externes de création de signature. Le dispositif de création de signature doit disposer d'une interface PKCS#11 pour être connecté au serveur de sécurité.

Si une clé existe déjà sur l'appareil avec un certificat, le Responsable des clés peut importer le certificat sur le serveur. S'il n'y a pas de clé sur le dispositif, le Responsable des clés peut générer une clé sur celui-ci, demander un certificat à l'autorité de certification et importer le certificat sur le serveur.



Seules les clés de signature peuvent être stockées sur les dispositifs de création de signature. Les clés d'authentification et les clés TLS du serveur de sécurité sont toujours stockées sur le jeton logiciel.

10.1.1. Dispositif de création de signature (PKCS#11)

Le serveur de sécurité a été testé et confirmé pour fonctionner avec le HSM nShield Connect d'Entrust. En outre, d'autres dispositifs de création de signature dotés d'une interface PKCS#11 standard pourraient fonctionner avec le serveur de sécurité, mais ils n'ont pas été testés.

Installer le module complémentaire UXP pour les dispositifs de création de signature (PKCS#11)

Installez le module complémentaire UXP pour activer la prise en charge des jetons provenant de dispositifs PKCS#11 sur le serveur de sécurité en exécutant les commandes suivantes :

```
sudo apt install uxp-addon-pkcs11
```

Connecter le dispositif et installer les pilotes

Droits d'accès : privilèges de l'utilisateur root



Si vous avez déjà installé les pilotes pour ce modèle de périphérique, vous pouvez

continuer à [ajouter le périphérique](#).

Déterminez les informations suivantes avant de connecter un dispositif de création de signature.

Dispositif de création de signature

- que l'appareil dispose d'une interface PKCS#11 ;
- les instructions du fabricant sur la manière de connecter le dispositif au serveur Ubuntu exécutant le serveur de sécurité ;
- que le dispositif dispose d'au moins un jeton prêt à être utilisé ;
- le(s) code(s) PIN pour le(s) jeton(s).

Pour connecter un dispositif de création de signature au serveur de sécurité, procédez comme suit :

1. Connectez le dispositif au serveur Ubuntu qui exécute le serveur de sécurité conformément aux instructions du fabricant.
2. Installez le logiciel du fabricant du dispositif sur le serveur de sécurité.
3. Déterminez l'emplacement de la bibliothèque PKCS#11 de votre dispositif sur le serveur de sécurité. N'oubliez pas l'emplacement et le nom du fichier de la bibliothèque, vous en aurez besoin plus tard.



Pour nShield Connect HSM, la bibliothèque se trouve probablement dans le dossier `/opt/nfast/toolkits/pkcs11/`.

4. Assurez-vous que le fichier de bibliothèque PKCS#11 installé dispose des autorisations de lecture pour l'utilisateur `uxp`. Pour accorder des autorisations de lecture au fichier, exécutez la commande suivante (remplacez `<library>` par le chemin d'accès à la bibliothèque PKCS#11) :

```
chmod o+r <library>
```

5. Vérifiez si la connexion avec l'appareil est établie :

```
sudo su uxp -c 'pkcs11-tool --module <library> -L'
```

La connexion est établie si la sortie est une liste des emplacements disponibles avec les informations relatives à ces emplacements.

Ajouter un dispositif

Droits d'accès : Administrateur serveur

1. Ouvrez l'interface utilisateur du serveur de sécurité.
2. Si le module complémentaire a été installé avec succès, vous pouvez voir une page pour

les **dispositifs de création de signature** dans le menu latéral. Allez sur cette page.

3. Cliquez sur **Ajouter un dispositif** et, si l'on vous demande le type de dispositif, choisissez **Dispositif de création de signature (PKCS#11)**.

Donnez un nom le dispositif et indiquez l'emplacement de la bibliothèque PKCS#11 du fabricant sur le serveur de sécurité.

Vous pouvez modifier des paramètres spécifiques du dispositif dans la section des paramètres avancés.



La méthode par défaut utilisée par le serveur de sécurité pour mapper les emplacements physiques d'un dispositif sur les jetons du serveur est l'utilisation de l'identifiant de l'emplacement. Cela suppose que les identifiants des emplacements sont stables sur le dispositif. Lorsque les identifiants des emplacements sont susceptibles de changer, utilisez le numéro de série de l'emplacement comme source d'identité du jeton.

4. Cliquez sur **Ajouter**. Le serveur de sécurité tente de se connecter au dispositif. Lorsque la connexion est établie, le serveur de sécurité détecte un ou plusieurs jetons sur le dispositif.



Si le serveur de sécurité ne trouve aucun jeton, la connexion a échoué ou il y a un problème avec le dispositif. Vérifiez le chemin d'accès à la bibliothèque et consultez la documentation du fabricant du dispositif.

En outre, vous pouvez essayer de redémarrer les services UXP (Attention : le redémarrage du service `uxp-proxy` interrompt l'échange de messages pendant une courte période) :

```
sudo systemctl restart uxp-securityserver-rest-api uxp-proxy
```

Après le redémarrage ou d'autres modifications, vérifiez si l'état du dispositif est passé de « erreur » à « opérationnel ». Une fois que l'état est devenu « opérationnel », accédez à la page **Clés et certificats**, cliquez sur **Ajouter un jeton** et choisissez **Jeton matériel**.

5. Choisissez un jeton pour stocker les clés de signature. Attribuez le jeton à un membre UXP, le jeton sera alors accessible au Responsable des clés du membre. Si vous ne savez pas quel jeton choisir, vous pouvez revenir plus tard pour ajouter le jeton.

10.2. Ajouter un jeton matériel

Droits d'accès : Administrateur serveur

Contrairement au jeton logiciel intégré au serveur de sécurité, les jetons sur les dispositifs de création de signature sont appelés jetons matériels dans UXP.

Pour utiliser un dispositif de création de signature afin de stocker les clés de signature, vous devez d'abord ajouter un jeton provenant du dispositif au serveur de sécurité.

Pour ajouter un jeton matériel d'un dispositif au serveur de sécurité, procédez comme suit.

1. Accédez à la page **Clés et certificats**.
2. Cliquez sur **Ajouter un jeton**.
3. Choisissez **Jeton matériel**.
4. Choisissez le jeton du dispositif que vous souhaitez ajouter au serveur de sécurité.
Si le dispositif ne s'affiche pas, vous devez d'abord l'ajouter. Voir la section [Connexion d'un dispositif de création de signature](#).
5. Cliquez sur **Ajouter**.
6. Choisissez le propriétaire du jeton parmi les membres du serveur de sécurité.



L'attribution d'un propriétaire au jeton garantit que seuls les Responsables des clés de ce membre peuvent accéder au jeton sur un serveur mutualisé.

Le nouveau jeton apparaîtra dans la liste des jetons ajoutés au serveur de sécurité. Après l'ajout du jeton, le jeton est déconnecté. Le Responsable des clés du propriétaire du jeton doit **Se connecter** au jeton. Si le jeton ne dispose d'aucune option de connexion ou de déconnexion, cela signifie qu'il présente un problème qui doit être résolu avant que le Responsable des clés ne puisse l'utiliser. Pour plus d'informations sur les statuts des jetons, voir la section [États des jetons matériels](#).

Après avoir ajouté un jeton, celui-ci ne dispose d'aucune clé utilisable par le serveur de sécurité. Le Responsable des clés a deux options pour obtenir la clé sur le jeton :

- si le jeton ne dispose pas encore de clé, le Responsable des clés peut [générer une clé et une CSR](#) sur le jeton, demander le certificat à un fournisseur de services de certification, puis [importer le certificat](#) sur le serveur de sécurité ou
- si le jeton contient déjà une clé de signature et un certificat, le Responsable des clés doit [importer le certificat du jeton](#) vers le serveur de sécurité.

10.3. États des jetons matériels

Le serveur de sécurité distingue les états suivants pour les jetons matériels :

- Indisponible — le serveur de sécurité a perdu la connexion avec le jeton, le serveur de sécurité ne peut pas utiliser les clés du jeton.
Raisons possibles pour lesquelles un jeton peut être indisponible :
 - le dispositif est désactivé sur le serveur de sécurité ;
 - le dispositif est physiquement déconnecté ;
 - l'emplacement de la bibliothèque PKCS#11 a changé ;
 - le jeton a été retiré du dispositif ;
 - l'identifiant de l'emplacement du jeton a changé sur le dispositif.



Lorsqu'un jeton est ajouté au serveur de sécurité, celui-ci mémorise l'identifiant de l'emplacement du jeton afin d'identifier le jeton sur le dispositif. Si, pour une raison

quelconque, l'identifiant de l'emplacement du jeton change sur le dispositif (ou si le jeton a été retiré), le serveur de sécurité ne peut plus trouver le jeton et les clés qu'il contient. Pour vérifier si le dispositif dispose toujours d'un jeton avec l'identifiant de l'emplacement du jeton indisponible, comparez les identifiants des emplacements des jetons sur le dispositif (voir les détails du dispositif) et l'identifiant du jeton indisponible (voir les détails du jeton). Le format de l'identifiant du jeton de périphérique PKCS#11 est `pkcs11-<deviceID>-<slotID>`.

Pour les dispositifs dont les identifiants d'emplacement ne sont pas stables, choisissez le numéro de série comme identifiant du jeton lors de l'ajout du dispositif.

- **Déconnecté** — le jeton est protégé par un code PIN et celui-ci n'a pas été saisi, le serveur de sécurité ne peut pas utiliser les clés du jeton. Le Responsable des clés doit saisir le code PIN du jeton pour que le serveur de sécurité puisse utiliser les clés.
- **Connecté** — le code PIN du jeton a été saisi, le serveur de sécurité peut utiliser les clés du jeton pour la signature.
- **Non initialisé** — le jeton n'est pas prêt à être utilisé. Utilisez les outils fournis par le fabricant du dispositif ou l'outil `pkcs11` pour vous connecter au dispositif et initialiser le jeton.
- **Verrouillé** — le jeton est verrouillé, trop de tentatives de saisie du code PIN, le serveur de sécurité ne peut pas utiliser les clés du jeton. Utilisez les outils fournis par le fabricant du dispositif pour vous connecter au dispositif et déverrouiller le jeton.

10.4. Supprimer un jeton matériel

Droits d'accès : Administrateur serveur

Vous pouvez supprimer un jeton matériel du serveur de sécurité lorsqu'il n'est plus utilisé. Le jeton physique reste sur le dispositif. Les clés et les certificats qui se trouvent sur le dispositif physique restent sur celui-ci.

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

10.5. Supprimer un dispositif de création de signature

Droits d'accès : Administrateur serveur

Pour éviter de supprimer des clés par accident, le serveur de sécurité n'autorise que la suppression des dispositifs pour lesquels aucun jeton n'a été enregistré sur le serveur de sécurité.

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

10.6. Désactiver et activer un dispositif de création de signature

Droits d'accès : Administrateur serveur

Pour cesser temporairement d'utiliser un dispositif de création de signature sans le supprimer lui ou ses jetons du serveur de sécurité, vous pouvez désactiver le dispositif.

Lorsqu'un dispositif de création de signature est désactivé, le serveur de sécurité n'essaie pas de se connecter au dispositif et de détecter les jetons jusqu'à ce que le dispositif soit à nouveau activé.

Pour désactiver un dispositif, recherchez-le et cliquez sur **Désactiver**.

Pour activer un dispositif, recherchez-le et cliquez sur **Activer**.

10.7. Modification des paramètres d'un dispositif de création de signature

Droits d'accès : Administrateur serveur

Lors de l'ajout d'un dispositif, le serveur de sécurité propose de modifier un ensemble de paramètres avancés. Certains dispositifs peuvent nécessiter une modification de ces paramètres pour fonctionner correctement avec le serveur de sécurité. Consultez la documentation du fabricant du dispositif.

Pour modifier les paramètres d'un dispositif de création de signature déjà ajouté au serveur de sécurité, recherchez le dispositif, cliquez sur **Modifier** et **Afficher les paramètres avancés**.

L'effet de chaque paramètre avancé est expliqué à côté de celui-ci.

Si vous souhaitez réinitialiser un paramètre, les valeurs par défaut des paramètres des dispositifs PKCS#11 sont les suivantes :

- source d'identité du jeton : SLOT_ID
- threads natifs autorisés : coché
- Verrouillage des threads natifs autorisé : coché
- mécanisme de signature RSA : CKM_RSA_PKCS
- nombre maximal de sessions de signature : 20
- délai d'inactivité de la session de signature : 30
- délai d'expiration de l'opération du jeton : 10

Les autres paramètres avancés n'ont pas de valeur par défaut.

Une fois que vous avez enregistré les nouvelles valeurs des paramètres, il faudra quelques minutes pour qu'elles prennent effet.

