

# Serveur de sécurité UXP 1.25

**Guide de mise à jour**

UXP-UPG-SS

# Table des matières

---

<b>1. Introduction</b>	<b>1</b>
1.1. Public cible	1
1.2. Références	1
<b>2. Avant une mise à jour du serveur de sécurité vers une nouvelle version</b>	<b>2</b>
2.1. Faire une sauvegarde	2
2.2. Déterminer la voie de mise à jour	2
<b>3. Mise à jour de la version 1.17 à la version 1.18</b>	<b>4</b>
<b>4. Mise à jour de la version 1.18 à la version 1.19</b>	<b>6</b>
<b>5. Mise à jour de la version 1.19 à la version 1.20</b>	<b>8</b>
<b>6. Mise à jour de la version 1.20 à la version 1.21</b>	<b>10</b>
<b>7. Mise à jour de la version 1.21 à la version 1.24</b>	<b>11</b>
<b>8. Mise à jour de la version 1.24 à la version 1.25</b>	<b>22</b>
<b>9. Mises à jour des correctifs</b>	<b>24</b>
<b>Annexe A: Notes de mise à jour</b>	<b>25</b>

# 1. Introduction

---

## 1.1. Public cible

Ce guide s'adresse aux administrateurs système responsables de la mise à jour 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. Références

- [UXP-UG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-SS
- [UXP-IG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-SS
- [UXP-UPG-UB20] Cybernetica AS. Mise à jour des serveurs UXP d'Ubuntu 18.04 vers Ubuntu 20.04. Identifiant du document : UXP-UPG-UB20
- [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
- [Elastic-Upgrade-7.0] Mise à jour d'Elasticsearch | Guide Elasticsearch [7.0], <https://www.elastic.co/guide/en/elasticsearch/reference/7.0/setup-upgrade.html>
- [Elastic-Upgrade-8.18] Mise à jour d'Elasticsearch | Guide Elasticsearch [8.18], <https://www.elastic.co/guide/en/elasticsearch/reference/8.18/setup-upgrade.html>
- [Zabbix-Upgrade-5.0] Manuel Zabbix, 5 Procédure de mise à jour, <https://www.zabbix.com/documentation/5.0/en/manual/installation/upgrade>
- [Zabbix-Upgrade-6.0] Manuel Zabbix, 6 Procédure de mise à jour, <https://www.zabbix.com/documentation/6.0/en/manual/installation/upgrade>
- [Zabbix-Upgrade-7.0] Manuel Zabbix, 7 Procédure de mise à jour, <https://www.zabbix.com/documentation/7.0/en/manual/installation/upgrade>

## 2. Avant une mise à jour du serveur de sécurité vers une nouvelle version

### 2.1. Faire une sauvegarde



Avant chaque mise à jour, effectuez une sauvegarde du système.

Suivez les instructions du guide de l'utilisateur du serveur de sécurité [\[UXP-UG-SS\]](#) de la version actuellement installée.

Si la mise à jour échoue, procédez à une installation propre de la version précédente en suivant les étapes du guide de mise à jour vers cette version. Restaurez votre serveur à partir du fichier de sauvegarde créé avant la tentative de mise à jour, puis réessayez le processus de mise à jour. Par exemple, si la mise à jour de 1.24 vers 1.25 échoue, réinstallez 1.24 en suivant les instructions de ce guide pour la mise à jour vers 1.24, restaurez à partir de la sauvegarde 1.24, puis tentez à nouveau la mise à jour vers 1.25.

### 2.2. Déterminer la voie de mise à jour

Le serveur de sécurité doit être mis à jour de manière séquentielle. Par exemple, pour passer directement à la version 1.25, la version 1.24 doit être installée. Si les conditions préalables pour la version cible ne sont pas remplies, vous devez procéder à toutes les mises à jour une par une.



Si vous souhaitez uniquement appliquer des corrections de bogues et des mises à jour de sécurité à votre version actuelle, consultez la section concernant [Mises à jour des correctifs](#).

