

Serveur de sécurité UXP 1.25

Guide de gestion des clés de signature

UXP-UG-SSKEY

Table des matières

Dernières notes de mise à jour	1
1. Introduction	3
1.1. Serveur de sécurité UXP	3
1.2. Concepts UXP	3
1.3. Références	7
2. Gérer mon compte	9
2.1. Affichage de mes rôles	9
2.2. Changer de mot de passe	9
2.3. Réinitialiser un mot de passe oublié	9
2.4. Tentatives de connexion et verrouillage	9
3. Clés de signature	10
3.1. Jetons	10
3.1.1. Jetons logiciels	10
3.1.2. Jetons matériels	11
3.2. Générer une clé et une CSR	12
3.3. Importer un fichier de certificat	12
3.4. Importer un certificat depuis un dispositif	13
3.5. Activer et désactiver les certificats	14
3.6. Supprimer un certificat ou une demande de signature de certificat	14
3.7. Validité d'un certificat	14
3.8. Types de clés	15
4. API de gestion	17
4.1. Rest API	17
4.1.1. API d'administration du serveur de sécurité	17
4.1.2. API du fournisseur d'identité	17
Annexe A: Notes de mise à jour	18

Dernières notes de mise à jour

1.25.0 (11.2025)

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

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

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

1. Introduction

Ce guide s'adresse aux Responsable des clés, qui sont responsables de la clé de signature d'un membre UXP sur le serveur de sécurité.

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

- la gestion des utilisateurs ;
- dispositifs de création de signature ;
- la santé du serveur ;
- les journaux du système.

1.1. Serveur de sécurité UXP

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

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

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

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

1.2. Concepts UXP

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

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

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

Sous-système représente une partie du système d'information d'un membre UXP. Les membres UXP doivent déclarer certaines parties de leurs systèmes d'information comme

sous-systèmes afin d'utiliser ou de fournir des services UXP.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

OCSP signifie Online Certificate Status Protocol (protocole d'état des certificats en ligne). Les répondeurs OCSP sont des serveurs exploités par l'autorité de certification afin de permettre la vérification de la validité des certificats.

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

Une clé UXP est soit :

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

Certificats UXP sont des certificats délivrés par un fournisseur de services de certification

agréé par l'autorité de gouvernance UXP.

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

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

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

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

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

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

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

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

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

- **Identifiant de transaction** est un identifiant de transaction que le serveur de sécurité du client du service attribue lors du traitement d'un message de demande provenant du système d'information. L'identifiant de transaction est généré automatiquement par le serveur de sécurité afin de contenir une valeur unique pour chaque message transmis par le serveur de sécurité.
L'identifiant de transaction est également enregistré dans le journal des messages et peut être utilisé pour identifier de manière unique les messages UXP.

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

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

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

- Pour les services SOAP, voir les en-têtes dans [UXP-PR-MESS].
- Pour les services REST, les en-têtes UXP sont :
 - `Uxp-Client`
 - `Uxp-Service`