11. 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.

11.1. 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.

11.1.1. 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.

11.1.2. 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.

11.1.3. 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**.

11.1.4. 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](#)).

11.1.5. 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.

11.1.6. 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.

11.1.7. 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

11.2. Gestion des API REST

11.2.1. 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.

11.2.2. 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.

11.2.3. 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.

11.2.4. 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**.

11.2.5. 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](#)).

11.2.6. 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.

11.2.7. 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

11.2.8. 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.

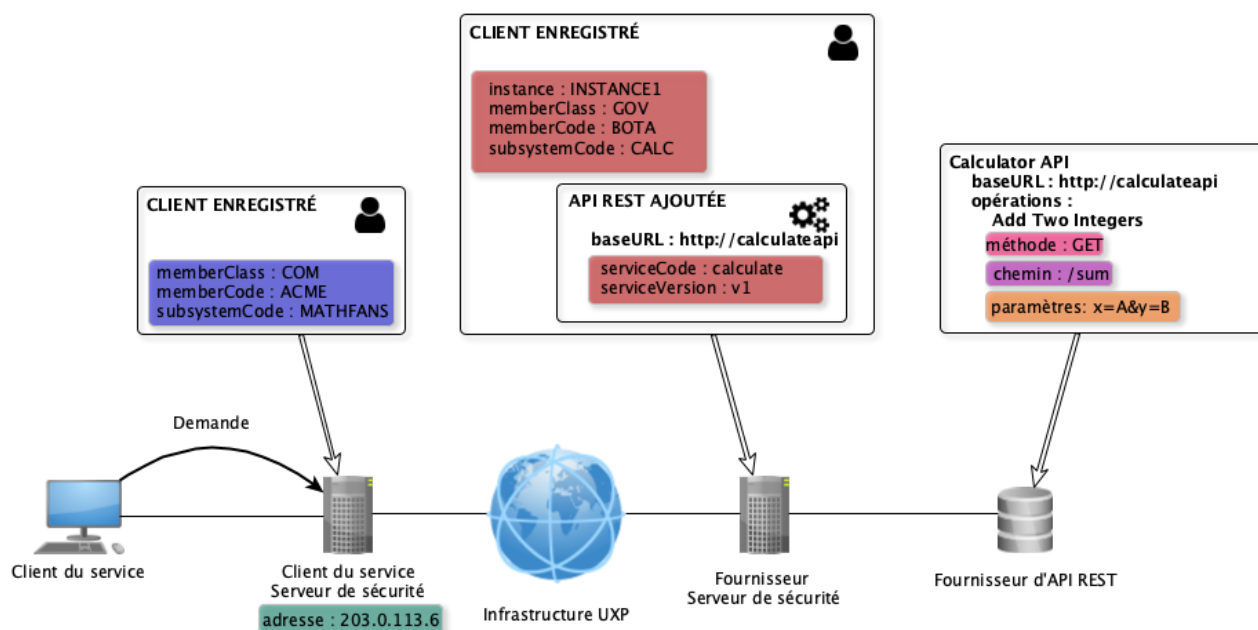
Pour supprimer une API REST, recherchez l'API REST, cliquez sur **Supprimer** et confirmez.

11.3. 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.

11.3.1. 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. (L'enregistrement et la gestion des clients du serveur de sécurité sont traités à la section [Clients du 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.

11.3.2. 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.

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

Uxp-Client: <code>EXAMPLE/COM/ACME/MATHFANS</code>			
Uxp-Service: <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.

11.3.3. 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 :

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

Uxp-Client: <code>EXAMPLE/COM/ACME/MATHFANS</code>			
Uxp-Service: <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.

11.4. 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.

12. 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](#)).

12.1. 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.

12.2. 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)

13. 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.

13.1. 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.

13.2. 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**.

13.3. 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**.

13.4. 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.

14. 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.

14.1. 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_-]

14.2. 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**.

14.3. 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.

15. Communication avec les systèmes d'information des clients

15.1. 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.

15.2. 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.

15.3. 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.

16. Paramètres du système

16.1. Ancre de configuration

Droits d'accès : Administrateur serveur

L'ancre de configuration contient des données que le serveur de sécurité utilise pour télécharger périodiquement la configuration signée à partir du serveur de registre et pour vérifier la signature de la configuration téléchargée.

La première ancre de configuration est téléchargée lors de l'initialisation du serveur. Si vous devez remplacer l'ancre, suivez les étapes suivantes.

1. Accédez à la page **Paramètres du système**.
2. Dans la section **Ancre de configuration**, cliquez sur **Télécharger**.
3. Recherchez le fichier d'ancre sur votre ordinateur et cliquez sur **Télécharger**.
4. Assurez-vous que le fichier d'ancrage que vous téléchargez est valide en comparant la valeur de hachage du fichier téléchargé avec la valeur de hachage de l'ancre valide publiée par l'autorité de gouvernance UXP. Si les valeurs de hachage correspondent, confirmez le téléchargement.

Pour **télécharger** l'ancre de configuration, allez à la page **Paramètres du système**, trouvez la section **Ancre de configuration** et cliquez sur **Télécharger**.

16.2. Services d'horodatage

Droits d'accès : Administrateur serveur

Le serveur de sécurité utilise l'horodatage pour préserver la valeur probante des messages échangés par UXP. L'horodatage est fourni par un service externe et chaque serveur de sécurité doit avoir au moins un fournisseur de services d'horodatage.

Le premier service d'horodatage est ajouté lors de l'initialisation du serveur. Si vous devez en ajouter un nouveau ou bien en rajouter un autre, procédez comme suit.

1. Accédez à la page **Paramètres du système**.
2. Dans la section **Services d'horodatage**, cliquez sur **Ajouter**.
3. Dans la fenêtre qui s'ouvre, sélectionnez un service et cliquez sur **Ajouter**.

Pour **ne plus utiliser un service d'horodatage**, choisissez un service, cliquez sur **Supprimer** et confirmez.

16.3. Port d'écoute (transport) du serveur de sécurité

Droits d'accès : Administrateur serveur

Le port d'écoute (transport) du serveur est le port sur lequel le serveur de sécurité écoute les demandes des autres serveurs de sécurité.

La valeur par défaut du port d'écoute du serveur est 5500.



Reportez-vous à la section [Fichiers de configuration](#) pour obtenir des instructions et remplacer les valeurs par défaut du paramètre `server-listen-port` dans la section `[proxy]` respectivement.

Vous pouvez consulter le port d'écoute du serveur de sécurité défini dans le fichier de configuration sur la page **Paramètres du système**.

Les autres serveurs de sécurité obtiennent des informations sur le port d'écoute d'un serveur de sécurité à partir de la configuration globale.



Si le port dans la configuration globale ne correspond pas au port du fichier de configuration, le serveur de sécurité dans le rôle de fournisseur de services ne peut pas se connecter aux autres serveurs de sécurité. Dans ce cas, le serveur de sécurité affichera un avertissement.

Pour résoudre ce problème, il existe deux solutions :

Option 1 : Modifier le fichier de configuration

Si le port d'écoute du serveur de sécurité (`server-listen-port`) est incorrect sur celui-ci, modifiez-le dans le fichier de configuration `/etc/uxp/conf.d/local.ini`.



Le système ne valide pas les valeurs des paramètres, soyez donc vigilant lorsque vous changez la configuration. Par exemple, si vous définissez le numéro de port sur une valeur non numérique dans la configuration, le système plantera.



La modification de la valeur du port d'écoute du serveur dans le fichier de configuration nécessite le redémarrage des services `uxp-proxy` et `uxp-securityserver-rest-api` :

```
sudo systemctl restart uxp-proxy uxp-securityserver-rest-api
```

Après le redémarrage de `uxp-proxy`, le nouveau port d'écoute du serveur de sécurité sera utilisé pour l'échange de messages. Après le redémarrage de `uxp-securityserver-rest-api`, le message d'avertissement est supprimé de l'interface utilisateur du serveur de sécurité.

Option 2 : Demande de modification au serveur de registre

Si le port d'écoute du serveur de sécurité est incorrect dans la configuration globale,

contactez l'administrateur du serveur de registre et demandez-lui de le modifier.

16.4. Fichiers de configuration

Droits d'accès : privilèges de l'utilisateur root

D'autres paramètres de configuration sont définis dans les [fichiers INI\[INI\]](#), où chaque section contient les paramètres d'un composant particulier du serveur de sécurité. La configuration par défaut du serveur de sécurité se trouve dans le fichier

```
/etc/uxp/conf.d/proxy.ini
```

Pour modifier la configuration par défaut, créez ou modifiez le fichier

```
/etc/uxp/conf.d/local.ini
```

Les paramètres pour le passage des messages sont situés dans la section `[proxy]` du fichier (si elle n'est pas présente, vous devez la créer). Sous le début de la section, listez les valeurs des paramètres, une par ligne.

Par exemple, pour configurer les paramètres

`client-http-port` et `client-httpclient-connect-timeout`,

ajouter les lignes suivantes au fichier de configuration :

```
[proxy]
client-http-port=80
client-httpclient-connect-timeout=300000
```



La modification des valeurs des paramètres du proxy dans les fichiers de configuration nécessite le redémarrage du service `uxp-proxy` :

```
sudo systemctl restart uxp-proxy
```



Le système ne valide pas les valeurs des paramètres, soyez donc vigilant lorsque vous changez la configuration. Par exemple, si vous définissez le numéro de port sur une valeur non numérique dans la configuration, le système plantera.

Voici quelques paramètres utiles pour la configuration du proxy :

- `client-httpclient-connect-timeout` — définit la période (en millisecondes) pendant laquelle le serveur de sécurité du client du service tente de se connecter au serveur de sécurité du fournisseur de services. Lorsque le délai est atteint, le serveur de sécurité du client du service informe le système d'information du client du service qu'un délai de service s'est écoulé. La valeur 0 signifie qu'un temps d'attente infini est autorisé. La valeur par défaut est 30 000.

- `client-httpclient-read-timeout` - le temps maximum (SO_TIMEOUT, en millisecondes) pendant lequel les connexions entre le serveur de sécurité d'un client et le serveur de sécurité d'un fournisseur de services sont autorisées à attendre une réponse avant que le serveur de sécurité du client n'abandonne. La valeur 0 signifie qu'un temps d'attente infini est autorisé. La valeur par défaut est 300 000.
- `client-http-port` — Port TCP sur lequel le serveur de sécurité du client du service écoute les demandes HTTP des applications clientes. La valeur par défaut est 80.
- `client-https-port` — Port TCP sur lequel le serveur de sécurité du client du service écoute les demandes HTTPS des applications clientes. La valeur par défaut est 443.
- `connector-host` — Adresse IP sur laquelle le serveur de sécurité du client du service écoute les connexions des applications clientes. La valeur 0.0.0.0 autorise l'écoute sur toutes les interfaces IPv4 et est la valeur par défaut.
- `server-listen-address` — Adresse IP sur laquelle le serveur de sécurité du fournisseur de services écoute les connexions des serveurs de sécurité du client du service. La valeur 0.0.0.0 autorise l'écoute sur toutes les interfaces IPv4 et est la valeur par défaut.
- `server-listen-port` — port sur lequel le serveur de sécurité du fournisseur de services écoute les connexions des serveurs de sécurité du client du service. La valeur par défaut 5500

16.5. Certificat TLS Nginx

Droits d'accès : privilèges de l'utilisateur root

Le certificat TLS Nginx est nécessaire pour afficher l'interface utilisateur du serveur de sécurité. Le serveur de sécurité utilise le certificat TLS Nginx pour établir une connexion sécurisée avec le navigateur Web de l'utilisateur. Lors de l'installation du serveur, un certificat TLS Nginx est généré pour le serveur de sécurité et sa période de validité est de 100 ans.

Voici quelques-unes des situations qui nécessitent le remplacement d'un certificat :

- changement d'hôte ou d'adresse IP du serveur de sécurité ;
- la clé du certificat est compromise ;
- le certificat nécessite un nouvel algorithme cryptographique différent.

Pour remplacer le certificat TLS Nginx ultérieurement, utilisez le script `generate_certificate.sh`.

