

Serveur de sécurité UXP 1.25

Guide d'installation et de configuration

UXP-IG-SS

Table des matières

Dernières notes de mise à jour	1
1. Introduction	3
1.1. Public cible	3
1.2. Concepts UXP	3
1.3. Aperçu du processus	7
1.4. Références	8
2. Installation	10
2.1. Configuration requise	10
2.2. Informations requises	12
2.3. Installer les paquets Serveur de sécurité UXP	12
2.4. Vérifications après l'installation	13
3. Configuration du Serveur de sécurité UXP	16
3.1. Informations requises	16
3.2. Connexion au Serveur	16
3.3. Télécharger la licence	16
3.4. Télécharger l'ancre de configuration	17
3.5. Définir le propriétaire du Serveur	17
3.6. Définir le code du Serveur	17
3.7. Initialisation du jeton logiciel	17
3.8. Sélectionner le service d'horodatage	17
3.9. Générer des clés et des CSR	18
3.10. Demande de certificats	18
3.11. Importer des certificats	18
3.12. Serveur de registre	18
4. Configuration du Serveur de sécurité UXP avec un dispositif de création de signature externe	20
4.1. Connecter un dispositif de création de signature	20
4.1.1. Dispositif de création de signature (PKCS#11)	20
Installer le module complémentaire UXP pour les dispositifs de création de signature (PKCS#11)	20
Connecter le dispositif et installer les pilotes	20

Ajouter un dispositif	21
4.2. Importer un certificat de signature à partir d'un dispositif	22
4.3. Générer des clés et des CSR	23
4.4. Demande de certificats	23
4.5. Importer des certificats	23
4.6. Serveur de registre	23
5. Dépannage	25
5.1. Fichiers journaux	25
5.2. Outil de diagnostic	27
5.2.1. Dépannage des journaux dans l'interface utilisateur	27
Visualisation des journaux	28
Filtrer les journaux	29
5.2.2. Exporter des journaux	29
5.2.3. Générer un rapport de diagnostic	29
Générer un rapport à partir de l'interface utilisateur	30
Générer un rapport à partir de l'interface de programmation	30
5.3. Cannot Set LC_ALL to Default Locale.....	31
5.4. PostgreSQL Is Not UTF8 Compatible.....	31
5.5. Could Not Create Default Cluster.....	32
5.6. Is Postgres Running on Port 5432?.....	32
5.7. Impossible de se connecter	33
5.8. Relation "public.databasexchangelock" Does Not Exist.....	34
Annexe A: Notes de mise à jour	35

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 s'adresse aux administrateurs système responsables de l'installation et de la configuration du logiciel Serveur de sécurité UXP.

Le fonctionnement quotidien et la maintenance du serveur de sécurité sont décrits dans le guide d'utilisation [\[UXP-UG-SS\]](#).

Ce document s'adresse à des lecteurs ayant une connaissance moyenne de la gestion des serveurs Linux et des réseaux informatiques.

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.

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.

OCSF signifie Online Certificate Status Protocol (protocole d'état des certificats en ligne). Les répondeurs OCSF 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