#### 1. Vérifiez la version installée :

```
dpkg -s uxp-securityserver | grep Version
```

#### 2. Vérifiez la dernière version mineure disponible de uxp-securityserver. La commande suppose que le nom d'utilisateur et le mot de passe du dépôt sont déjà configurés dans le fichier /etc/apt/auth.conf.d/uxp.conf, comme décrit dans le guide d'installation :

```
curl -L -u "$(awk '/login/ {l=$2} /password/ {p=$2} END {print l ":" p}' \
/etc/apt/auth.conf.d/uxp.conf)" https://repo.cyber.ee/uxp/latest.json
```



Ce document a été publié avec la version 1.25 du Serveur de sécurité UXP. Si la vérification de la version indique qu'il existe une version mineure plus récente que 1.25, un nouveau guide de mise à jour alors est également disponible. Consultez le guide de mise à jour le plus récent pour suivre la mise à jour vers la dernière version.

3. Vérifiez si une mise à jour séquentielle est autorisée depuis votre version installée vers la dernière version. Consultez les sections de ce guide consacrées à la mise à jour.
  - Si vous avez installé la version requise pour la mise à jour séquentielle, suivez les instructions de la section correspondante de ce guide.
  - Si la version du serveur de sécurité n'est pas celle requise pour la mise à jour séquentielle vers la dernière version, recherchez la mise à jour séquentielle à partir de votre version actuelle et suivez-la étape par étape jusqu'à la version cible. Par exemple, si vous avez la version 1.17 du serveur de sécurité et que vous souhaitez mettre à jour vers la version 1.25, parcourez les sections :
    - [Mise à jour de la version 1.17 à la version 1.18](#)
    - [Mise à jour de la version 1.18 à la version 1.19](#)
    - [Mise à jour de la version 1.19 à la version 1.20](#)
    - [Mise à jour de la version 1.20 à la version 1.21](#)
    - [Mise à jour de la version 1.21 à la version 1.24](#)
    - [Mise à jour de la version 1.24 à la version 1.25](#)
4. Pour en savoir plus sur les changements introduits par chaque nouvelle version dans les notes de mise à jour, consultez [l'Annexe](#).

## 3. Mise à jour de la version 1.17 à la version 1.18

---

### Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour de la version [1.18.0](#) du serveur de sécurité et les éventuels correctifs des versions 1.17 et 1.18, dans l'Annexe.

Faites attention aux changements suivants dans la version 1.18 de Serveur de sécurité UXP et prenez les mesures décrites pour assurer le bon fonctionnement du serveur.

- La prise en charge de la version **6.0** d'Elasticsearch a été supprimée.

Si un Elasticsearch local a été configuré pour ce serveur de sécurité, mettez à jour vers Elasticsearch 7.0 avant de mettre à jour le logiciel du serveur de sécurité.

Suivez les instructions figurant dans [la documentation officielle d'Elasticsearch \[Elastic-Upgrade-7.0\]](#).

### Étapes de la mise à jour

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.18 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Mise à jour du serveur de sécurité :

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

4. Si le processus de mise à jour découvre que le fichier `/etc/uxp/monitor-agent.ini` a été mis à jour depuis l'installation, il vous demandera de choisir entre l'ancien et le nouveau fichier. Choisissez l'ancien fichier (N). Si vous utilisez Elasticsearch en local, consultez les nouvelles options de configuration dans les notes de mise à jour de [1.18.0](#).