Utilisation du script :

```
Usage: /usr/share/uxp/scripts/generate_certificate.sh -n <basename>
<-s "<certificate DN>" | -S> [-a "<subjectAltName>" | -f]
[-d <path>] [-p] [-c <path>] [-2 | -3 | -4 | -e <EC> | -w <ED>]

Generate TLS certificate (by default NIST P-256).

OPTIONS:
  -h      show this message
  -n      basename, like 'internal' or 'nginx'
  -d      working/output directory, defaults to /etc/uxp/ssl
  -m      multiple certs generation support (cert is generated to the '<basename>-<epoch-
millis>' subdirectory)
  -f      fill subjectAltName automatically from hostname and IP addresses
  -S      fill Subject with /CN=${HOST} value
  -s      subject, optional. Format "/C=EE/O=Company/CN=server.name.tld"
  -x      extension basename, like 'internal' or 'nginx', defaults to basename value
  -a      subjectAltName, optional. Format
"DNS:serverAlt.name.tld,IP:1.1.1.1,IP:2.2.2.2"
  -p      generate .p12 also, friendly name and password will default to basename value
  -c      configuration directory containing openssl.cnf, defaults to /etc/uxp/ssl
  -2      generate 2k RSA key
  -3      generate 3k RSA key
  -4      generate 4k RSA key
  -e      generate EC key. Possible values: 'p256' (NIST P-256 aka secp256r1),
'p384' (NIST P-384 aka secp384r1), 'p521' (NIST P-521 aka secp521r1)
  -w      generate Edwards-curve Digital Signature Algorithm (EdDSA) key.
Possible values: '25519' (Ed25519), '448' (Ed448).
May not be accepted by browsers for HTTPS, support is not yet widespread.
```

Utilisez l'option `-n nginx` pour indiquer que vous générez le certificat TLS Nginx.

L'option `-m` ne doit pas être utilisée pour un certificat TLS Nginx.

L'une des options `-s` ou `-S` est obligatoire. L'option `-S` remplit le champ Objet avec le nom de l'hôte. Utilisez `-s` si vous souhaitez remplir vous-même le champ Objet (voir la description des options pour connaître le format correct).

`-a` prend en charge un nombre illimité de noms DNS et/ou d'adresses IP (voir la description des options pour connaître le format correct).

Le répertoire de travail/sortie par défaut (`/etc/uxp/ssl`) convient pour générer le certificat TLS Nginx.

Exemple d'exécution du script :

```
sudo /usr/share/uxp/scripts/generate_certificate.sh -n nginx \
-s <subject> -a <subjectAltName>
```

Une fois le nouveau certificat TLS Nginx généré, le service `nginx` doit être rechargé :

```
sudo systemctl reload nginx
```

17. Journal des messages

Droits d'accès : privilèges de l'utilisateur root

Le journal des messages permet de prouver qu'un serveur de sécurité a reçu une demande UXP ou envoyé un message de réponse. Les messages échangés entre les serveurs de sécurité sont signés et cryptés. Pour chaque message de demande ou de réponse régulier, le serveur de sécurité produit un document complet signé et horodaté, appelé conteneur de signature associé (Associated Signature Container, ASiC) [\[ASiC\]](#).

Le flux de travail du journal des messages peut être résumé comme suit :

1. Le serveur de sécurité enregistre de manière synchrone les messages UXP, leurs métadonnées et leurs signatures dans le journal des messages pendant l'échange de messages.
2. Périodiquement, toutes les nouvelles signatures de messages dans le journal des messages sont horodatées avec un horodatage par lots.



Si l'horodatage a échoué pendant une période définie (4 heures par défaut), le journal des messages cesse d'accepter des messages. Cela provoque l'arrêt du serveur de sécurité, qui n'accepte plus aucune demande.

L'objectif de cette fonctionnalité est d'éviter l'échange de messages qui ne peuvent pas être correctement horodatés. Pour désactiver cette fonction ou modifier la période acceptable pour l'échec de l'horodatage, voir la section [Paramètres d'horodatage](#).

3. Le serveur de sécurité collecte périodiquement les messages signés et horodatés du journal des messages et archive chaque message dans un conteneur ASiC.
 - Le journal des messages peut archiver les messages soit sur le système de fichiers local, soit dans un compartiment S3 (les compartiments [AWS S3 \[S3\]](#) et les compartiments non similaires à Amazon S3 sont pris en charge). Pour plus de détails, voir la section [Changer la configuration du journal des messages](#).
4. Après l'archivage, le serveur de sécurité supprime les données de signature des messages archivés du stockage du journal des messages. Le serveur de sécurité supprime également les données d'horodatage si tous les messages comportant cet horodatage ont été archivés.
 - Les métadonnées restent dans le journal des messages pour toujours ou jusqu'à ce que la durée de vie maximale configurée soit atteinte (voir la section [Configurer la durée de vie du journal des messages](#)). Les métadonnées de chaque message contiennent un identifiant unique du fichier d'archive de ce message. Cela signifie que vous pouvez utiliser les métadonnées pour trouver le fichier d'archive correspondant à chaque message.
5. Sur la page Messages du serveur de sécurité, les utilisateurs ayant le rôle d'Auditeur de transactions peuvent :
 - vérifier les détails et la validité de la signature et de l'horodatage des messages ;

- télécharger l'ASiC pour voir le contenu intégral du message.
Notez que pour les messages REST, la charge utile du message est sauvegardée dans un fichier nommé `attachment1`. Ceci afin de garantir la vérifiabilité dans le contexte du protocole de message UXP (pour plus d'informations, voir le Document protocole de message v4.0. [\[UXP-PR-MESS\]](#)).

17.1. Changer la configuration du journal des messages

Les paramètres de configuration sont définis dans les [fichiers INI\[INI\]](#), où chaque section contient les paramètres d'un composant particulier du serveur de sécurité.

Pour modifier la configuration par défaut, créez ou modifiez le fichier `/etc/uxp/conf.d/local.ini`. Créez la section `[message-log]` (si elle n'existe pas) dans le fichier. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.

Par exemple, pour configurer les paramètres `archive-path` et `archiver-batch-size`, les lignes suivantes doivent être ajoutées à `local.ini` :

```
[message-log]
archive-path=/my/archive/path/
archiver-batch-size=200
```



Après avoir changé la configuration, vous devez redémarrer un ou plusieurs des services `uxp-proxy`, `uxp-messagelog-archiver` et `uxp-messagelog-timestamper`, comme indiqué dans les sous-sections suivantes.



Le système ne valide pas les valeurs des paramètres, soyez donc vigilant lorsque vous changez la configuration. Par exemple, définir une valeur d'identifiant d'algorithme de hachage non valide dans la configuration provoquera le plantage du système.

17.1.1. Paramètres communs



Après avoir changé le paramètre suivant, vous devez redémarrer le service `uxp-proxy` :

```
sudo systemctl restart uxp-proxy
```

1. `hash-algo-id` — algorithme de hachage utilisé pour le hachage dans le journal des messages. Les choix possibles sont SHA-256, SHA-384, SHA-512. La valeur par défaut est SHA-512.



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-proxy` et le service `uxp-messagelog-archiver` :

```
sudo systemctl restart uxp-proxy uxp-messagelog-archiver
```

1. `storage-path`—chemin absolu vers le répertoire où est stocké le journal des messages. La valeur par défaut est `/var/lib/uxp/messagelog`.
2. `temp-files-path`—chemin absolu vers le répertoire où sont stockés les fichiers temporaires. La valeur par défaut est `/var/lib/uxp/messagelog/tmp`.

17.1.2. Paramètres d'horodatage

Paramètres de la stratégie d'horodatage

Pour changer ces paramètres, créez la section `[message-log]` (si elle n'existe pas) dans le fichier `local.ini`. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-proxy` et le service `uxp-messagelog-timestamper` :

```
sudo systemctl restart uxp-proxy uxp-messagelog-timestamper
```

1. `timestamping-mode`—mode d'horodatage appliqué aux signatures. La valeur par défaut est `SCHEDULED_BATCH`.

Valeurs possibles :

- `NONE` – les signatures ne sont pas horodatées.
 - `SCHEDULED_BATCH` – utilise le démon `uxp-messagelog-timestamper` pour créer de manière asynchrone des horodatages par lots dans des groupes définis par `timestamper-batch-size`.
 - `SCHEDULED` – utilise le démon `uxp-messagelog-timestamper` pour créer de manière asynchrone un horodatage distinct pour chaque signature.
 - `IMMEDIATE` – utilise le processus `uxp-proxy` pour horodater chaque signature de manière synchrone pendant l'échange de messages.
2. `timestamp-provider-round-robin`—si le fournisseur principal d'horodatage pour l'horodatage des signatures est sélectionné à l'aide d'une stratégie de rotation. Si `false`, le fournisseur principal d'horodatage est le même pour toutes les demandes (dans l'ordre d'addition) et les fournisseurs suivants ne sont utilisés que si le fournisseur principal échoue. La valeur par défaut est `false`.

Paramètres d'horodatage par lots

Pour changer ces paramètres, créez la section `[message-log]` (si elle n'existe pas) dans le fichier `local.ini`. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-messagelog-timestamper` :

```
sudo systemctl restart uxp-messagelog-timestamper
```

1. `timestamper-batch-size`—nombre maximum d'enregistrements de signature de message à horodater dans un lot. La valeur par défaut est 100. Ce paramètre n'a de sens que si `timestamping-mode` est `SCHEDULED_BATCH`.
2. `timestamper-client-connect-timeout`—délai d'expiration de la connexion du client de l'horodateur par lots en millisecondes. La valeur 0 permet de désactiver ce délai. La valeur par défaut est 10 000 millisecondes (10 secondes). Ce paramètre n'a de sens que lorsque `timestamping-mode` est soit `SCHEDULED`, soit `SCHEDULED_BATCH`.
3. `timestamper-client-read-timeout`—délai d'expiration de lecture du client de l'horodateur par lots en millisecondes. La valeur 0 permet de désactiver ce délai. La valeur par défaut est de 5 000 millisecondes (5 secondes). Ce paramètre n'a de sens que lorsque `timestamping-mode` est soit `SCHEDULED`, soit `SCHEDULED_BATCH`.

Pour changer ces paramètres, créez la section `[message-log]` (si elle n'existe pas) dans le fichier `local.ini`. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-proxy` :

```
sudo systemctl restart uxp-proxy
```

1. `acceptable-timestamp-failure-period`—période de temps en secondes, pendant laquelle l'horodatage des lots peut échouer avant que l'échange de messages entre les serveurs de sécurité ne soit interrompu. La valeur 0 permet de désactiver cette vérification. La valeur par défaut est de 14 400 secondes (4 heures). Ce paramètre n'a de sens que lorsque `timestamping-mode` est soit `SCHEDULED`, soit `SCHEDULED_BATCH`.

Paramètres d'horodatage immédiat

Pour changer ces paramètres, créez la section `[proxy]` (si elle n'existe pas) dans le fichier `local.ini`. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-proxy` :

```
sudo systemctl restart uxp-proxy
```

1. `timestamper-httpclient-connect-timeout`—délai d'attente de la connexion du client de l'horodateur immédiat en millisecondes. La valeur 0 permet de désactiver ce délai. La

valeur par défaut est 10 000 millisecondes (10 secondes). Ce paramètre n'a de sens que si `timestamping-mode` est `IMMEDIATE`.

2. `timestamp-httpclient-read-timeout`—délai d'attente de lecture du client d'horodatage immédiat en millisecondes. La valeur 0 permet de désactiver ce délai. La valeur par défaut est de 5 000 millisecondes (5 secondes). Ce paramètre n'a de sens que si `timestamping-mode` est `IMMEDIATE`.

17.1.3. Paramètres d'archivage



Après avoir changé les paramètres suivants, vous devez redémarrer le service `uxp-messagelog-archiver` :

```
sudo systemctl restart uxp-messagelog-archiver
```

1. `archive-storage-type`—type d'implémentation de stockage d'archives à utiliser. Les options sont `AWS S3` (`s3`) ou le système de fichiers (`fs`). La valeur par défaut est `fs`.
2. `archive-path`—chemin absolu vers le répertoire où les enregistrements de journal horodatés sont archivés lors de l'utilisation du stockage d'archives du système de fichiers (`fs`). La valeur par défaut est `/var/lib/uxp/messagelog/archive`.
3. `archive-interval`—intervalle de temps comme [expression Cron \[CRON\]](#) pour l'archivage des enregistrements horodatés. La valeur par défaut est `0 0 0/6 1/1 * ? *` (exécution toutes les 6 heures).
4. `archiver-batch-size`—nombre maximum d'enregistrements de signatures de messages à archiver dans un lot. La valeur par défaut est 100.
5. `archive-transfer-command`—commande exécutée après le processus d'archivage (périodique). Cela permet de configurer un script externe pour transférer automatiquement les fichiers d'archives à partir du serveur de sécurité. La commande est appelée avec le chemin absolu de l'archive générée comme premier argument. Par défaut, aucune opération n'est effectuée.
6. `archiver-admin-port`—Port TCP (HTTP) sur lequel l'Archiveur de messages écoute les commandes administratives. Une demande `/execute` peut être envoyée pour déclencher immédiatement le processus d'archivage, et une demande `/clean-metadata` peut être envoyée pour déclencher la suppression immédiate des métadonnées expirées. La valeur par défaut est 5 765.
7. `metadata-cleaner-batch-size`—nombre maximum d'anciens enregistrements de métadonnées à nettoyer en un seul lot. La valeur par défaut est 1 000.
8. `metadata-cleanup-interval`—intervalle de temps comme [expression Cron \[CRON\]](#) pour nettoyer les anciens enregistrements de métadonnées. La valeur par défaut est `0 0 0 * * ? *` (s'exécute tous les jours à minuit).
9. `metadata-record-cleanup-operation`—opération de nettoyage des anciens enregistrements de métadonnées. Les valeurs possibles sont `KEEP`, `DELETE`, et `EXTRACT`. `KEEP` signifie que les anciens enregistrements restent dans le stockage des métadonnées et ne sont pas supprimés.