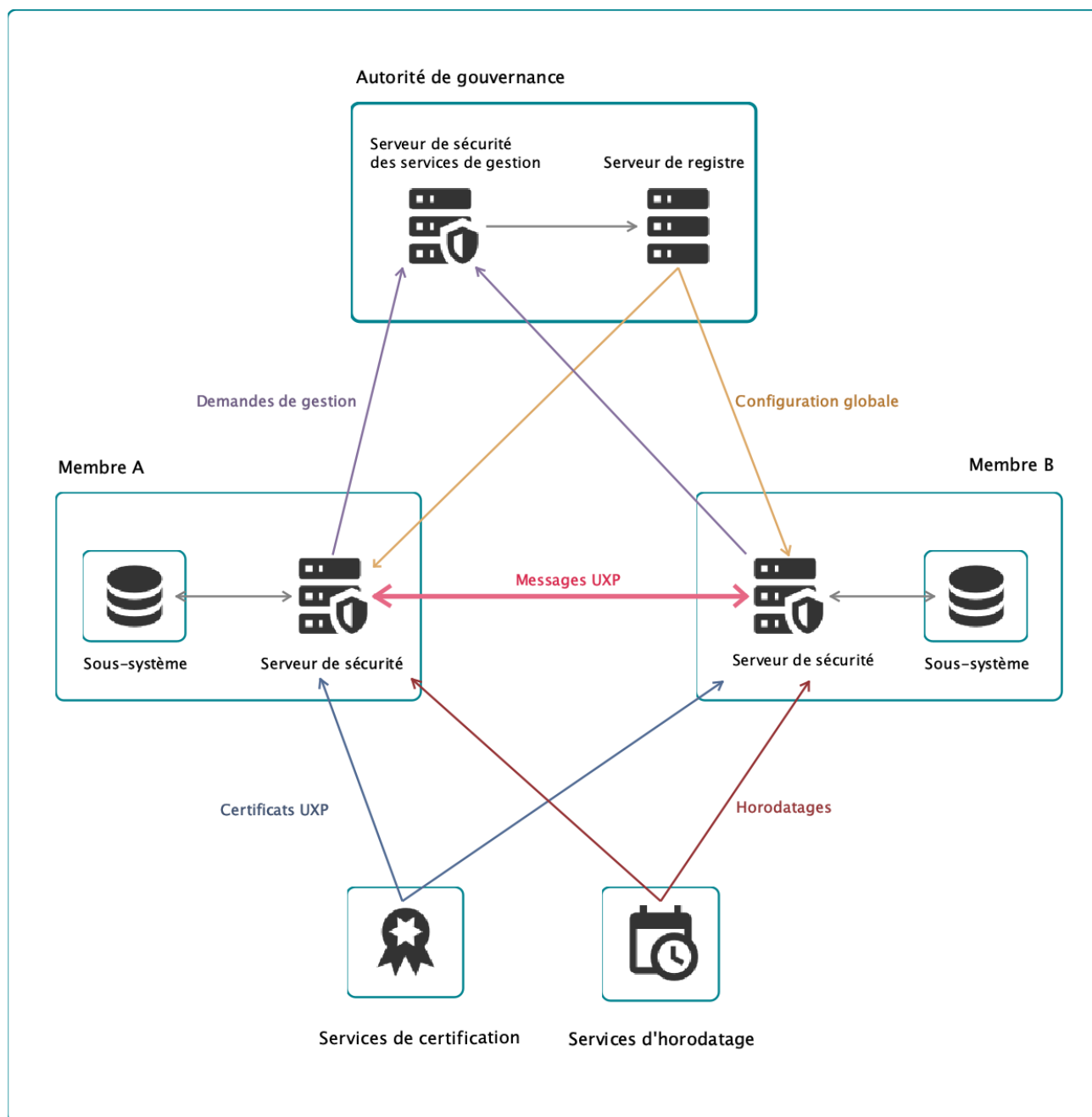


Figure 1. Schéma illustrant les composants d'une instance UXP

1.3. Aperçu du processus

Le diagramme donne un aperçu des étapes à suivre pour configurer un Serveur de sécurité UXP pleinement fonctionnel.

Chaque étape est décrite en détail dans les sections suivantes. Les étapes qui nécessitent une réponse d'une partie externe (par exemple, un fournisseur de services de certification) et peuvent donc inclure une période d'attente sont signalées par 🕒.

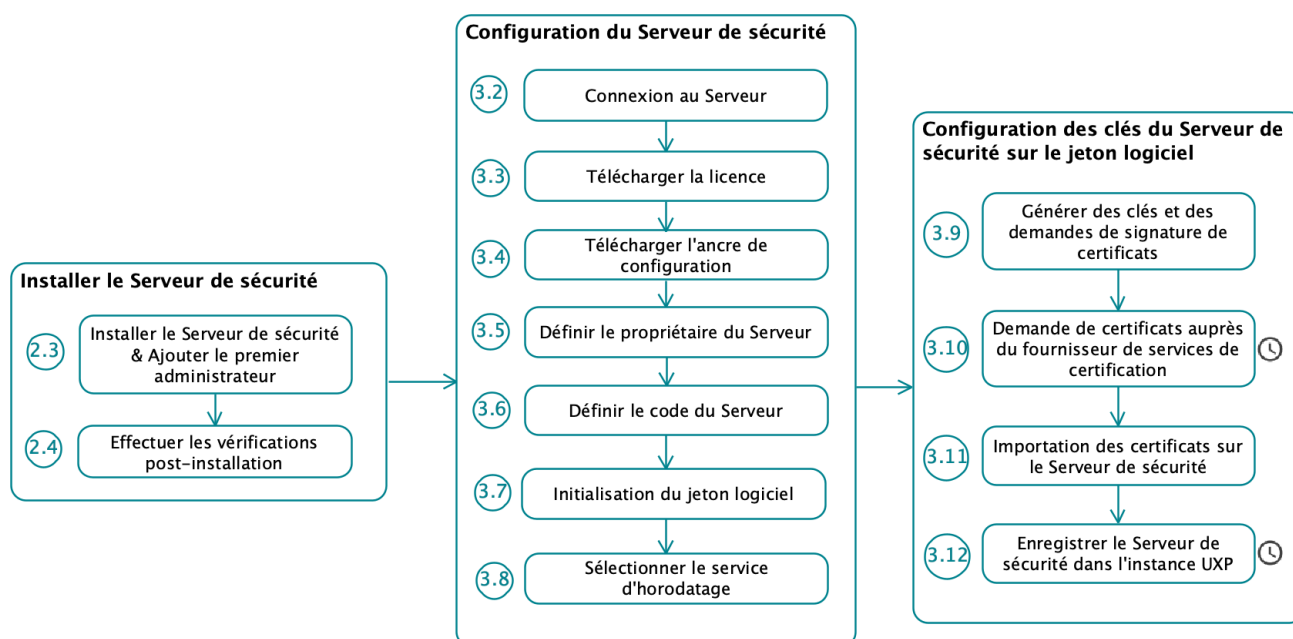


Figure 2. Étapes nécessaires pour configurer un serveur de sécurité avec une clé de signature sur un jeton logiciel