5. Vérifiez si la version installée est maintenant 1.18 :

```
dpkg -s uxp-securityserver | grep Version
```

6. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-*
```

7. Supprimez le paquet `uxp-signer` désormais obsolète :

```
sudo apt purge uxp-signer  
sudo systemctl reset-failed uxp-signer.service
```

8. Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.

## 4. Mise à jour de la version 1.18 à la version 1.19

---

### Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour de la version [1.19.0](#) du serveur de sécurité, ainsi que les éventuels correctifs des versions 1.18 et 1.19 figurant dans l'Annexe.

### Mettez à jour Ubuntu vers la version 20.04

La plate-forme minimale supportée pour le serveur de sécurité 1.19 est Ubuntu **20.04** LTS. Si le système d'exploitation de votre serveur de sécurité est toujours Ubuntu 18.04, effectuez la mise à jour vers Ubuntu 20.04 avant celle du logiciel.

Vous pouvez vérifier la version Ubuntu de votre serveur à l'aide de la commande suivante :

```
lsb_release -a
```

Si Ubuntu 20.04 n'est pas installé :

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.18 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Suivez les instructions du guide de mise à jour d'Ubuntu 18 vers Ubuntu 20 pour UXP [\[UXP-UPG-UB20\]](#). Notez que le guide a été mis à jour depuis sa publication initiale en 2021. Veuillez utiliser la version 1.24, publiée en 2025, pour obtenir les instructions les plus précises et les plus récentes.

### Étapes de la mise à jour

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list`:

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.19 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Mise à jour du serveur de sécurité :

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

4. Vérifiez si la version installée est maintenant 1.19 :

```
dpkg -s uxp-securityserver | grep Version
```

5. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-"
```

6. Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.
7. Mettez le serveur à jour vers Ubuntu 22.04, suivez les instructions du guide de mise à jour d'Ubuntu 20 vers Ubuntu 22 pour UXP [\[UXP-UPG-UB22\]](#). Notez que le guide a été mis à jour depuis sa publication initiale en 2022. Veuillez utiliser la version 1.24, publiée en 2025, pour obtenir les instructions les plus précises et les plus récentes.

## 5. Mise à jour de la version 1.19 à la version 1.20

---

### Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour de la version [1.20.0](#) du serveur de sécurité, ainsi que les éventuels correctifs des versions 1.19 et 1.20 figurant dans l'Annexe.

Faites attention aux changements suivants dans la version 1.20 de Serveur de sécurité UXP et prenez les mesures décrites pour assurer le bon fonctionnement du serveur.

- Remplacement du client Java REST de haut niveau d'Elasticsearch, obsolète, par le client Java API dans l'Agent de surveillance de proxy (PMA).

Mettre à jour Elasticsearch au moins vers la version **7.17** pour être compatible avec Java API Client.

- Les modèles Zabbix sont désormais utilisés pour configurer le serveur de sécurité hôte de Zabbix.

La migration vers les modèles supprime l'ancien hôte du serveur de sécurité de Zabbix. Faites une sauvegarde de Zabbix si nécessaire.

- La prise en charge de la version **4.0 LTS** de Zabbix a été supprimée.

Si un Zabbix local a été configuré pour ce serveur de sécurité, effectuez la mise à jour vers Zabbix 5.0 LTS avant de procéder avec celle du logiciel du serveur de sécurité.

Suivez les instructions fournies dans [la documentation officielle de Zabbix \[Zabbix-Upgrade-5.0\]](#).

### Étapes de la mise à jour

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.20 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Mise à jour du serveur de sécurité :

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

4. Si le processus de mise à jour découvre que le fichier `/etc/uxp/monitor-agent.ini` a été mis à jour depuis l'installation, il vous demandera de choisir entre l'ancien et le nouveau fichier. Choisissez l'ancien fichier (N). Si vous utilisez Zabbix local, consultez les nouvelles options de configuration dans les notes de mise à jour de [1.20.0](#).
5. Vérifiez si la version installée est maintenant 1.20 :

```
dpkg -s uxp-securityserver | grep Version
```

6. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-*
```

7. Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.

## 6. Mise à jour de la version 1.20 à la version 1.21

---

### Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour de la version [1.21.0](#) du serveur de sécurité, ainsi que les éventuels correctifs des versions 1.20 et 1.21 figurant dans l'Annexe.

La version 1.21 de Serveur de sécurité UXP ne contient pas de changements radicaux et ne nécessite pas d'étapes de migration supplémentaires.

### Étapes de la mise à jour

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.21 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Mise à jour du serveur de sécurité :

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

4. Vérifiez si la version installée est maintenant 1.21 :

```
dpkg -s uxp-securityserver | grep Version
```

5. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-"
```

6. Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.