DELETE supprime simplement les anciens enregistrements du stockage des métadonnées.
EXTRACT enregistre les enregistrements supprimés dans un fichier .csv dans 'metadata-record-extract-path'.

10. metadata-record-extract-path — le répertoire où sont enregistrés les fichiers .csv contenant les anciennes métadonnées extraites si l'opération de nettoyage est EXTRACT. La valeur par défaut est /var/lib/uxp/message-log/old-metadata.
11. metadata-record-lifetime-minutes — durée de vie maximale d'un enregistrement de métadonnées dans le stockage des métadonnées, en minutes. La valeur par défaut est 1 576 800 minutes (3 ans).

Les paramètres suivants sont utilisés pour archiver le journal des messages sur S3. Pour changer ces paramètres, créez la section [message-log-s3] (si elle n'existe pas) dans le fichier local.ini. Dans cette section, indiquez les nouvelles valeurs des paramètres, un paramètre par ligne.

1. bucket-name — nom du compartiment S3 où les enregistrements de journal horodatés sont archivés lors de l'utilisation du stockage d'archives « s3 ».
2. access-key — clé d'accès à utiliser pour l'authentification avec S3 lors de l'utilisation du stockage d'archives « s3 ».
3. secret-key — clé secrète à utiliser pour l'authentification avec S3 lors de l'utilisation du stockage d'archives « s3 ».
4. address — adresse du service S3, doit être fournie pour le stockage d'archives « s3 » lorsqu'un compartiment de type S3 non AWS est utilisé.
5. region — région AWS préférée lors de l'utilisation du stockage d'archives AWS « s3 ». La valeur par défaut est us-west-1.
6. storage-class — classe de stockage AWS S3 facultative pour les données d'archives téléchargées. Dépend de la politique AWS S3 par défaut. Valeurs possibles : STANDARD, REDUCED_REDUNDANCY, GLACIER, STANDARD_IA, ONEZONE_IA, INTELLIGENT_TIERING, DEEP_ARCHIVE, OUTPOSTS.
7. trusted-certificate — chemin complet vers un certificat de confiance lors de l'utilisation du stockage d'archives « s3 ». Soit le certificat auto-signé du fournisseur S3, soit celui de l'autorité de certification émettrice.
8. request-timeout — valeur du délai d'attente en secondes de la durée totale autorisée pour les requêtes S3. La valeur par défaut est 0 (attente indéfinie).

17.2. Configurer la durée de vie du journal des messages

Vous pouvez configurer la durée de vie des métadonnées du journal des messages et des messages archivés (ASiC) dans le stockage S3.

Métadonnées du journal des messages

Les métadonnées du journal des messages sont stockées sur le serveur de sécurité et sont utilisées pour retrouver les messages dans les archives. Par défaut, les métadonnées sont stockées pour toujours.

Lorsque la quantité de métadonnées occupe trop d'espace de stockage et que ces métadonnées ne sont pas indispensables, vous pouvez activer la suppression automatique des enregistrements de métadonnées. Réglez la valeur du paramètre `metadata-record-cleanup-operation` sur `DELETE`. Lorsque le nettoyage est activé, le serveur de sécurité commence à supprimer les enregistrements de métadonnées datant de plus de trois ans. La durée de vie maximale peut être configurée à l'aide du paramètre `metadata-record-lifetime-minutes` (voir [Paramètres d'archivage](#)). Choisissez une durée de stockage optimale pour votre serveur en fonction du volume de messages et de la demande de récupération des messages archivés.

La suppression des métadonnées compliquera la recherche d'un message spécifique si les messages sont archivés sur le système de fichiers du serveur de sécurité. Cependant, lorsque les messages sont archivés dans le stockage S3, la solution S3 fournit probablement des méthodes pour rechercher les messages.

L'activation de la suppression des métadonnées ne supprime pas les messages proprement dits ; le cycle de vie des conteneurs ASiC doit être traité séparément.

Voir également les autres paramètres de `metadata-*` pour affiner le nettoyage des métadonnées.

Messages archivés (ASiC)

L'archivage des messages vers le stockage S3 permet également de gérer le cycle de vie des objets stockés, y compris la suppression automatique des objets expirés. Reportez-vous au manuel de la solution de stockage S3 utilisée.

Si vous utilisez l'archivage vers le système de fichiers, configurez la commande exécutée après le processus d'archivage périodique (paramètre `archive-transfer-command`, voir [Paramètres d'archivage](#)). Cela permet de configurer un script externe pour transférer automatiquement les fichiers d'archives à partir du serveur de sécurité. Dans le cas contraire, les messages archivés restent sur le serveur de sécurité et ne sont pas supprimés. La possibilité de configurer la durée de vie des messages archivés sur le système cible dépend des capacités de ce système.

17.3. Transfert des fichiers d'archive à partir du système de fichiers local



Si vous archivez le journal des messages sur S3, le transfert des fichiers d'archive n'est pas nécessaire et vous pouvez ignorer cette section.

Si vous archivez le journal des messages sur le système de fichiers local, il est recommandé de transférer périodiquement les fichiers d'archive du serveur de sécurité (manuellement ou automatiquement) vers un emplacement externe, afin d'économiser de l'espace sur le disque dur.



Après avoir déplacé les fichiers d'archive vers un autre emplacement, vous ne pourrez plus utiliser le Vérificateur pour télécharger le message ou vérifier sa signature.

Pour l'archivage local du système de fichiers, les fichiers d'archive (conteneurs ZIP) sont situés dans le répertoire spécifié par le paramètre de configuration `archive-path`. Les noms de fichiers sont au format `mlog_X_Y.zip`, où `X` est l'horodatage de l'archivage (heure UTC au format `YYYYMMDDHHmmss`) et `Y` est l'identifiant de l'archive (qui est également sauvegardé dans les métadonnées des messages archivés). Voici un exemple de nom de fichier d'archive :

```
mlog_20210415120018_490a7a48-1e0a-480b-b6e0-3eac5d45f658.zip
```

Pour configurer un script de transfert, remplacez le paramètre de configuration `archive-transfer-command` (créez ou modifiez le fichier `/etc/uxp/conf.d/local.ini`).



Après avoir modifié la configuration, vous devez redémarrer le service `uxp-messagelog-archiver` :

```
sudo systemctl restart uxp-messagelog-archiver
```

Un exemple de script est fourni avec le logiciel SS UXP qui utilise le téléchargement HTTP POST pour le service web générique `/usr/share/uxp/scripts/archive-transport-http.sh`.

17.3.1. Exemple : HTTP POST

Le paquet `journal des messages` fournit un script d'aide `/usr/share/uxp/scripts/archive-transport-http.sh` pour transférer les fichiers d'archive. Ce script utilise le protocole HTTP/HTTPS (méthode POST, le nom du formulaire est `file`) pour transférer des fichiers d'archives vers un serveur d'archivage.

[message-log]

```
;; run after every 15 minutes
archive-interval=0 */15 * ? * * *
;; Command to run. By default, the mlog*zip filename is appended to command-line
automatically.
archive-transfer-command=/usr/share/uxp/scripts/archive-transport-http.sh
```

[archive-transport-http]

```
;; The URL of the archive server. Required. No default value.
url=http://host.domain/cgi-bin/upload

;; Location of the mlog*zip files. Default: directory=/var/lib/uxp/messagelog/archive/
directory=/var/lib/uxp/messagelog/archive/

;; If https server is used, the client certificate auth is attempted. Default: UXP
internal key/cert.
tls_key=/etc/uxp/ssl/internal.key
tls_cert=/etc/uxp/ssl/internal.crt
;; If additional CA or the host certificate pinning is used. Location of the PEM
formatted file.
```

```
;tls_trusted=/etc/ssl/archive-server.pem

;; resend=true -- send all (including unsent/failed) mlog*.zip files to server.
;; resend=false -- send only the file provided with command argument.
;; Default: resend=true
;resend=true

;; action=delete -- remove files from disk after successful transfer.
;; action=rename -- rename files after successful transfer. See rename_prefix option.
;; Default: action=rename
;action=rename

;; If rename is enabled -- the prefix added to filename. Default:
rename_prefix=transferred_
;rename_prefix=transferred_
```

Le fichier d'archive a été transféré avec succès lorsque le serveur d'archivage renvoie le code d'état HTTP 200.

17.4. Désactivation du stockage des signatures du métaservice, de la surveillance et/ou des messages réguliers

S'il n'est pas nécessaire de fournir des moyens de prouver la réception du métaservice [\[UXP-PR-META\]](#), de la surveillance [\[UXP-UG-PMA\]](#) et/ou des messages réguliers de demande et de réponse à une tierce partie, il est possible de désactiver l'enregistrement des signatures de ces messages.

Reportez-vous à la section [Fichiers de configuration](#) pour obtenir des instructions et remplacer les valeurs par défaut des paramètres booléens `log-metaservice-signatures`, `log-monitoring-signatures`, et `log-signatures` dans la section `[proxy]` respectivement. Par exemple :

```
[proxy]
log-metaservice-signatures=false
log-monitoring-signatures=false
log-signatures=false
```



Après avoir modifié la configuration, vous devez redémarrer le service `uxp-proxy` :

```
sudo systemctl restart uxp-proxy
```

18. Sauvegarde et restauration

Les fichiers de sauvegarde permettent de rétablir l'état antérieur du serveur de sécurité en cas de sinistre, de modification accidentelle ou de défaillance critique. Effectuez des sauvegardes régulières en fonction de la fréquence des modifications de la configuration de votre serveur afin de garantir qu'une sauvegarde fiable est toujours disponible pour la version actuelle de votre serveur de sécurité. Le serveur de sécurité ne prend en charge que la restauration à partir d'un fichier de sauvegarde créé dans la même version que le serveur cible.

La sauvegarde du serveur de sécurité est divisée en deux parties :

- La [sauvegarde de la configuration du serveur](#) comprend :
 - la copie de la base de données de configuration du serveur de sécurité, qui elle-même comprend :
 - le propriétaire du serveur de sécurité, les clients et leurs paramètres ;
 - la liste des membres UXP et de leurs sous-systèmes ;
 - les paramètres des dispositifs de création de signature connectés ;
 - les services d'horodatage sélectionnés ;
 - les jetons avec clés et certificats ;
 - les fichiers de configuration (par exemple, `local.ini`, `securityserver-rest-api-logback.xml`) ;
 - les certificats TLS des serveurs externes connectés (par exemple, Elasticsearch local) ;
 - l'ancre de configuration ;
 - la licence.
- La [sauvegarde du fournisseur d'identité](#) comprend :
 - la copie de la base de données du fournisseur d'identité du serveur de sécurité, qui contient les utilisateurs créés dans le gestionnaire des utilisateurs UXP ;
 - les fichiers de configuration du fournisseur d'identité.

Les sauvegardes ne comprennent pas :

- les fichiers journaux (vous pouvez transférer les fichiers journaux à un système externe de gestion des journaux à l'aide de `rsyslog`) ;
- le journal des messages (vous pouvez archiver les messages dans des compartiments S3, voir la section [Journal des messages](#)) ;
- les fichiers de sauvegarde (stockez des copies des fichiers de sauvegarde en dehors du serveur pour éviter de perdre la sauvegarde en cas de panne du serveur) ;
- les clés sur les dispositifs externes de création de signatures (suivez les instructions du fabricant pour le processus de sauvegarde des clés).

18.1. Sauvegarde du serveur de sécurité

Pour sauvegarder l'ensemble du serveur de sécurité, effectuez des sauvegardes de la configuration du serveur et du fournisseur d'identité. Pour restaurer complètement le serveur, restaurez les deux composants à partir de leurs fichiers de sauvegarde respectifs.

Par ailleurs, pour les sauvegardes régulières, vous pouvez choisir de sauvegarder et de restaurer uniquement la configuration du serveur ou uniquement le fournisseur d'identité – par exemple, si l'un des composants n'a pas changé.

Voir les instructions dans les sections suivantes.