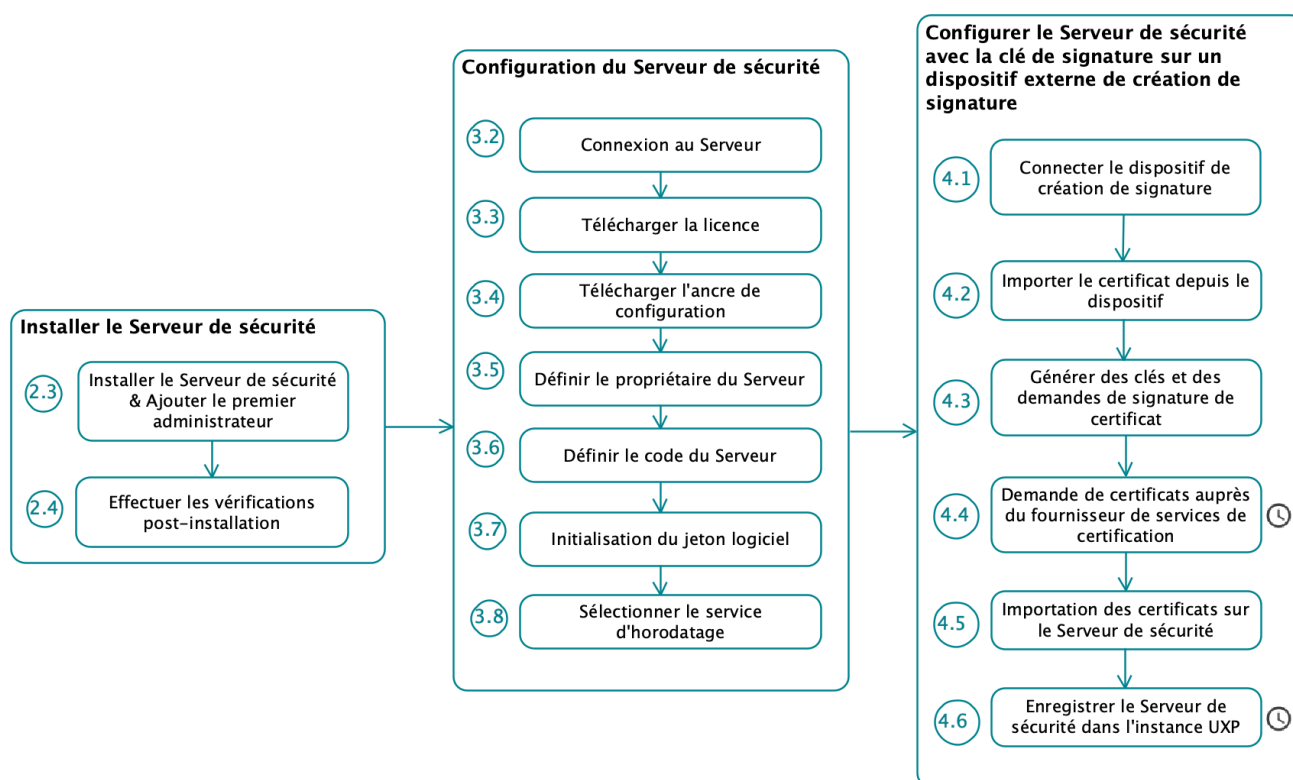


Figure 3. Étapes nécessaires pour configurer un serveur de sécurité avec une clé de signature sur un dispositif externe de création de signature

1.4. Références

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

- [\[UXP-UG-SS\]](#) Cybernetica AS. Serveur de sécurité UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-SS
- [UXP-UG-PMA] Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA
- [UXP-UPG-UB22] Cybernetica AS. Mise à jour des serveurs UXP d'Ubuntu 20.04 à Ubuntu 22.04. Identifiant du document : UXP-UPG-UB22
- [UXP-UPG-UB24] Cybernetica AS. Mise à jour des serveurs UXP d'Ubuntu 22.04 à Ubuntu 24.04. Identifiant du document : UXP-UPG-UB24

2. Installation

2.1. Configuration requise

Plates-formes prises en charge

Le système d'exploitation requis est **Ubuntu Server 24.04 Long-Term Support (LTS)** sur une plate-forme **64 bits**. Ubuntu Server 22.04 LTS est également pris en charge.

Le logiciel du serveur de sécurité peut être installé à la fois sur du matériel physique et virtualisé (pour ce dernier, Xen et Oracle VirtualBox ont été testés).

Paramètres matériels minimaux recommandés

- Le matériel du serveur (carte mère, processeur, cartes réseau, système de stockage) doit être pris en charge par Ubuntu 24.04 (ou Ubuntu 22.04) en général ;
- Intel Xeon E5-2630 v4 64 bits (architecture Broadwell et plus récentes) ou AMD EPYC 7452 (et plus récentes) ;
- 1 CPU, 2 vCPU ;
- 4 Go de RAM ;
- 40 Go d'espace disque 3000 IOPS ;
- Carte d'interface réseau 100 Mbps ;
- si des dispositifs externes de création de signature sont utilisés, les interfaces de connexion des dispositifs.

Paramètres matériels recommandés

- Le matériel du serveur (carte mère, processeur, cartes réseau, système de stockage) doit être pris en charge par Ubuntu 24.04 (ou Ubuntu 22.04) en général ;
- Intel Xeon E5-2630 v4 64 bits (architecture Broadwell et plus récentes) ou AMD EPYC 7452 (et plus récentes) ;
- 4 CPU, 4 vCPU ;
- 16 Go de RAM ;
- 200 Go d'espace disque 3000 IOPS ;
- Carte d'interface réseau 1 Gbps.
- si des dispositifs externes de création de signature sont utilisés, les interfaces de connexion des dispositifs.