# 7. Mise à jour de la version 1.21 à la version 1.24

---

## Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour des versions [1.22.7](#) et [1.24.0](#) du serveur de sécurité, ainsi que toutes les versions de correctifs existantes de la version 1.24 figurant dans l'Annexe.

Alors que les mises à jour de produits UXP impliquent généralement une incrémentation de la version par un, cette version comprend une mise à jour séquentielle de la version 1.21 à la version 1.24. Ce saut de version est intentionnel et attendu car les versions intermédiaires (1.22 et 1.23) n'ont pas été rendues publiques. Vous pouvez en toute sécurité poursuivre la mise à jour de la version 1.21 vers la version 1.24, car ce chemin est entièrement pris en charge.

## Étapes de la mise à jour

### Définir le FQDN comme nom d'hôte

Veuillez vérifier la configuration du réseau du serveur. À partir de la version 1.24, le serveur de sécurité exige, pour fonctionner correctement, que son nom de domaine complet (Fully Qualified Domain Name - FQDN), par exemple `server.company.com`, soit configuré en tant que nom d'hôte et dans le fichier `/etc/hosts`.

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
```

## Mettez à jour Ubuntu vers la version 22.04

La plate-forme minimale supportée pour le serveur de sécurité 1.24 est Ubuntu **22.04** LTS. Si le système d'exploitation de votre serveur de sécurité est toujours Ubuntu 20.04, effectuez la mise à jour vers Ubuntu 22.04 avant de continuer avec celle du logiciel.

Vous pouvez vérifier la version Ubuntu de votre serveur à l'aide de la commande suivante :

```
lsb_release -a
```

Si Ubuntu 22.04 n'est pas installé :

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. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list` :

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.21 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

3. Suivez les instructions du guide de mise à jour d'Ubuntu 20 vers Ubuntu 22 pour UXP [\[UXP-UPG-UB22\]](#).

## Mettre à jour Zabbix vers 6.0



Cette étape ne s'applique que si un Zabbix local a été configuré pour ce serveur de sécurité ; sinon, ignorez cette section.

La prise en charge de la version **5.0** LTS de Zabbix a été supprimée. Si vous l'utilisez encore, mettez Zabbix à jour vers la version 6.0 LTS avant de mettre à jour le logiciel du serveur de sécurité. Après la mise à jour du serveur de sécurité, vous pouvez passer à Zabbix 7.0.

Suivez les instructions fournies dans [la documentation officielle de Zabbix \[Zabbix-Upgrade-6.0\]](#).

## Nouveau système de gestion des utilisateurs UXP 1.24

Jusqu'à la version 1.21, Serveur de sécurité UXP s'appuyait sur la gestion des utilisateurs du système Ubuntu pour gérer les utilisateurs de l'interface utilisateur du serveur de sécurité. La gestion des utilisateurs du système Ubuntu était connectée au serveur de sécurité via le mécanisme PAM (Pluggable Authentication Module).

Depuis la version 1.24, Serveur de sécurité UXP dispose d'une gestion des utilisateurs intégrée qui est le nouveau gestionnaire des utilisateurs par défaut pour les serveurs de

sécurité. La gestion des utilisateurs avec Gestionnaire des utilisateurs UXP est traitée dans le guide de l'utilisateur [UXP-UG-SS].

Le gestionnaire des utilisateurs UXP apporte les avantages suivants par rapport au gestionnaire des utilisateurs Ubuntu.

	Gestion des utilisateurs Ubuntu	Gestionnaire des utilisateurs UXP
<b>Interface de gestion des utilisateurs</b>	Interface de ligne de commande	Interface utilisateur du serveur de sécurité
<b>Rôle de Responsable des clés</b>	Non pris en charge	Pris en charge
<b>Les utilisateurs peuvent modifier leur propre mot de passe</b>	Non	Oui
<b>Flux d'informations d'identification client machine-à-machine OAuth</b>	Non	Oui

Pour les serveurs de sécurité installés avant la version 1.24, il est recommandé de commencer à utiliser le gestionnaire des utilisateurs UXP après la mise à jour vers la version 1.24. Les utilisateurs Ubuntu et l'authentification via l'interface PAM seront pris en charge dans plusieurs versions à venir pour des raisons de compatibilité ascendante, mais cette fonctionnalité sera finalement supprimée lorsque la fonctionnalité du gestionnaire des utilisateurs UXP évoluera.

La migration automatique des utilisateurs du système Ubuntu vers le gestionnaire des utilisateurs UXP n'est pas disponible. Vous devez créer de nouveaux comptes pour tous les utilisateurs.

Vous allez d'abord mettre à jour le serveur de sécurité vers la version 1.24. Lors de la mise à jour, vous créerez un nouveau compte d'administrateur serveur. S'il existe d'autres comptes sur le serveur de sécurité, vous pouvez créer de nouveaux comptes pour les utilisateurs restants en suivant les instructions de ce guide.

## Mise à jour des paquets du serveur de sécurité

1. Remplacez l'URL du dépôt des paquets UXP dans le fichier `/etc/apt/sources.list.d/uxp.list`:

```
echo "deb [signed-by=/usr/share/keyrings/uxp-pub.gpg] \
https://repo.cyber.ee/uxp/securityserver 1.24 main" | \
sudo tee /etc/apt/sources.list.d/uxp.list
```

2. Décidez si vous voulez utiliser immédiatement le gestionnaire des utilisateurs UXP après la mise à jour ou si vous voulez continuer à utiliser l'ancienne gestion au moins temporairement pendant que vous créez de nouveaux comptes d'utilisateur pour ceux-ci. La mise à jour avec la première méthode désactivera la connexion au serveur de sécurité

pour tous les utilisateurs du système Ubuntu.

Si vous avez décidé de ne plus utiliser les anciens comptes d'utilisateur Ubuntu pour vous connecter, mettez à jour le serveur de sécurité à l'aide des commandes suivantes.

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

Si vous souhaitez continuer à utiliser l'ancien gestionnaire des utilisateurs, même temporairement, utilisez les commandes suivantes pour mettre à jour le serveur de sécurité.

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

Cette dernière ajoutera l'intégration PAM qui ne fait plus partie de la nouvelle version par défaut.

3. Lors de la mise à jour, vous êtes invité à créer un nouveau compte d'administrateur serveur.



La réutilisation du nom d'utilisateur d'un utilisateur actuel d'Ubuntu désactivera sa connexion au serveur de sécurité, car ce dernier donne la priorité aux comptes du gestionnaire des utilisateurs UXP.

Saisissez le nom d'utilisateur et le mot de passe pour le nouveau compte de l'Administrateur serveur du gestionnaire des utilisateurs UXP.

## Choisissez la configuration de la surveillance



Cette étape ne s'applique que si `/etc/uxp/monitor-agent.ini` a été modifié depuis l'installation. Le fichier `/etc/uxp/monitor-agent.ini` est lié à Zabbix ou Elasticsearch et Kibana. Si la surveillance locale n'a jamais été configurée pour ce serveur, il est probable que la mise à jour saute cette étape.

Si le processus de mise à jour découvre que le fichier `/etc/uxp/monitor-agent.ini` a été mis à jour depuis l'installation, il vous demandera de choisir entre l'ancien et le nouveau fichier.

Si vous utilisez activement Zabbix ou Elasticsearch, choisissez l'ancien fichier (N). Vous combinerez les deux versions en une seule après la mise à jour.

Si vous ne disposez pas d'une surveillance locale active, vous pouvez également choisir le nouveau fichier (Y) et mettre en place la surveillance locale à l'avenir en vous basant sur le nouveau fichier.

## Vérifications après la mise à jour



1. Vérifiez si la version installée est maintenant 1.24 :

```
dpkg -s uxp-securityserver | grep Version
```

2. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-*
```

## Créer de nouveaux comptes pour les utilisateurs Ubuntu dans Gestionnaire des utilisateurs UXP

1. Connectez-vous à l'interface utilisateur du serveur de sécurité avec le compte de l'administrateur serveur créé lors de la mise à jour.