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

Instance UXP

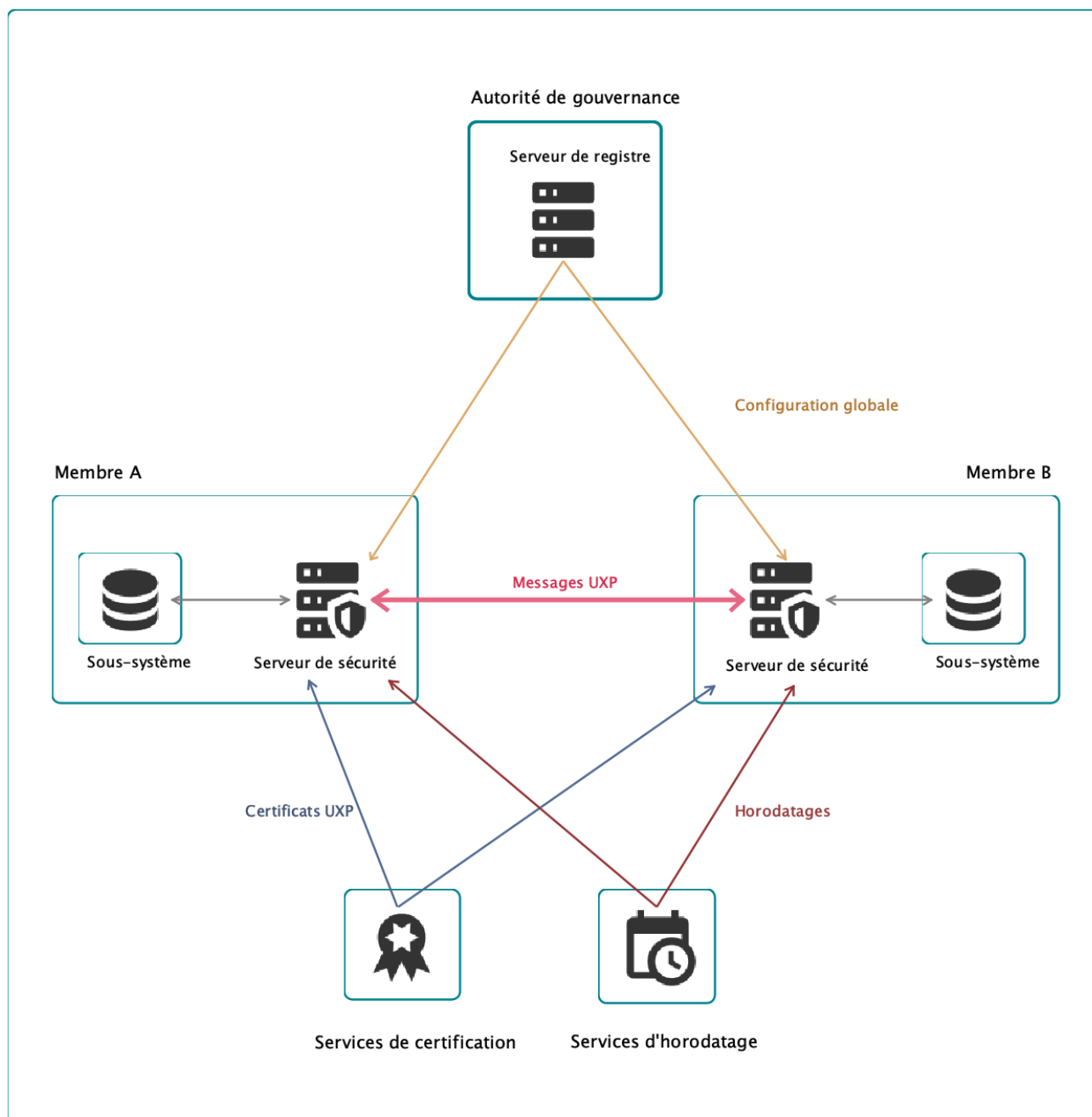


Figure 1. Schéma illustrant les composants d'une instance UXP

1.3. Références

- [\[UXP-PR-MESS\]](#) Cybernetica AS. UXP: Protocole de message v4.0. Identifiant du document : UXP-PR-MESS

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. 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.

3.1. 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) ;
- 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.

3.1.1. 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.

3.1.2. 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.](#)

3.2. 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 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](#).

3.3. 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 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.

3.4. 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 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.

3.5. 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.

3.6. 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.

3.7. 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).

3.8. 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.

4. API de gestion

4.1. Rest API

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

4.1.1. 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
```

4.1.2. API du fournisseur d'identité

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

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

Annexe A: Notes de mise à jour

1.25.0 (11.2025)

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

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

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

1.24.0 (09.2025)

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

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

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

1.22.7 (05.2025)

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

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

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

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

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

1.21.9 (05.2025)

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

1.21.8 (04.2025)

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

1.21.7 (09.2024)

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

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

1.21.6 (08.2024)

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

1.21.5 (07.2024)

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

1.21.4 (05.2024)

- Ajout de la prise en charge de la localisation.

1.21.3 (04.2024)

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

1.21.2 (02.2024)

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

1.21.1 (01.2024)

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

1.21.0 (11.2023)

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

1.20.1 (07.2023)

- Changement de version.

1.20.0 (06.2023)

- 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 multiconnexion.
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.