Paramètres logiciels requis

- un système d'exploitation Ubuntu 24.04 LTS x86-64 (ou Ubuntu 22.04) installé et configuré ;
- si le serveur de sécurité est séparé d'autres réseaux par un pare-feu et/ou un NAT, les connexions nécessaires vers et depuis le serveur de sécurité doivent être autorisées (voir les ports utilisés dans les tableaux suivants) ;

- si le serveur de sécurité a une adresse IP privée, un enregistrement NAT correspondant doit être créé dans le pare-feu.



L'activation des services supplémentaires nécessaires au fonctionnement et à la gestion du système d'exploitation (tels que DNS, NTP et SSH) n'entre pas dans le cadre de ce guide.

Ports requis pour les connexions entrantes au serveur de sécurité

Port (TCP)	Objectif	Portée du réseau
4000	Accès à l'interface utilisateur en ligne	PRIVÉ
2082	Écoute des requêtes du service d'information sur l'état (nécessaire uniquement en cas d'utilisation d'un équilibreur de charge interne pour répartir les requêtes entre les nœuds de la grappe, voir [UXP-UG-SSHA])	PRIVÉ
80	Connexions HTTP à partir de systèmes d'information	PRIVÉ
443	Connexions HTTPS à partir de systèmes d'information	PRIVÉ
5500	Échange de messages UXP entre les serveurs de sécurité	PUBLIC

Ports requis pour les connexions sortantes du serveur de sécurité

Port (TCP)	Objectif	Portée du réseau
80	Connexions HTTP aux systèmes d'information ; mises à jour de logiciels ; configuration globale ; autres services complémentaires	PUBLIC
443	Connexions HTTPS aux systèmes d'information ; autres services complémentaires	PUBLIC
4400	Demandes de service à un Connecteur UXP (uniquement requis lors de l'utilisation de Connecteur UXP)	PRIVATE
8080	Configuration à distance du serveur Zabbix (nécessaire uniquement lorsque le serveur Zabbix est utilisé pour surveiller localement le serveur de sécurité, voir [UXP-UG-PMA])	PRIVATE
10051	Transmission des données de surveillance au serveur Zabbix (nécessaire uniquement lorsque le serveur Zabbix est utilisé pour surveiller localement le serveur de sécurité, voir [UXP-UG-PMA])	PRIVATE
9200	Transmission des données de surveillance opérationnelle au serveur Elasticsearch (API RESTful) (nécessaire uniquement en cas d'utilisation du serveur Elasticsearch pour surveiller localement le serveur de sécurité, voir [UXP-UG-PMA])	PRIVATE
5500	Échange de messages entre les serveurs de sécurité	PUBLIC
4001	Demandes de gestion adressées à un serveur de registre	PUBLIC

La portée du réseau spécifie si le port doit être visible uniquement au sein du réseau PRIVÉ (par exemple, au sein de votre organisation) ou si les ports doivent être visibles sur le réseau PUBLIC (Internet). Le masquage des ports utilisés uniquement pour les communications au sein du réseau privé de votre organisation réduit le risque d'attaques de sécurité en provenance du réseau public.

2.2. Informations requises

Déterminez les informations suivantes avant l'installation.

Accès au logiciel Serveur de sécurité UXP

- le nom d'utilisateur et le mot de passe du dépôt logiciel UXP.

Informations spécifiques au Serveur que le propriétaire du serveur doit attribuer ou fournir

- le nom d'utilisateur et le mot de passe du premier administrateur du serveur de sécurité, qui disposera de tous les privilèges dans l'interface utilisateur ;
- l'adresse IP privée ou DNS du serveur de sécurité ;

2.3. Installer les paquets Serveur de sécurité UXP

Définir le FQDN comme nom d'hôte

Avant l'installation, veuillez vérifier la configuration du réseau du serveur. Le serveur de sécurité exige que le nom de domaine complet (FQDN), par exemple `server.company.com`, soit configuré comme nom d'hôte.

Listez tous les FQDN :

```
hostname -A
```

Si la sortie de la commande ne renvoie pas le FQDN attendu :

1. Définissez le FQDN comme nom d'hôte, remplacez `<fqdn>` dans la commande et exécutez :

```
sudo hostnamectl set-hostname <fqdn>
```

2. Ajoutez l'IP et le FQDN au fichier `/etc/hosts`, remplacez `<ip-address>` et `<fqdn>` dans la commande et exécutez :

```
echo "<ip-address> <fqdn>" | sudo tee -a /etc/hosts
```

3. Listez tous les FQDN pour confirmer que la modification a bien été appliquée :

```
hostname -A
```

Installation

Pour installer le logiciel Serveur de sécurité UXP sur Ubuntu, suivez les étapes suivantes :

1. Ajoutez la clé de signature du dépôt UXP au dossier `/usr/share/keyrings` :

```
curl https://repo.cyber.ee/uxp/pub.gpg | gpg --dearmor | \
sudo tee /usr/share/keyrings/uxp-pub.gpg >/dev/null
```

2. Ajoutez l'URL du dépôt des paquets UXP et l'emplacement de la clé de signature au fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.25 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Ajoutez les informations d'authentification du dépôt UXP au fichier `/etc/apt/auth.conf.d/uxp.conf` :

```
machine repo.cyber.ee
  login <repo-username>
  password <repo-password>
```

4. Exécutez les commandes suivantes pour installer les paquets Serveur de sécurité UXP :

```
sudo apt update
sudo apt install uxp-securityserver
```

5. Lorsque le système le demande, saisissez le nom d'utilisateur et le mot de passe du premier administrateur du serveur.