18.1.1. Sauvegarder la configuration du serveur

Droits d'accès : privilèges de l'utilisateur root

Le processus de sauvegarde créera un fichier contenant la configuration du serveur de sécurité et le cryptera éventuellement. Vous pouvez ensuite utiliser ce fichier pour restaurer l'état de la configuration du serveur de sécurité au moment de la sauvegarde.

1. Pour créer un fichier de sauvegarde pour un serveur de sécurité, utilisez la commande :

```
sudo -u uxp /usr/share/uxp/scripts/backup_uxp_proxy_configuration.sh -s <security-
server-ID> \
-f <backup-file-location-and-name>
```

L'identifiant du serveur de sécurité se compose de l'identifiant du propriétaire et du code du serveur.

Vous pouvez utiliser le dossier `/var/lib/uxp/backup/` pour stocker des fichiers de sauvegarde.

Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/backup_uxp_proxy_configuration.sh -s
AA/GOV/SS10WNER/SS1 \
-f /var/lib/uxp/backup/ss_backup_`date +%Y%m%d-%H%M%S`.tar
```

Fournissez l'argument `-e` pour chiffrer la sauvegarde avec GPG, la phrase secrète est utilisée.

Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/backup_uxp_proxy_configuration.sh -s
AA/GOV/SS10WNER/SS1 \
-f /var/lib/uxp/backup/ss_backup_`date +%Y%m%d-%H%M%S`.tar -e
```

Saisissez une phrase secrète forte.

La phrase secrète sera utilisée pour crypter le fichier de sauvegarde. Conservez la phrase

secrète en toute sécurité, par exemple dans un gestionnaire de mots de passe. Vous aurez besoin de la phrase secrète pour décrypter le fichier de sauvegarde lors de la restauration du serveur.

2. Le script calcule et renvoie le hachage (digest) du fichier de sauvegarde. Enregistrez le hachage pour vérifier ultérieurement que le fichier de sauvegarde n'a pas été modifié.
3. Copiez le fichier de sauvegarde vers un emplacement de stockage externe afin de vous protéger contre la perte de données sur le serveur.



Le fichier de sauvegarde contient des données sensibles. Il doit être stocké en toute sécurité (par exemple, crypté et à accès contrôlé) afin d'empêcher tout accès non autorisé.

18.1.2. Sauvegarde du fournisseur d'identité

Droits d'accès : privilèges de l'utilisateur root

Le processus de sauvegarde créera un fichier d'archive tarball compressé et crypté par GPG contenant la configuration du fournisseur d'identité. Vous pouvez utiliser ce fichier ultérieurement pour restaurer l'état du fournisseur d'identité au moment de la sauvegarde.

1. Créez un fichier de sauvegarde pour le fournisseur d'identité à l'aide de la commande suivante :

```
sudo -u uxp /usr/share/uxp/scripts/identity-provider-backup.sh \
-d <backup-file-location>
```

`-d` est un argument facultatif, par défaut l'emplacement du fichier de sauvegarde est `/var/lib/uxp/backup/`.

Par exemple :

```
sudo -u uxp /usr/share/uxp/scripts/identity-provider-backup.sh
```

2. Saisissez une phrase secrète forte.
La phrase secrète sera utilisée pour crypter le fichier de sauvegarde. Conservez la phrase secrète en toute sécurité, par exemple dans un gestionnaire de mots de passe. Vous aurez besoin de la phrase secrète pour décrypter le fichier de sauvegarde lors de la restauration du serveur.
3. Le résultat sera un fichier nommé `uxp-identity-provider-backup_<server-hostname>_<datetime>.tar.gz.gpg`, enregistré dans le répertoire `/var/lib/uxp/backup/`.
4. Le script calcule et renvoie le hachage (digest) du fichier de sauvegarde. Enregistrez le hachage pour vérifier ultérieurement que le fichier de sauvegarde n'a pas été modifié.
5. Copiez le fichier de sauvegarde vers un emplacement de stockage externe afin de vous protéger contre la perte de données sur le serveur.



Le fichier de sauvegarde contient des données sensibles. Il doit être stocké en toute sécurité (par exemple, crypté et à accès contrôlé) afin d'empêcher tout accès non autorisé.

18.2. Restaurer un serveur de sécurité

18.2.1. Restaurer une configuration de serveur

Droits d'accès : privilèges de l'utilisateur root

Pour restaurer la configuration du serveur, vous avez besoin de l'identifiant du serveur de sécurité et d'un fichier de sauvegarde de la configuration du serveur créé pour la même version du serveur que le serveur cible. Consultez également le hachage du fichier de sauvegarde pour vérifier son intégrité et préparez la phrase secrète si le fichier est crypté.

Si le fichier de sauvegarde ne se trouve pas sur le serveur, déplacez-le d'abord du stockage externe vers le serveur. Vous pouvez le placer dans le répertoire `/var/lib/uxp/backup/`. Définissez les bons privilèges pour le fichier avec `sudo chown uxp:uxp <path-to-backup-file>`.



Veillez noter que le processus de restauration entraînera la déconnexion de tous les jetons de sécurité. Après la restauration, les codes PIN des jetons doivent être saisis dans l'interface utilisateur du serveur de sécurité pour recommencer à utiliser les clés stockées sur les jetons. Lors de la restauration d'un serveur en cours d'utilisation, l'échange de messages s'interrompt jusqu'à ce que les codes PIN des jetons soient saisis.

1. Pour restaurer le serveur de sécurité à partir d'un fichier de sauvegarde, utilisez la commande suivante :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_proxy_configuration.sh -s <security-  
server-ID> \  
-f <backup-file-location-and-name>
```

Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_proxy_configuration.sh -s  
AA/GOV/SS10WNER/SS1 \  
-f /var/lib/uxp/backup/ss_backup_20241001-104958.tar
```

Les sauvegardes cryptées par GPG sont décryptées automatiquement, la phrase secrète est utilisée.

Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_proxy_configuration.sh -s
AA/GOV/SS10WNER/SS1 \
-f /var/lib/uxp/backup/ss_backup_20241001-104958.tar.gpg
```

Lorsque vous y êtes invité, saisissez la phrase secrète du fichier de sauvegarde.

S'il est absolument nécessaire de restaurer le système à partir d'une sauvegarde effectuée sur un autre serveur de sécurité, le mode forcé de la commande restore peut être utilisé avec l'option `-F`. Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/restore_uxp_proxy_configuration.sh -F \
-f /var/lib/uxp/backup/ss_backup_20241001-104958.tar
```

2. Comparez le hachage calculé (digest) à celui calculé lors de la création de la sauvegarde pour vous assurer que le fichier n'a pas été modifié.
Il est fortement déconseillé de restaurer le serveur de sécurité à partir d'un fichier de sauvegarde dont les modifications sont inconnues.
3. Si vous disposez d'un compte utilisateur fonctionnel qui peut se connecter aux jetons, connectez-vous aux jetons de sécurité dans l'interface utilisateur du serveur de sécurité.
4. Si vous devez également restaurer les comptes utilisateur, passez à [restaurer un fournisseur d'identité](#).

18.2.2. Restaurer un fournisseur d'identité

Droits d'accès : privilèges de l'utilisateur root

Pour restaurer le fournisseur d'identité, vous avez besoin du fichier de sauvegarde du fournisseur d'identité créé pour la même version de serveur que le serveur cible et de sa phrase secrète. Consultez également le hachage du fichier de sauvegarde pour vérifier son intégrité et préparez la phrase secrète.

Si le fichier de sauvegarde ne se trouve pas sur le serveur, déplacez-le d'abord du stockage externe vers le serveur. Vous pouvez le placer dans le répertoire `/var/lib/uxp/backup/`. Définissez les bons privilèges pour le fichier avec `sudo chown uxp:uxp <path-to-backup-file>`.



Lorsque vous restaurez le fournisseur d'identité à partir d'une sauvegarde sur un serveur de sécurité mutualisé, assurez-vous que la licence appropriée est téléchargée, car les rôles spécifiques aux membres nécessitent une licence qui autorise la mutualisation. L'utilisation d'une licence qui n'autorise pas la mutualisation désactivera ces rôles, ce qui pourrait restreindre l'accès des utilisateurs.

1. Pour restaurer le fournisseur d'identité à partir d'un fichier de sauvegarde, utilisez la commande :

```
sudo -u uxp /usr/share/uxp/scripts/identity-provider-restore.sh \
<encrypted-backup-file>
```

Par exemple (tout sur une seule ligne) :

```
sudo -u uxp /usr/share/uxp/scripts/identity-provider-restore.sh \  
/var/lib/uxp/backup/uxp-identity-provider-backup_my-server.com_20250507-  
091320.tar.gz.gpg
```

2. Lorsque vous y êtes invité, saisissez la phrase secrète du fichier de sauvegarde.
3. Comparez le hachage calculé (digest) à celui calculé lors de la création de la sauvegarde pour vous assurer que le fichier n'a pas été modifié.
Il est fortement déconseillé de restaurer le serveur de sécurité à partir d'un fichier de sauvegarde dont les modifications sont inconnues.
4. Connectez-vous à l'interface utilisateur et vérifiez que les comptes d'utilisateur nécessaires sont présents.

18.2.3. Après la restauration

Une fois le processus de restauration terminé :

- si vous avez restauré la configuration du serveur, connectez-vous vous-même aux jetons de sécurité dans l'interface utilisateur du serveur de sécurité ou demandez à un Responsable des clés de le faire ;
- si vous avez restauré le fournisseur d'identité, vérifiez dans l'interface utilisateur si les comptes d'utilisateur nécessaires ont été restaurés.

19. API de gestion

19.1. Rest API

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

19.1.1. 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
```

19.1.2. 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
```

19.1.3. API du vérificateur

L'API du Vérificateur est utilisée pour consulter l'historique des transactions et vérifier les signatures des transactions enregistrées. La documentation de l'API est disponible à l'adresse suivante :

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

20. Maintenance

20.1. Changer l'adresse IP ou le nom DNS du serveur de sécurité

Droits d'accès : privilèges de l'utilisateur root + Administrateur Serveur

Pour changer l'adresse IP ou le nom DNS du serveur de sécurité, procédez comme suit.

1. Si le serveur de sécurité est déjà enregistré auprès de l'autorité de gouvernance (AG) UXP, vous devez informer l'AG de la nouvelle adresse IP ou du nouveau nom DNS conformément aux procédures organisationnelles de votre instance UXP (par exemple, par courrier électronique ou via le portail de support). Indiquez la nouvelle adresse IP ou le nouveau nom DNS ainsi que le code du serveur dans votre demande de changement.

Une fois que l'AG a appliqué les changements, la nouvelle adresse IP ou le nouveau nom DNS du serveur de sécurité est reflété dans la configuration globale.

2. Remplacez le certificat TLS Nginx en suivant les étapes décrites dans la section [Certificat TLS Nginx](#).
3. Connectez-vous à l'interface utilisateur du serveur de sécurité. Si vous ne parvenez pas à vous connecter et recevez une erreur `Authentication failed` alors que vous utilisez des identifiants corrects, suivez la section « Impossible de se connecter » du guide d'installation du serveur de sécurité [\[UXP-IG-SS\]](#) pour mettre à jour la configuration du fournisseur d'identité (section `[identity-provider]`) dans le fichier `/etc/uxp/conf.d/local.ini`.
4. Ajoutez un nouveau certificat TLS interne pour le serveur de sécurité et remplacez le certificat TLS interne actuellement actif en suivant les étapes décrites dans la section [Certificat TLS interne du serveur de sécurité](#).
5. Remplacez le certificat TLS du client Elasticsearch en suivant les étapes décrites dans le guide « Configuration de la surveillance du serveur de sécurité » [\[UXP-UG-PMA\]](#).
6. Reconfigurez tous les systèmes d'information concernés (client/service) connectés au serveur de sécurité afin qu'ils utilisent la nouvelle adresse IP ou le nouveau nom DNS du serveur, ainsi que le nouveau certificat TLS interne.

21. Journaux et services du système

Droits d'accès : privilèges de l'utilisateur root

21.1. Journaux

Pour lire les journaux, vous devez avoir les droits d'utilisateur root ou appartenir au groupe système adm.