Si vous ne parvenez pas à vous connecter avec le nouveau compte, examinez les causes possibles suivantes :

- La création du compte a peut-être échoué ou vous avez oublié le mot de passe.  
Suivez les instructions de la section « Ajouter un compte d'administrateur serveur sans accès à l'interface utilisateur » du guide d'utilisation [\[UXP-UG-SS\]](#) et ajoutez un nouveau compte d'administrateur serveur.
- L'étape [Définir le FQDN comme nom d'hôte](#) peut avoir été ignorée ou un nom d'hôte incorrect a été configuré.  
Réappliquez les étapes décrites dans la section [Définir le FQDN comme nom d'hôte](#), puis redémarrez le service du fournisseur d'identité en exécutant `sudo systemctl restart uxp-identity-provider-rest-api.service`.

Essayez de vous connecter à nouveau.

2. Accédez à la page **Comptes d'utilisateurs**. Vous devriez voir apparaître votre compte d'administrateur serveur et vous pouvez continuer à ajouter des comptes supplémentaires pour d'autres utilisateurs.
3. Vérifiez si d'autres utilisateurs du système Ubuntu peuvent accéder à l'interface utilisateur du serveur de sécurité. Pour ce faire, listez les utilisateurs dans les groupes UXP :

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

4. Créez de nouveaux comptes pour les utilisateurs Ubuntu et attribuez un ou plusieurs rôles en conséquence :
  - Si l'utilisateur fait partie du groupe `uxp-server-administrator`, ajoutez le rôle d'Administrateur serveur et le rôle de Responsable des clés.
  - Si l'utilisateur fait partie du groupe `uxp-service-administrator`, ajoutez le rôle de Responsable des services.
  - Si l'utilisateur fait partie du groupe `uxp-transaction-auditor`, ajoutez le rôle d'Auditeur de transactions.

Soyez vigilant lorsque vous utilisez les mêmes noms d'utilisateur pour les nouveaux

comptes. Si vous avez installé le support PAM pour permettre l'accès aux anciens comptes pendant la période de transition, en cas de chevauchement des noms d'utilisateur, le serveur de sécurité donne la priorité au compte dans le gestionnaire des utilisateurs UXP et les comptes utilisateurs Ubuntu portant le même nom cessent de fonctionner.

5. Distribuez les nouveaux identifiants de connexion aux utilisateurs en personne ou par le biais d'un canal de communication crypté. Les utilisateurs seront invités à définir un nouveau mot de passe lors de leur première connexion.
6. Sur la page **Comptes d'utilisateurs**, vous pouvez voir quels sont les utilisateurs qui ont déjà activé leur compte.
7. Une fois que les utilisateurs ont commencé à utiliser leurs nouveaux comptes, il est recommandé, pour des raisons de sécurité et de clarté, de supprimer les anciens comptes d'utilisateur Ubuntu :

```
sudo deluser <username>
```

ou simplement supprimer le privilège d'accès à l'interface utilisateur du serveur de sécurité :

```
sudo deluser <username> <group-name>
```

8. Après avoir créé de nouveaux comptes et supprimé les anciens, vous pouvez supprimer l'intégration PAM :

```
sudo apt remove uxp-addon-identity-provider-pam
```

## Combiner l'ancienne et la nouvelle version du fichier `monitor-agent.ini`

Dans cette mise à jour, le fichier de configuration `/etc/uxp/monitor-agent.ini` a été mis à jour. Bien que la plupart des changements soient automatiques (voir la note à la fin de cette section), certaines opérations manuelles sont nécessaires. Ces étapes supposent que, lors de l'installation, vous avez choisi de conserver votre ancien fichier `/etc/uxp/monitor-agent.ini`.