Cet utilisateur disposera de tous les privilèges dans l'interface utilisateur du serveur de sécurité et pourra terminer la configuration du serveur. Cet utilisateur peut ajouter des comptes d'utilisateurs supplémentaires.

2.4. Vérifications après l'installation

1. Pour vérifier que les services système UXP fonctionnent, exécutez la commande `sudo uxp-installation-verification` :

```
admin@uxp-security-server:~$ sudo uxp-installation-verification
Checking installed UXP packages...
✓ uxp-addon-diagnostics-tool
✓ uxp-addon-metasevices
✓ uxp-addon-monitor
✓ uxp-confclient
✓ uxp-identity-provider-locales
✓ uxp-identity-provider-rest-api
✓ uxp-identity-provider-ui
✓ uxp-proxy
✓ uxp-securityserver
✓ uxp-securityserver-locale-en
✓ uxp-securityserver-prereqs
```



```
✓ uxp-securityserver-rest-api
✓ uxp-securityserver-ui
✓ uxp-verifier

Checking database services...
✓ postgresql
✓ postgresql@16-main

Checking database connections...
✓ Successfully connected to identity-provider
✓ Successfully connected to serverconf
✓ Successfully connected to messagelog-metadata
✓ Successfully connected to op-monitor

Checking UXP services...
✓ uxp-confclient
✓ uxp-identity-provider-rest-api
✓ uxp-messagelog-archiver
✓ uxp-messagelog-timestamper
✓ uxp-monitor
✓ uxp-ocsp-cache
✓ uxp-proxy (Security server license file is missing; uxp-proxy auto-restarts
continuously)
✓ uxp-securityserver-rest-api
✓ uxp-verifier-rest-api

Checking other services...
✓ nginx
```

✓ All checks passed.

Found the following server administrator accounts **in** UXP User Management (IdP DB):
✓ uxpadmin

To add a new user use the following **command**:

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

UXP Security Server UI should be accessible from one of these addresses:

```
✓ https://192.168.0.2:4000
✓ https://uxp-security-server.cyber.ee:4000
```

If your DNS/IP address of the Security Server UI does not appear on the list, you may have problems with logging **in**. In such **case set** the address with the following **command**:

```
sudo crudini --set /etc/uxp-idp/conf.d/local.ini identity-provider hostname <dns/ip>
```

After changing the parameter, restart the login service with the following **command**:

```
sudo systemctl restart uxp-identity-provider-rest-api
```

2. Assurez-vous que vous pouvez accéder à l'interface utilisateur du serveur de sécurité à l'adresse `https://<security-server>:4000/` à partir d'un navigateur Web. Remplacez `<security-server>` par l'adresse privée du serveur de sécurité.



Lors du démarrage de l'interface utilisateur, le navigateur Web peut afficher l'erreur 502 Bad Gateway.



Lors de la première visite, le navigateur affiche un message indiquant qu'il ne fait pas confiance au certificat auto-signé du serveur de sécurité. Ajoutez une exception confirmant que le certificat est fiable. Le navigateur stocke alors le certificat afin de fournir une connexion sécurisée au serveur.

Le serveur de sécurité a été installé avec succès. Pour poursuivre la configuration du serveur de sécurité dans l'interface Web, consultez les instructions fournies dans les sections suivantes. Voir les instructions dans les sections suivantes.



Si vous ne parvenez pas à vous connecter, veuillez consulter la section de dépannage [Impossible de se connecter](#).

3. Configuration du Serveur de sécurité UXP

3.1. Informations requises

Licence du serveur de sécurité

Le serveur de sécurité une licence valide pour fonctionner.

Adhésion à UXP

Le propriétaire du serveur de sécurité doit être enregistré en tant que membre UXP avant de pouvoir configurer le serveur. Si vous n'avez pas encore de coordonnées de membre UXP, contactez votre autorité de gouvernance pour recevoir les informations suivantes :

- le fichier d'ancrage de la configuration globale ;
- la classe de membre du propriétaire du serveur de sécurité ;
- le code de membre du propriétaire du serveur de sécurité ;

Informations spécifiques au Serveur que le propriétaire du serveur doit attribuer ou fournir

- l'adresse privée du serveur de sécurité ;
- l'adresse publique du serveur de sécurité ;
- le code du serveur de sécurité ;
- le code PIN du jeton logiciel ;
- le service d'horodatage approuvé que le serveur de sécurité utilisera ;
- lequel des services de certification agréés sera utilisé pour demander des certificats.

3.2. Connexion au Serveur

1. Ouvrez l'URL `https://<security-server>:4000/` dans un navigateur Web. Remplacez `<security-server>` par l'adresse privée du serveur de sécurité.