Emplacement du journal	Description
/var/log/uxp/api.log	Enregistrements des activités liées à l'utilisation de l'API d'administration du serveur de sécurité
/var/log/uxp/verifier.log	Enregistrements des activités liées à l'utilisation de l'API de vérification des messages signés du serveur de sécurité
/var/log/uxp/identity-provider-rest-api.log	Enregistrements des activités liées à la gestion des utilisateurs du serveur de sécurité et à l'API d'authentification
/var/log/uxp/audit.log	Enregistrements des actions réussies et échouées des utilisateurs dans l'interface utilisateur du serveur de sécurité
/var/log/uxp/clientproxy_access.log	Enregistrements standards d'accès Web des demandes provenant d'un système d'information client vers le serveur de sécurité
/var/log/uxp/configuration_client.log	Enregistrements des activités liées au téléchargement de la configuration globale
/var/log/uxp/message_log_archiver.log	Enregistrements des activités liées à l'archivage périodique des enregistrements du journal des messages
/var/log/uxp/message_log_timestamper.log	Enregistrements des activités liées à l'horodatage périodique par lots des enregistrements du journal des messages
/var/log/uxp/ocsp_cache.log	Enregistrements des activités liées aux actualisations périodiques du cache et à l'utilisation du répondeur OCSP intégré
/var/log/uxp/proxy.log	Enregistrements des activités liées à l'échange de messages UXP (connexion aux serveurs de sécurité, droits d'accès, transmission des demandes, horodatage, archivage)
/var/log/uxp/proxymonitoragent.log	Enregistrements des activités liées à la collecte de données de surveillance environnementale et de statistiques réseau concernant le serveur de sécurité

Emplacement du journal	Description
<code>/var/log/uxp/serverproxy_access.log</code>	Enregistrements standards d'accès Web des demandes provenant d'un autre serveur de sécurité vers le serveur de sécurité actuel
<code>/var/log/uxp/serverconf-cli.log</code>	Enregistrements des activités liées à l'exportation et à l'importation de la configuration du serveur
<code>/var/log/postgresql/postgresql-<version>-main.log</code>	Enregistrement des erreurs d'accès à la base de données

21.2. Services du système

Les services système les plus importants d'un serveur de sécurité sont les suivants.

Service	Objectif	Journal
uxp-confclient	Processus client pour le distributeur de configuration globale	<code>/var/log/uxp/configuration_client.log</code>
uxp-messagelog-archiver	Archivage du journal des messages	<code>/var/log/uxp/messagelog_archiver.log</code>
uxp-messagelog-timestamper	Horodatage du journal des messages	<code>/var/log/uxp/messagelog_timestamper.log</code>
uxp-monitor	Processus de surveillance	<code>/var/log/uxp/proxymonitoragent.log</code>
uxp-ocsp-cache	Cache OCSP	<code>/var/log/uxp/ocsp_cache.log</code>
uxp-proxy	Échangeur de messages	<code>/var/log/uxp/proxy.log</code>
uxp-securityserver-rest-api	API REST du serveur de sécurité	<code>/var/log/uxp/api.log</code>
uxp-verifier-rest-api	API REST du Vérificateur du serveur de sécurité	<code>/var/log/uxp/verifier.log</code>
uxp-identity-provider-rest-api	API REST du Fournisseur d'identité du Serveur de sécurité	<code>/var/log/uxp/identity-provider-rest-api.log</code>
nginx	Serveur Web qui échange les services du serveur d'application de l'interface utilisateur et de l'échangeur de messages	<code>/var/log/nginx/</code>
postgresql	Service de base de données pour le stockage de données dynamiques	<code>/var/log/postgresql/postgresql-16-main.log</code>

Les services système sont gérés via la fonctionnalité `systemd`.

Pour démarrer un service :

```
sudo systemctl start <service>
```

Pour arrêter un service :

```
sudo systemctl stop <service>
```

Pour vérifier l'état du service :

```
sudo systemctl status <service>
```

Pour vérifier les journaux des services du système :

```
sudo journalctl -u <service>
```

21.3. Configuration de la journalisation

Le système **Logback** est utilisé pour la journalisation.

Dans Logback, les niveaux de journalisation sont classés du plus bas au plus haut en fonction de leur gravité :

TRACE < DEBUG < INFO < WARN < ERROR.

Notez qu'il n'est pas recommandé de définir un niveau de journalisation inférieur à `INFO` sur les systèmes de production pendant plus longtemps que nécessaire, car la verbosité excessive des niveaux inférieurs peut épuiser les ressources de votre système.

Les paramètres par défaut de la journalisation sont les suivants :

- les enregistrements sont consignés au niveau `INFO` ;
- une nouvelle archive ZIP des enregistrements du journal est créée une fois par jour ou lorsque la taille du fichier journal atteint 100 Mo (`maxFileSize` dans la politique de roulement) ;
- les enregistrements sont conservés pendant 60 jours (`maxHistory`) ou jusqu'à ce que 1 Go d'espace de stockage (`totalSizeCap`) ait été utilisé.

21.3.1. Configuration des paramètres de journalisation des composants

Chaque composant UXP possède son propre fichier de configuration **Logback**

Service	Fichier de configuration
uxp-confclient	/etc/uxp/conf.d/confclient-logback.xml

Service	Fichier de configuration
uxp-messagelog-archiver	/etc/uxp/conf.d/messagelog-archiver-logback.xml
uxp-messagelog-timestamper	/etc/uxp/conf.d/messagelog-timestamper-logback.xml
uxp-monitor	/etc/uxp/conf.d/addons/proxy-monitor-agent-logback.xml
uxp-ocsp-cache	/etc/uxp/conf.d/ocsp-cache-logback.xml
uxp-proxy	/etc/uxp/conf.d/proxy-logback.xml
uxp-securityserver-rest-api	/etc/uxp/conf.d/securityserver-rest-api-logback.xml
uxp-verifier-rest-api	/etc/uxp/conf.d/verifier-rest-api-logback.xml
uxp-identity-provider-rest-api	/etc/uxp/conf.d/identity-provider-rest-api-logback.xml

Tous les fichiers de configuration de journalisation suivent la même structure générale. Par exemple, pour chaque fichier journal généré par un composant, il existe une section qui configure la politique de stockage des anciens fichiers journaux :

```
<appender name="FILE" class="ch.qos.logback.core.rolling.RollingFileAppender">
  <file>${logOutputPath}/proxy.log</file>
  <rollingPolicy class="ch.qos.logback.core.rolling.SizeAndTimeBasedRollingPolicy">
    <fileNamePattern>${logOutputPath}/proxy.%d{yyyy-MM-dd}.%i.log.zip</fileNamePattern>
    <!-- Each file should be at most 100MB, keep 60 days worth of history, but at
    most 1GB -->
    <maxFileSize>100MB</maxFileSize>
    <maxHistory>60</maxHistory>
    <totalSizeCap>1GB</totalSizeCap>
  </rollingPolicy>
  <encoder>
    <pattern>%d [%thread] %-5level %logger{36} - [%X{transactionId}]
    %msg%n</pattern>
    <charset>UTF-8</charset>
  </encoder>
</appender>
```

Pour modifier la taille des archives ZIP et la durée de stockage des archives, modifiez les paramètres `maxFileSize`, `maxHistory` et `totalSizeCap` dans la section `rollingPolicy`.

En outre, le paramètre `pattern` décrit le modèle de journalisation utilisé pour les entrées du fichier journal. Elle peut être configurée conformément à [\[LOGBACK-PATTERNS\]](#). Le modèle de composant proxy comprend un mot de conversion spécial `transactionId`, qui lie chaque entrée de journal à une transaction spécifique traitée par le composant.

21.4. Détail de l'erreur UUID

Si un serveur de sécurité rencontre une condition d'erreur pendant l'échange de messages, il renvoie au système d'information du client du service un message d'erreur SOAP [\[UXP-PR-MESS\]](#) contenant un UUID (identificateur universel unique, par exemple 1328e974-4fe5-412c-a4c4-f1ac36f20b14) comme détail de l'erreur. L'UUID peut être utilisé pour trouver les détails de l'erreur survenue dans le journal `uxp-proxy`.

21.5. Journal d'audit

Le serveur de sécurité conserve un journal d'audit — journal des tentatives réussies et échouées de modification de la configuration du serveur de sécurité.

Les événements du journal d'audit sont générés par l'API du serveur de sécurité. Ainsi, les actions des utilisateurs et celles effectuées par un système externe qui utilise l'API du serveur de sécurité sont consignées.

Toutes les actions utilisateur ayant échoué ne sont pas consignées. Dans certains cas, l'interface utilisateur du serveur de sécurité renvoie une erreur à l'utilisateur sans envoyer la requête à l'API du serveur de sécurité.

Les actions qui modifient la configuration du serveur mais qui ne sont pas effectuées à l'aide de l'interface utilisateur du serveur de sécurité ne sont pas consignées (par exemple, l'installation et la mise à jour du logiciel UXP, ainsi que la modification des fichiers de configuration).

Le format des événements et la liste complète des événements du journal d'audit sont décrits dans [\[UXP-SPEC-AL\]](#).

Exemple d'enregistrement dans le journal d'audit :

```
{
  "createdAt": "2024-09-04T14:53:12.136+0300",
  "hostname": "securityserver1",
  "version": "1.22",
  "event": {
    "name": "Upload license",
    "result": "FAILURE",
    "request": {
      "httpMethod": "POST",
      "path": "/api/v1/license",
    },
    "error": {
      "message": "Malformed license file.",
      "code": "license.malformed_file",
      "data": {}
    },
  },
  "actor": {
```

```
"username": "johnsmith",
"clientId": "uxp-ss-ui",
"remoteAddress": "192.168.0.38"
}
}
```

Par défaut, le journal d'audit est situé dans le fichier :

```
/var/log/uxp/audit.log
```

21.5.1. Changer la configuration du journal d'audit

Le logiciel UXP écrit le journal d'audit dans `syslog` (`rsyslog`) à l'aide de l'interface UDP (le port par défaut est 514). La configuration correspondante se trouve dans le fichier

```
/etc/rsyslog.d/90-udp.conf
```

Les enregistrements du journal d'audit sont rédigés avec le niveau `INFO` et l'origine `LOCAL0`. Par défaut, les enregistrements de ce niveau et de cette origine sont sauvegardés dans le fichier d'audit UXP

```
/var/log/uxp/audit.log
```

Le comportement par défaut peut être modifié en éditant le fichier de configuration de `rsyslog`

```
/etc/rsyslog.d/40-uxp.conf
```

Redémarrez le service `rsyslog` pour appliquer les modifications apportées au fichier de configuration

```
sudo systemctl restart rsyslog
```

Le journal d'audit fait l'objet d'une rotation mensuelle par `logrotate`. Pour configurer la rotation du journal d'audit, modifiez le fichier de configuration de `logrotate`

```
/etc/logrotate.d/uxp-proxy
```

21.5.2. Archivage du journal d'audit

Afin d'économiser de l'espace sur le disque dur et d'éviter la perte des enregistrements du journal d'audit en cas de panne du serveur de sécurité, il est recommandé d'archiver périodiquement les fichiers du journal d'audit sur un support de stockage externe ou sur un serveur de journalisation.

Le logiciel UXP n'offre pas d'outils spéciaux pour l'archivage du journal d'audit. `rsyslog` peut être configuré pour rediriger le journal d'audit vers un emplacement externe.

22. Outil de diagnostic

Si l'interface utilisateur du serveur est fonctionnelle et que la configuration initiale est terminée, vous pouvez utiliser l'**Outil de diagnostic** de l'interface utilisateur pour le dépannage. Sur la page **Outil de diagnostic**, vous pouvez :

- afficher et filtrer les événements d'erreur et d'avertissement des 7 derniers jours ;
- identifier et analyser les événements les plus urgents et les plus fréquents sur le serveur ;
- télécharger les journaux relatifs à un service particulier du système UXP pour effectuer une analyse hors ligne ou pour les transmettre à l'équipe d'assistance UXP ;
- générer et télécharger le rapport de diagnostic du système pour le transmettre à l'équipe d'assistance UXP.

22.1. Dépannage des journaux dans l'interface utilisateur

L'outil de diagnostic utilise la terminologie suivante lorsqu'il traite des journaux et des données liées aux journaux :

Événement — Enregistrements similaires du même service du système UXP, qui sont regroupés en fonction du message de l'enregistrement. Les événements peuvent contenir des problèmes.

Problème — Messages analysés à partir des traces de pile des enregistrements de journal d'un événement.

Les fichiers journaux sont divisés en plusieurs catégories :

Échange de messages — Enregistre les données relatives à l'échange de messages entre deux serveurs de sécurité ou entre un serveur de sécurité et des systèmes d'information.

Surveillance — Enregistrements liés aux processus de surveillance UXP.

Gestion — Enregistre les journaux liés aux activités backend et frontend du serveur de sécurité.

Journal des messages — Enregistrements liés au Vérificateur UXP et aux processus du journal des messages.