1. Confirmez que vous avez enregistré l'ancien et le nouveau fichier :

```
sudo ls /etc/uxp/
```

Vous devriez voir l'ancien fichier `monitor-agent.ini` et le nouveau fichier `monitor-agent.ini.dpkg-dist`.

2. Trouvez les paramètres utilisés dans l'ancien fichier en recherchant les lignes contenant des paires de clés et de valeurs qui ne sont pas commentées :

```
sudo grep -v '^#s*;' /etc/uxp/monitor-agent.ini
```

3. Modifiez le nouveau fichier, ajoutez les lignes, les paramètres et les valeurs trouvés dans l'ancien fichier aux bons endroits dans le nouveau fichier :

```
sudo nano /etc/uxp/monitor-agent.ini.dpkg-dist
```

- Si vous utilisiez les anciennes valeurs par défaut de `conf_api_path` et `conf_api_port` (`/zabbix/api_jsonrpc.php` et `80`), veuillez à remettre à jour ces paramètres de configuration dans le nouveau fichier.
  - Si les paramètres de configuration nommés ne sont pas configurés correctement, `/var/log/uxp/proxymonitoragent.log` contiendra une erreur similaire :

```
2025-08-01 18:47:40,947 [pool-3-thread-1] WARN e.c.u.c.m.zabbix.ZabbixClient -
Zabbix (<Zabbix-server-hostname>) failed to process some parameters of request:
EXAMPLE/COM/ACME/SS1, 'processed: 47; failed: 13; total: 60; seconds spent:
0.000510'
```

- N'ajoutez pas le paramètre `send_interval_seconds` au nouveau fichier. La mise à jour a renommé ce paramètre en `elasticsearch-send-interval-seconds` et l'a déplacé vers `/etc/uxp/conf.d/addons/proxy-monitor-agent.ini`

4. Renommez l'ancien fichier pour le sauvegarder :

```
sudo mv /etc/uxp/monitor-agent.ini /etc/uxp/monitor-agent.ini.backup-$(date +%Y%m%d)
```

5. Renommez le nouveau fichier pour l'utiliser :

```
sudo mv /etc/uxp/monitor-agent.ini.dpkg-dist /etc/uxp/monitor-agent.ini
```

6. Rechargez PMA :

```
sudo reload-monitor-agent
```

7. Confirmez que la connexion à Zabbix et Elasticsearch fonctionne toujours :

- Vérifiez dans Zabbix si les données du serveur de sécurité sont mises à jour : Accédez à Monitoring → Hosts et cliquez sur Latest data sur la ligne du serveur de sécurité.
- Vérifiez dans Elasticsearch si les données sont mises à jour.
  - Si les données ne sont pas mises à jour dans Elasticsearch, vérifiez les erreurs commençant par `ERROR e.c.u.p.LocalElasticSender` dans `/var/log/uxp/proxymonitoragent.log`. En cas de problème avec le nom d'hôte et le certificat, voir la section [Confirmer la connexion entre le serveur de sécurité et Elasticsearch](#).



Certains paramètres de configuration dans les champs `[proxy-monitoring-agent]` et `[op-monitor]` de `proxy-monitor-agent.ini` ont été unifiés et renommés automatiquement lors de la mise à jour du paquet, y compris les valeurs ignorées dans `local.ini` :

- [proxy-monitor-agent.ini]
  - port → listen-port,
  - params-collecting-interval-seconds → data-collection-interval-seconds,
  - sending-interval-seconds → zabbix-send-interval-seconds,
- [op-monitor]
  - keep-records-for-days → retain-records-for-days.

En outre, le paramètre `send_interval_seconds`, qui se trouvait auparavant dans la section [elasticsearch] du fichier `monitor-agent.ini`, a été déplacé dans la section [proxy-monitoring-agent] du fichier `proxy-monitor-agent.ini` et renommé `elasticsearch-send-interval-seconds`. L'ancienne valeur de `send_interval_seconds` a été automatiquement déplacée vers `local.ini` sous le paramètre `elasticsearch-send-interval-seconds`.