Lors de la première visite, le navigateur affiche un message indiquant qu'il ne fait pas confiance au certificat auto-signé du serveur de sécurité. Ajoutez une exception pour confirmer que le certificat est fiable. Le navigateur stocke alors le certificat afin de fournir une connexion sécurisée au serveur.

2. Connectez-vous en utilisant le **nom d'utilisateur** et le **mot de passe** de l'administrateur ajouté lors de l'installation.

3.3. Télécharger la licence

Téléchargez la **licence** du serveur de sécurité.

Le serveur de sécurité a besoin d'une licence valide pour échanger des messages. La licence peut être assortie d'une date d'expiration et d'une limite au nombre de sous-systèmes individuels connectés au serveur.

3.4. Télécharger l'ancre de configuration

Téléchargez le **fichier d'ancrage de configuration** global.

L'ancre de configuration détermine l'instance UXP dont le serveur fera partie. Le serveur de sécurité utilisera l'ancre de configuration pour télécharger périodiquement des informations sur l'instance UXP, par exemple la liste des autres membres UXP.



Veuillez vérifier la valeur de hachage de l'ancre avec la valeur de hachage publiée par l'autorité de gouvernance.

3.5. Définir le propriétaire du Serveur

Saisissez l'**identifiant UXP de l'organisation propriétaire de ce serveur de sécurité**.

Vous pouvez rechercher l'identifiant du propriétaire dans la liste des membres UXP déjà enregistrés sur l'instance UXP ou saisir l'identifiant et compléter l'enregistrement du membre auprès de l'autorité de gouvernance ultérieurement.



Un code membre est limité au jeu de caractères [a-zA-Z0-9_-].

3.6. Définir le code du Serveur

Attribuez un **code de serveur de sécurité** pour distinguer ce serveur de sécurité des autres serveurs de sécurité de ce propriétaire. Le code du serveur doit être unique pour tous les serveurs de sécurité appartenant au propriétaire.



Un code de serveur de sécurité est limité au jeu de caractères [a-zA-Z0-9_-].

3.7. Initialisation du jeton logiciel

Le serveur de sécurité utilise des clés cryptographiques et les stocke sur un **jeton logiciel**.

Les clés du jeton logiciel sont protégées par un code PIN. Choisissez un code PIN pour le jeton et conservez-le en lieu sûr. Les clés peuvent devenir inutilisables lorsque le code PIN est oublié.

3.8. Sélectionner le service d'horodatage

Sélectionnez un **service d'horodatage** dans la liste des services d'horodatage approuvés par l'Autorité de gouvernance. Si plusieurs services d'horodatage sont nécessaires, vous pouvez

en ajouter d'autres ultérieurement.



L'utilisation d'un service d'horodatage peut nécessiter la conclusion d'un accord de niveau de service avec le fournisseur. Renseignez-vous auprès de votre Autorité de gouvernance pour obtenir plus d'informations sur les procédures requises.

3.9. Générer des clés et des CSR

Le serveur de sécurité dispose de deux certificats importants : le **certificat de signature** et le **certificat d'authentification**.

Tous deux sont nécessaires pour l'échange de messages et l'enregistrement d'un serveur de sécurité auprès de l'autorité de gouvernance.



L'assistant d'initialisation du serveur de sécurité ne permet pas de stocker la clé de signature du propriétaire du serveur sur un dispositif de création de signature (par exemple, un module de sécurité matériel). Si vous devez utiliser un dispositif de création de signature, passez à la section [Configuration du serveur avec un dispositif externe de création de signature](#) pour savoir comment connecter le dispositif au serveur de sécurité, ajouter les clés et les certificats, et terminer l'enregistrement du serveur.

Générez une demande de signature de certificat (CSR) pour le certificat de signature et une autre pour le certificat d'authentification. Les fichiers CSR seront téléchargés automatiquement.

3.10. Demande de certificats

Transmettez les **fichiers CSR** au fournisseur de services de certification que vous avez sélectionné lors de la génération des CSR pour recevoir les certificats. La période d'attente dépend du fournisseur de services de certification et peut varier de quelques minutes à plusieurs mois.

3.11. Importer des certificats

Après avoir reçu les certificats, **importez les deux certificats** sur le serveur de sécurité. Le serveur fera correspondre les certificats avec les clés et les CSR générés précédemment.

3.12. Serveur de registre

La dernière étape consiste à enregistrer le serveur de sécurité et son certificat d'authentification au sein de l'instance UXP.

1. Saisissez le **nom DNS public** ou **l'adresse IP** du serveur de sécurité et envoyez une **demande d'enregistrement** à partir du serveur de sécurité.

2. Pour compléter l'enregistrement vous devez **envoyer le certificat d'authentification** à l'Autorité de gouvernance par d'autres moyens. Suivez les instructions de votre Autorité de gouvernance.

La configuration initiale est terminée et vous serez redirigé vers le panneau de l'administrateur du serveur de sécurité.

L'Autorité de gouvernance doit confirmer l'enregistrement du serveur avant que celui-ci puisse échanger des messages, mais vous pouvez continuer à connecter des services au serveur de sécurité en attendant l'approbation.