L'outil de diagnostic affiche les événements `WARN` et `ERROR` ainsi que les problèmes associés aux services de système UXP suivant au cours des 7 derniers jours :

Service système UXP	Fichier journal source	Catégorie
uxp-proxy	proxy.log	Échange de messages
uxp-confclient	configuration_client.log	Échange de messages

Service système UXP	Fichier journal source	Catégorie
uxp-ocsp-cache	ocsp_cache.log	Échange de messages
uxp-monitor	proxymonitoragent.log	Surveillance
uxp-identity-provider-rest-api	identity-provider-rest-api.log	Gestion
uxp-securityserver-rest-api	api.log	Gestion
uxp-verifier-rest-api	verifier.log	Journal des messages
uxp-messagelog-timestamper	messagelog_timestamper.log	Journal des messages
uxp-messagelog-archiver	messagelog_archiver.log	Journal des messages



Les journaux se trouvent dans le répertoire `/var/log/uxp/`.



L'outil de diagnostic n'affiche pas les événements avec les niveaux de gravité TRACE, DEBUG et INFO, ni les événements antérieurs aux 7 derniers jours. Pour afficher tous les enregistrements du journal, vous devez vous connecter au serveur à l'aide de SSH.



Toutes les alertes et erreurs ne nécessitent pas une intervention administrative, certaines sont simplement informatives, par exemple en cas de saisie incorrecte du mot de passe.

22.1.1. Visualisation des journaux

Droits d'accès : Administrateur serveur

Pour afficher les événements, accédez à la page **Outil de diagnostic**.

Dans le tableau des événements, chaque événement est décrit par :

- Gravité — ● ERROR ou ● WARN ;
- Message d'événement — description unique de l'événement ;
- Source — fichier journal source dans lequel l'événement a été lu ;
- Nombre — nombre d'enregistrements de journal qui se sont produits au cours des 7 derniers jours pour cet événement ;
- Dernière occurrence — horodatage de l'enregistrement le plus récent dans le journal, en heure locale ;
- Première occurrence — horodatage de l'enregistrement le plus ancien dans les 7 derniers jours, en heure locale.

Cliquez sur une ligne d'événement pour afficher les problèmes concrets.



Cliquez sur une ligne pour afficher la description du problème correspondant :


- Nombre — nombre de fois où le problème s'est produit au cours des 7 derniers jours ;
- Dernière occurrence — horodatage de l'enregistrement le plus récent dans le journal ;
- Première occurrence — horodatage de l'enregistrement le plus ancien dans les 7 derniers jours ;
- Le dernier enregistrement du journal.

Si un événement ne présente pas de problèmes, les derniers enregistrements du journal sont affichés.

22.1.2. Filtrer les journaux

Pour filtrer les événements, cliquez sur l'une des options de filtrage disponibles :

- **Gravité**  ERROR / **Gravité**  WARN — le filtre affichera tous les événements avec la gravité d'erreur ou d'avertissement ;
- **Fichier journal source** spécifique — le filtre affiche tous les événements liés au fichier journal source sélectionné.

Notez que si un fichier journal source ne contient aucun événement d'erreur ou d'avertissement, il est masqué en tant qu'option de filtrage. Si le traitement du journal a échoué pour un fichier journal source, cela est indiqué par une icône d'erreur  et vous ne pouvez pas sélectionner l'affichage de ses événements.

S'il n'y a pas d'événements ERROR ou WARN, le nombre à côté de la gravité est omis.

22.2. Exporter des journaux

Droits d'accès : Administrateur serveur

Dans certains cas, l'outil de diagnostic ne fournit pas suffisamment d'informations pour diagnostiquer la cause d'un problème. Dans ce cas, il est possible d'exporter le journal depuis le serveur sans avoir à utiliser SSH.

Pour exporter un journal pour un composant/service spécifique, procédez comme suit.

1. Dans le tableau des événements, cliquez sur la ligne correspondant à l'événement.
2. Cliquez sur **Exporter le journal** pour exporter les journaux.

Le journal exporté (compressé dans un fichier .zip) contient le fichier journal du jour et tous les fichiers journaux archivés des 7 derniers jours.

22.3. Générer un rapport de diagnostic

Dans certains cas de problèmes complexes, il peut être nécessaire de générer un rapport de diagnostic complet du système. Ce rapport peut ensuite être transmis à l'équipe d'assistance.

Le rapport de diagnostic contient des informations pertinentes pour le débogage du système. Le fichier ne contient pas de vidages de bases de données ni d'informations sensibles en matière de sécurité, telles que des clés privées ou des mots de passe.

Ce rapport de diagnostic (comprimé dans un fichier `tar.gz`) comprend des informations sur les points suivants :

- Informations générales sur le serveur :
 - Nom d'hôte ;
 - FQDN ;
 - Interfaces réseau ;
 - Table de routage ;
 - Ports ouverts ;
 - Paramètres régionaux du système ;
 - Configuration de la date et de l'heure ;
 - Connectivité au dépôt de Cybernetica ;
 - Paquets installés ;
- Configuration Nginx `/etc/nginx` ;
- Configuration UXP `/etc/uxp` :
 - Configuration globale ;
 - Aperçu du service d'horodatage ;
 - Aperçu des services OCSP ;
 - Serveurs de sécurité ;
 - Serveurs de sécurité de gestion ;
 - Sous-systèmes ;
 - Adresses de serveurs, hachages de certificats et ports ouverts ;
- Fichiers journaux :
 - Services UXP `/var/log/uxp` (7 derniers jours) ;
 - PostgreSQL.

22.3.1. Générer un rapport à partir de l'interface utilisateur

Droits d'accès : Administrateur serveur

1. Naviguez jusqu'à la page de l'**Outil de diagnostic** dans l'interface utilisateur.
2. Cliquez sur **Générer un rapport**.

Le fichier est alors généré et téléchargé sur votre ordinateur.

22.3.2. Générer un rapport à partir de l'interface de programmation

Droits d'accès : privilèges de l'utilisateur root

1. Ouvrez une connexion SSH au serveur, avec les permissions root.
2. Exécutez la commande suivante :

```
sudo uxp-generate-diagnostics-report
```

Cela générera le rapport dans le répertoire actuel. Vous pouvez utiliser SCP ou SFTP pour copier le rapport sur votre ordinateur.

23. 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.

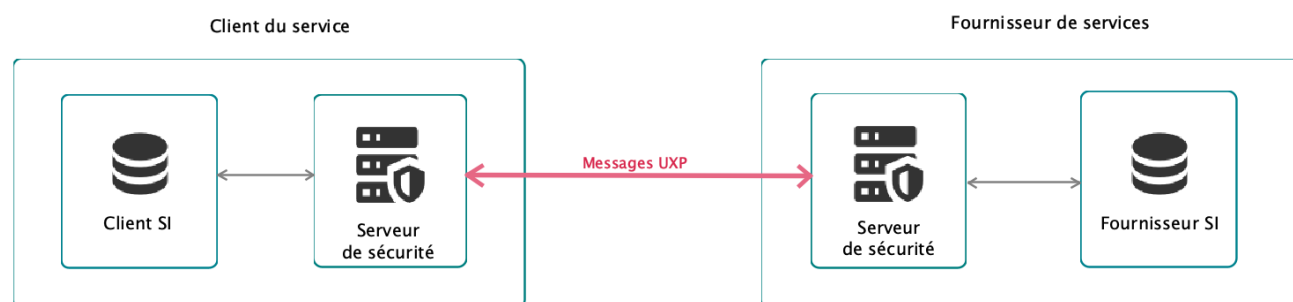


Figure 2. Diagramme montrant l'échange de messages UXP

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).

23.1. 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 />
<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 [\[UXP-PR-MESS\]](#).

23.2. Erreurs provenant du système d'information du client du service

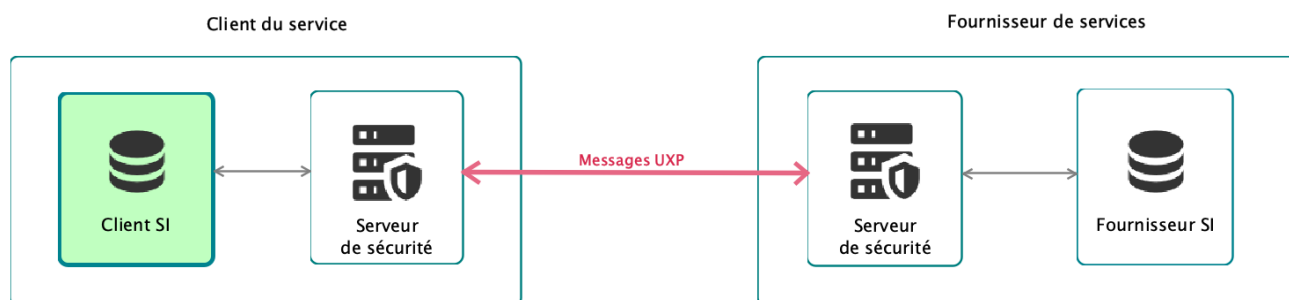


Figure 3. Cette section couvre les codes d'erreur provenant du système d'information du client du service (mis en évidence).

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 [UXP-PR-MESS]). 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 [UXP-PR-MESS]).	

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 [UXP-PR-MESS]). 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	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 [UXP-PR-MESS]). Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).	

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	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 [UXP-PR-MESS]). Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).	

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	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 [UXP-PR-MESS]). Pour plus de détails sur l'erreur, consultez le journal du proxy du SS du client du service (/var/log/uxp/proxy.log).	

23.3. Erreurs provenant du serveur de sécurité du client du service

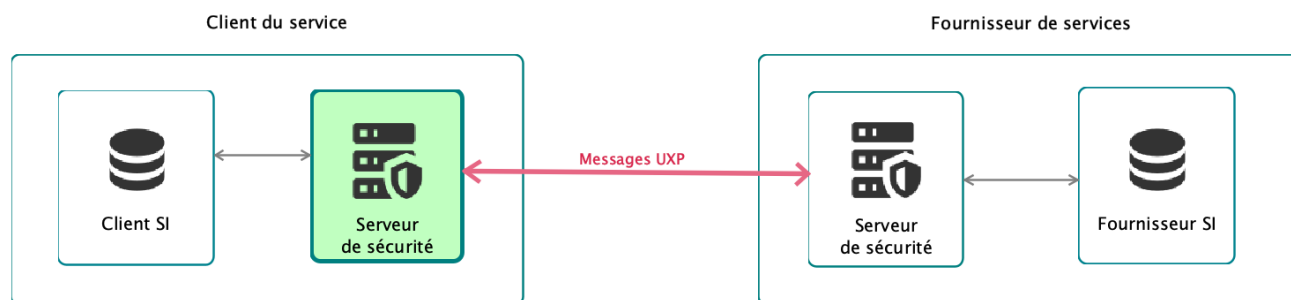


Figure 4. Cette section couvre les codes d'erreur provenant du serveur de sécurité du client du service (mis en évidence).

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 Envoi de demandes à une API REST).	

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 Ajouter un client au serveur de sécurité)

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"> • Le SS possède au moins un certificat d'authentification (voir la section UG-SS Ajouter une clé et un certificat d'authentification pour le serveur de sécurité). • Le certificat se trouve sur un jeton qui est connecté. • Le certificat est enregistré (voir UG-SS Section États d'enregistrement des certificats d'authentification). • Le certificat est actif (voir section UG-SS Activer et désactiver des certificats). • La réponse OCSP du certificat est bonne (voir UG-SS Section Validité du certificat).

Message d'erreur	Solution Responsable des services	Solution Administrateur SS
Service provider security server has no valid authentication certificate	Contactez l'administrateur SS du fournisseur de services	<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"> • Le SS possède au moins un certificat d'authentification (voir la section UG-SS Configurer une clé et un certificat d'authentification pour le serveur de sécurité). • Le certificat se trouve sur un jeton qui est connecté. • Le certificat est enregistré (voir UG-SS Section États d'enregistrement des certificats d'authentification). • Le certificat est actif (voir section UG-SS Activer et désactiver des certificats). • La réponse OCSP du certificat est bonne (voir UG-SS Section Validité du certificat).
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 Communication avec les systèmes d'information des clients).	

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"> • Il existe au moins un certificat de signature pour le membre auquel appartient le sous-système (voir la section UG-SS Configurer une clé et un certificat de signature pour un client du serveur de sécurité). • Le certificat se trouve sur un jeton qui est connecté. • Le certificat est actif (voir section UG-SS Activer et désactiver des certificats). • La réponse OCSP du certificat est bonne (voir UG-SS Section Validité du certificat).

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"> • Le SS du client du service peut se connecter au service d'horodatage. Vérifiez que tous les pare-feu sont correctement configurés. • Le service d'horodatage est disponible. Consultez le journal du proxy (/var/log/uxp/proxy.log) pour plus de détails.

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 fournisseur de services	Le SS du fournisseur de services est introuvable parce qu'il est enregistré avec le mauvais FQDN.