Vous pouvez vérifier l'état d'enregistrement du certificat d'authentification sur la page **Clés et certificats**.

4. Configuration du Serveur de sécurité UXP avec un dispositif de création de signature externe

4.1. Connecter 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.

4.1.1. 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



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

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 au 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 **Jetons matériels**.

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.

Pour en savoir plus sur l'utilisation des dispositifs de création de signature, consultez le guide de l'utilisateur du serveur de sécurité [\[UXP-UG-SS\]](#).

Si votre dispositif de création de signature est livré avec une clé et un certificat pré-générés, [importez le certificat](#) du dispositif vers le serveur. Si le dispositif n'a pas de clé de signature, passez à la [génération d'une nouvelle clé de signature](#).

4.2. Importer un certificat de signature à partir d'un dispositif

Si votre dispositif de création de signature est livré avec une clé et un certificat pré-générés :

1. Sur la page **Clés et certificats**, **connectez-vous** au jeton que vous avez choisi sur le périphérique. Le jeton doit être celui qui contient la clé et le certificat.

2. Cliquez sur **Importer un certificat** et choisissez **Importer à partir d'un dispositif**.
3. Trouvez le certificat et **importez-le**.

Lorsque l'importation a réussi, vous pouvez voir le certificat de signature sous le jeton. Le serveur de sécurité peut maintenant utiliser la clé avec ce certificat provenant du dispositif externe.

4.3. Générer des clés et des CSR

Si vous ne disposez pas d'une clé et d'un certificat pré-générés, générez une nouvelle clé de signature sur le jeton à partir du dispositif :

1. Sur la page **Clés et certificats**, **connectez-vous** au jeton que vous avez choisi sur le périphérique.
2. **Générez une clé et une CSR** sur le jeton pour le propriétaire du serveur. Enregistrez le fichier CSR.

Générer la clé d'authentification et la CSR :

1. Sur le jeton logiciel intégré, **générez la clé et la CSR** pour le certificat d'authentification. Enregistrez le fichier CSR.

4.4. Demande de certificats

Selon que vous disposiez déjà d'un certificat de signature ou que vous deviez générer des clés pour la signature et l'authentification, transmettez un ou deux **fichiers CSR** au fournisseur de services de certification que vous avez sélectionné lors de la génération des CSR pour recevoir les certificats.

La période d'attente dépend du fournisseur de services de certification et peut varier de quelques minutes à plusieurs mois.

4.5. Importer des certificats

Après avoir reçu les certificats, allez sur la page **Clés et certificats** et **importez les certificats** sur le serveur de sécurité. Le serveur fera correspondre les certificats avec les clés et les CSR générés précédemment.

Vous devriez maintenant avoir un certificat de signature actif sur le jeton du dispositif de création de signature et un certificat d'authentification enregistré sur le jeton logiciel.

4.6. Serveur de registre

La dernière étape consiste à enregistrer le serveur de sécurité et son certificat d'authentification au sein de l'instance UXP.

1. Sur la page **Clés et certificats**, recherchez le certificat d'authentification importé et cliquez

sur **Enregistrer**.

2. Saisissez le **nom DNS public ou l'adresse IP** du serveur de sécurité et cliquez sur **Enregistrer** pour envoyer une demande d'enregistrement au serveur de sécurité.
3. Pour compléter l'enregistrement vous devez **envoyer le certificat d'authentification** à l'Autorité de gouvernance par d'autres moyens. Suivez les instructions de votre Autorité de gouvernance.

L'Autorité de gouvernance doit confirmer l'enregistrement du serveur avant que celui-ci puisse échanger des messages, mais vous pouvez continuer à connecter des services au serveur de sécurité en attendant l'approbation.

5. Dépannage

5.1. Fichiers journaux

Les fichiers journaux aident à résoudre les erreurs qui surviennent et à détecter d'éventuels comportements inattendus. Le tableau suivant répertorie les fichiers journaux liés à l'UXP dans le serveur de sécurité. La lecture des fichiers journaux nécessite des privilèges root.

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

5.2. 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.

5.2.1. 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
uxp-ocsp-cache	ocsp_cache.log	Échange de messages

Service système UXP	Fichier journal source	Catégorie
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.

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.

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.

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

5.2.3. 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.

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.

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.

5.3. Cannot Set LC_ALL to Default Locale

Si l'exécution de la commande locale donne lieu à un message d'erreur :

```
locale: Cannot set LC_ALL to default locale: No such file or directory,
```

la prise en charge de cette langue particulière n'a pas été installée. Pour l'installer, exécutez la commande (exemple pour le pack de langue anglaise) :

```
sudo apt install language-pack-en
```

Ensuite, pour mettre à jour les fichiers de paramètres linguistiques du système, exécutez les commandes suivantes (exemple pour les paramètres linguistiques des États-Unis) :

```
sudo locale-gen en_US.UTF-8
sudo update-locale en_US.UTF-8
```

Définissez les paramètres régionaux du système d'exploitation. Ajoutez la ligne suivante au fichier `/etc/environment` :

```
LC_ALL=en_US.UTF-8
```

Après avoir mis à jour les paramètres linguistiques du système, il est recommandé de redémarrer le système d'exploitation.