23.4. Erreurs provenant du serveur de sécurité du fournisseur de services

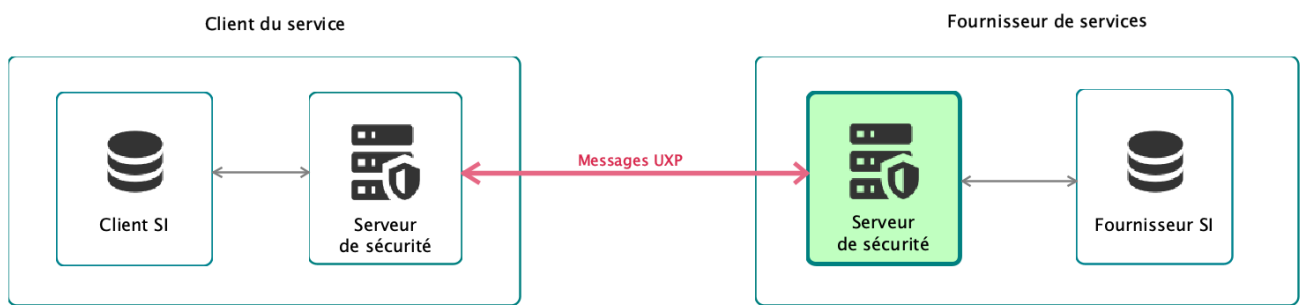


Figure 5. Cette section couvre les codes d'erreur provenant du serveur de sécurité du fournisseur de services (mis en évidence).

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 Droits d'accès .	

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 [UXP-PR-MESS] 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 Communication avec les systèmes d'information des clients . 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 Communication avec les systèmes d'information des clients).	

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"> • Il existe au moins un certificat de signature pour le membre auquel appartient le sous-système (voir la section UG-SS Configurer une clé et un certificat de signature pour un client du serveur de sécurité). • Le certificat se trouve sur un jeton qui est connecté. • Le certificat est actif (voir section UG-SS Activer et désactiver des certificats). • La réponse OCSP du certificat est bonne (voir UG-SS Section Validité du certificat).

`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 Services d'horodatage).

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"> • 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. • 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.

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>

24. Dépannage détaillé

24.1. Erreur de mémoire insuffisante du proxy

Droits d'accès : privilèges de l'utilisateur root

L'une des causes des erreurs de mémoire (`java.lang.OutOfMemoryError: Java heap space` dans `/var/log/uxp/proxy.log`) peut être que la charge totale (principalement la quantité de mémoire occupée par les messages reçus dans un court laps de temps) dépasse la mémoire allouée à la machine virtuelle Java (JVM) pour le service `uxp-proxy`.

La solution à ce problème consiste à augmenter la mémoire allouée à la JVM proxy. La valeur par défaut est de 512 Mo. Il est recommandé d'augmenter la mémoire par incréments jusqu'à ce que le problème soit résolu.

Pour remplacer la valeur par défaut, modifiez le fichier `/etc/uxp/services/local.conf` en ajoutant une nouvelle valeur de taille maximale du tas à la variable `PROXY_JVM_OPTS`.

Ajoutez la ligne suivante au fichier `local.conf` ou modifiez la ligne existante :

```
PROXY_JVM_OPTS="${PROXY_JVM_OPTS} -Xmx<size>"
```

Par exemple, pour fixer la valeur maximale du tas de mémoire à 1024 Mo :

```
PROXY_JVM_OPTS="${PROXY_JVM_OPTS} -Xmx1024m"
```

Après avoir modifié la configuration, redémarrez le service `uxp-proxy` pour appliquer les changements :

```
sudo systemctl restart uxp-proxy
```

24.2. Erreur de mémoire insuffisante du Vérificateur ou de l'archiveur Messagelog

Droits d'accès : privilèges de l'utilisateur root

De manière similaire à l'[Erreur de mémoire insuffisante du proxy](#), si des erreurs de mémoire insuffisante se produisent pendant la vérification (`java.lang.OutOfMemoryError: Java heap space` dans `/var/log/uxp/verifier.log`) ou l'archivage de messages (`java.lang.OutOfMemoryError: Java heap space` dans `/var/log/uxp/messagelog_archiver.log`), la solution consiste à augmenter la mémoire allouée à la JVM pour le service `uxp-verifier-rest-api` (vérificateur) et/ou le service `uxp-messagelog-archiver` (archiveur messagelog). La valeur par défaut et la valeur minimale recommandée pour la mémoire de la JVM est de 256 Mo.

La taille de mémoire par défaut de la JVM permet de vérifier et d'archiver des messages

d'une taille maximale de 64 Mo (y compris les pièces jointes). Par défaut, le serveur de sécurité stocke les messages dont la taille ne dépasse pas 5 Mo (potentiellement plus dans le cas d'un message SOAP avec des pièces jointes). Si vous avez augmenté les limites de stockage, de sorte que le serveur stocke des messages d'une taille supérieure à 64 Mo (avec les pièces jointes), vous devez ajouter de l'espace disque au vérificateur et/ou à l'archiver.



La prise en charge de la vérification et de l'archivage des messages jusqu'à 64 Mo avec les valeurs de mémoire par défaut de la JVM est une estimation. Les conditions réelles peuvent varier.

En fonction des informations dont vous disposez, choisissez votre méthode de calcul de la nouvelle valeur de la mémoire de la JVM :

- en fonction de vos nouvelles limites de stockage des messages, voir la section [Calcul de la mémoire JVM en fonction des limites de stockage](#) ;
- si la taille du message à l'origine de l'erreur est connue, vous pouvez calculer la nouvelle valeur de la mémoire de la JVM à l'aide de la taille du message, voir la section [Calcul de la mémoire JVM en fonction de la taille des messages](#) ;
- si la taille du message à l'origine de l'erreur est inconnue, vous pouvez augmenter progressivement la mémoire de la JVM, voir la section [Augmentation progressive de la mémoire JVM](#).

Pour remplacer la valeur par défaut, modifiez le fichier `/etc/uxp/services/local.conf` en ajoutant une nouvelle valeur de taille maximale du tas à la variable `VERIFIER_REST_API_JVM_OPTS` pour le service `uxp-verifier-rest-api` et/ou à la variable `MESSAGELOG_ARCHIVER_JVM_OPTS` pour le service `uxp-message-log-archiver`.

Augmenter la mémoire JVM du Vérificateur

Pour remplacer la valeur par défaut du vérificateur, ajoutez la ligne suivante au fichier `local.conf` ou modifiez la ligne existante :

```
VERIFIER_REST_API_JVM_OPTS="${VERIFIER_REST_API_JVM_OPTS} -Xmx<size>"
```

Par exemple, pour fixer la valeur maximale du tas de mémoire à 1024 Mo :

```
VERIFIER_REST_API_JVM_OPTS="${VERIFIER_REST_API_JVM_OPTS} -Xmx1024m"
```

Après avoir modifié la configuration, redémarrez le service `uxp-verifier-rest-api` pour appliquer les changements :

```
sudo systemctl restart uxp-verifier-rest-api
```

Augmenter la mémoire JVM de l'Archiver

Pour remplacer la valeur par défaut de l'archiver `message-log`, ajoutez la ligne suivante au fichier `local.conf` ou modifiez la ligne existante :

```
MESSAGELOG_ARCHIVER_JVM_OPTS="${MESSAGELOG_ARCHIVER_JVM_OPTS} -Xmx<size>"
```

Par exemple, pour fixer la valeur maximale du tas de mémoire à 1024 Mo :

```
MESSAGELOG_ARCHIVER_JVM_OPTS="${MESSAGELOG_ARCHIVER_JVM_OPTS} -Xmx1024m"
```

Après avoir modifié la configuration, redémarrez le service `uxp-message-log-archiver` pour appliquer les changements :

```
sudo systemctl restart uxp-message-log-archiver
```

24.2.1. Calcul de la mémoire JVM en fonction des limites de stockage

La taille de la mémoire JVM du vérificateur et de l'archivage est optimisée pour les limites de stockage par défaut. Si vous augmentez considérablement les limites de stockage et que vous souhaitez que la vérification et l'archivage continuent à fonctionner, vous devez augmenter la taille du tas.

Les limites de stockage des messages par défaut sont d'environ 5 Mo. Supposons que les nouvelles valeurs dans le fichier `local.ini` sous la section `[proxy]` sont fixées à 35 Mo :

```
[proxy]
max-retained-soap-attachment-size-bytes=36700160
max-retained-soap-message-size-bytes=36700160
max-retained-rest-payload-size-bytes=36700160
```

Voici les instructions pour calculer la valeur du tas en fonction de vos nouvelles limites de stockage :

1. Convertissez les limites de stockage en mégaoctets, en arrondissant si nécessaire :
 - a. `max-retained-soap-attachment-size-bytes` – 36 700 160 octets = 35 Mo ;
 - b. `max-retained-soap-message-size-bytes` – 36 700 160 octets = 35 Mo ;
 - c. `max-retained-rest-payload-size-bytes` – 36 700 160 octets = 35 Mo ;
2. Calculez la taille potentielle des messages SOAP stockés, y compris les pièces jointes :
 - a. estimez le nombre moyen de pièces jointes SOAP qui seront incluses, par exemple 2 pièces jointes ;
 - b. multipliez le nombre de pièces jointes par la taille des pièces jointes SOAP en Mo et ajouter la taille du message SOAP :

$$2 * 35 \text{ MB} + 35 \text{ MB} = 105 \text{ MB}$$

3. Choisissez la plus grande taille entre les messages REST et les messages SOAP, y compris les pièces jointes – dans l'exemple, 105 MB pour SOAP, 35 MB pour REST. Les services SOAP stockés sont potentiellement plus volumineux.
4. Calculez la taille estimée du tas – `size = 128 + 2 * total_message_size_in_mb`, où `total_message_size_in_mb` est la valeur la plus élevée. Dans l'exemple, `128 + 2 *`

105 = 338 MB, augmentez la taille de la mémoire JVM du vérificateur et de l'archivageur à 338 MB. Si le nombre calculé est inférieur à 256, la taille de la mémoire par défaut devrait suffire.

24.2.2. Calcul de la mémoire JVM en fonction de la taille des messages

Si la taille du message défaillant est connue, la valeur de `size` peut être calculée à l'aide de la formule $size = 128 + 2 * total_message_size_in_mb$, où `total_message_size_in_mb` est la taille totale du message en mégaoctets qui a provoqué l'erreur de mémoire insuffisante.

Exemple :

La vérification et/ou l'archivage d'un message de 100 Mo a échoué. Étant donné `total_message_size_in_mb = 100 MB`, nous calculons que la nouvelle `size` est $128 + 2 * 100 = 328$ MB.

Ajoutez ou modifiez la taille du tas du vérificateur dans `/etc/uxp/services/local.conf` :

```
VERIFIER_REST_API_JVM_OPTS="${VERIFIER_REST_API_JVM_OPTS} -Xmx328m"
```

Ajoutez ou modifiez la taille du tas de l'archivageur dans `/etc/uxp/services/local.conf` :

```
MESSAGELOG_ARCHIVER_JVM_OPTS="${MESSAGELOG_ARCHIVER_JVM_OPTS} -Xmx328m"
```

24.2.3. Augmentation progressive de la mémoire JVM

Si la taille du message défaillant est inconnue, la valeur de `size` peut être augmentée progressivement jusqu'à ce que l'erreur soit résolue. L'incrément recommandé est de 128 Mo, ajoutés à la valeur actuelle.

Exemple :

La vérification des messages a échoué pour un message de taille inconnue. Augmentez progressivement la valeur actuelle, qui dans cet exemple est de 256 Mo, jusqu'à 384 Mo, en ajoutant ou en modifiant `/etc/uxp/services/local.conf` :

Lors de l'augmentation de la taille du tas du vérificateur :

```
VERIFIER_REST_API_JVM_OPTS="${VERIFIER_REST_API_JVM_OPTS} -Xmx384m"
```

Lors de l'augmentation de la taille du tas de l'archivageur :

```
MESSAGELOG_ARCHIVER_JVM_OPTS="${MESSAGELOG_ARCHIVER_JVM_OPTS} -Xmx384m"
```

Répétez jusqu'à ce que l'erreur de mémoire insuffisante soit résolue : 384 Mo → 512 Mo → 640 Mo. Si l'erreur se résout avec 640 Mo, `/etc/uxp/services/local.conf` devrait avoir la valeur :

Lors de la correction de l'erreur de mémoire du vérificateur :

```
VERIFIER_REST_API_JVM_OPTS="${VERIFIER_REST_API_JVM_OPTS} -Xmx640m"
```

Lors de la correction de l'erreur de mémoire de l'archiver :

```
MESSAGELOG_ARCHIVER_JVM_OPTS="${MESSAGELOG_ARCHIVER_JVM_OPTS} -Xmx640m"
```

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.