5.4. PostgreSQL Is Not UTF8 Compatible

Si l'installation du serveur de sécurité est interrompue avec le message d'erreur :

```
postgreSQL is not UTF8 compatible,
```

le paquet PostgreSQL est installé avec une locale incorrecte.

Une façon de résoudre ce problème est de supprimer le magasin de données créé lors de l'installation de PostgreSQL et de le recréer avec le bon encodage. Utilisez la commande suivante, en remplaçant `<version>` par le numéro de version de PostgreSQL :



Toutes les données de la base seront effacées !

```
sudo pg_dropcluster --stop <version> main
LC_ALL="en_US.UTF-8" sudo pg_createcluster --start <version> main
```

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

5.5. Could Not Create Default Cluster

Si le message d'erreur suivant s'affiche lors de l'installation de PostgreSQL :

```
Error: The locale requested by the environment is invalid.

Error: could not create default cluster. Please create it manually with pg_createcluster
<version> main -start
```

Utilisez la commande suivante pour créer la grappe de données PostgreSQL, en remplaçant <version> par le numéro de version de votre PostgreSQL :

```
LC_ALL="en_US.UTF-8" sudo pg_createcluster --start <version> main
```

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

5.6. Is Postgres Running on Port 5432?

Si le message d'erreur suivant apparaît pendant l'installation :

```
Is postgres running on port 5432 ?

Aborting installation! please fix issues and rerun with apt -f install
```

vérifiez si l'une des erreurs suivantes s'est produite lors de l'installation de PostgreSQL.

- Erreur de l'installation la grappe de données. Reportez-vous à la section [Impossible de créer la grappe par défaut](#).
- La grappe de données PostgreSQL n'est pas configurée pour écouter sur le port 5432. Pour vérifier et configurer le port d'écoute, éditez le fichier de configuration de PostgreSQL à l'adresse `/etc/postgresql/<version>/main/postgresql.conf` (en remplaçant <version> par votre numéro de version de PostgreSQL). Si vous modifiez le port d'écoute, le service PostgreSQL doit être redémarré.

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

5.7. Impossible de se connecter

Si vous ne parvenez pas à vous connecter et que vous obtenez l'erreur `Authentication failed`. lorsque vous essayez de vous connecter avec les informations d'identification correctes :

Veuillez vérifier le journal du fournisseur d'identité `/var/log/uxp/identity-provider-rest-api.log`.

Si vous voyez une erreur liée à `redirect_uri`, par exemple `OAuth2AuthorizationCodeRequestAuthenticationException : OAuth 2.0 Parameter : redirect_uri` il se peut qu'il y ait des problèmes de configuration du réseau.

Ce problème est dû à une erreur de configuration entre le paramètre `redirect_uri` pour OAuth et l'adresse réelle de l'interface utilisateur du serveur de sécurité.

Pour résoudre le problème d'incompatibilité de configuration :

1. Vérifiez d'abord l'adresse de votre serveur :
 - a. Si vous utilisez une adresse basée sur le DNS/nom d'hôte, veuillez vérifier l'adresse DNS du serveur :

```
hostname -A
```

- b. Si vous utilisez une adresse IP, veuillez vérifier l'adresse IP du serveur :

```
hostname -I
```

2. Si le nom d'hôte et l'adresse IP correspondent à la valeur attendue, vérifiez la valeur du paramètre `redirect_url` du fournisseur d'identité dans la base de données :

```
sudo -u postgres -H -- psql -d identity-provider \
-c "SELECT redirect_uris FROM oauth2_client;"
```

3. Si l'adresse `redirect_uri` dans la base de données ne correspond pas à l'adresse utilisée pour accéder à l'interface utilisateur, il est possible de modifier le fichier de configuration `/etc/uxp-idp/conf.d/local.ini` en ajoutant le nom d'hôte/IP à la section `identity-provider`.

```
[identity-provider]
hostname=<security-server-ui-address>
```

Exemple de configuration:

```
[identity-provider]
hostname=securityserver.cyber.ee
```

4. La modification de la configuration nécessite le redémarrage du fournisseur d'identité :

```
sudo systemctl restart uxp-identity-provider-rest-api
```

5. Essayez de vous connecter à nouveau.

Si cela ne fonctionne pas ou si l'URL de redirection n'est pas liée au nom d'hôte dans votre configuration réseau :

1. Ajoutez des URI de redirection supplémentaires à l'aide du paramètre de configuration `public-client-redirect-uris`. Vous pouvez ajouter plusieurs URI séparés par des virgules.

```
[identity-provider]
public-client-redirect-uris=https://<security-server-ui-address>:4000
```

Exemple de configuration :

```
[identity-provider]
public-client-redirect-uris=https://securityserver.cyber.ee:4000
```

2. La modification de la configuration nécessite le redémarrage du fournisseur d'identité :

```
sudo systemctl restart uxp-identity-provider-rest-api
```

3. Essayez de vous connecter à nouveau.

5.8. Relation "public.databaseloglock" Does Not Exist

Après l'installation du serveur de sécurité, vous pouvez trouver des messages comme celui-ci dans le journal de PostgreSQL :

```
ERROR: relation "public.databaseloglock" does not exist at character 22
```

Ces avertissements font partie de l'installation normale du serveur de sécurité et aucune action n'est requise.

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](#) 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.