## Confirmer la connexion entre le serveur de sécurité et Elasticsearch



Cette étape ne s'applique que si un Elasticsearch local a été configuré pour ce serveur de sécurité ; sinon, ignorez cette section.

Assurez-vous que le client HTTP Elasticsearch du serveur de sécurité peut vérifier le nom d'hôte du serveur Elasticsearch ou désactivez la vérification :

- **Contexte :** 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`).
- **Confirmer :** Il y a un problème avec la vérification du nom d'hôte du serveur Elasticsearch, si `/var/log/uxp/proxymonitoragent.log` contient une erreur similaire :

```
2025-06-30 13:20:12,588 [DefaultQuartzScheduler_Worker-4] ERROR
e.c.u.p.LocalElasticSender - Failed to get Elasticsearch version: Host name '<ES-
server-hostname>' does not match the certificate subject provided by the peer
(CN=<hostname-in-cert>)
```

- **Action requise :** Si l'adresse du serveur Elasticsearch configurée dans `/etc/uxp/monitor-agent.ini` ne correspond pas au nom alternatif du sujet (SAN) dans le certificat TLS de l'API HTTP Elasticsearch, vous disposez des options suivantes :
  - Mettre à jour l'adresse du serveur Elasticsearch dans `/etc/uxp/monitor-agent.ini` afin qu'elle corresponde au SAN dans le certificat TLS de l'API HTTP Elasticsearch.
  - Générer à nouveau le certificat API HTTP Elasticsearch avec le SAN correct.
  - Désactiver la vérification du nom d'hôte sur le serveur de sécurité en définissant `verify-hostname=false` dans la section [elasticsearch] du fichier de configuration `/etc/uxp/monitor-agent.ini`.

## Mise à jour des visualisations dans Kibana



Cette étape s'applique uniquement si Elasticsearch et Kibana locaux ont été configurés pour ce serveur de sécurité ; sinon, ignorez cette section.

La mise à jour améliore les données de surveillance opérationnelle en faisant la distinction entre les messages SOAP et REST :

- Introduction d'un nouveau champ, `request_type`, dans le document de données de surveillance opérationnelle pour préciser si une demande est SOAP ou REST.
- Les données de surveillance reflètent désormais directement les caractéristiques du message REST, plutôt que le message SOAP enveloppant le message REST transmis entre les serveurs de sécurité.
  - Le champ `request_soap_size` représente maintenant la taille de la demande SOAP ou de la charge utile de la demande REST en octets.
  - Le champ `response_soap_size` représente maintenant la taille de la réponse SOAP ou de la charge utile de la réponse REST en octets.
  - Les champs `request_attachment_count` et `response_attachment_count` sont désormais définis sur 0 pour les messages REST (auparavant 1 si le message REST avait une charge utile ajoutée en tant que pièce jointe dans le message SOAP enveloppant).
  - Étant donné que la charge utile de la réponse REST n'est pas analysée par le serveur de sécurité, tout code d'état HTTP autre que 2XX est désormais considéré comme un échec, représenté par le champ `succeeded`.

Si nécessaire, mettez à jour vos visualisations de données de surveillance opérationnelle personnalisées dans Kibana.

## Fermer le port 5577

**Contexte :** Le répondeur OCSP du serveur de sécurité ne traite plus les demandes externes des serveurs de sécurité clients. À partir de la version 1.18, le serveur de sécurité a commencé à utiliser le protocole TLS 1.3 OCSP-stapling. Le port OCSP 5577 restait pertinent pour assurer la rétrocompatibilité avec les anciens serveurs de sécurité. Ce port peut être fermé car le répondeur OCSP ne traite plus de demandes externes.

### Action requise :

- Bloquer le trafic entrant sur le port 5577.
- Si vous n'êtes pas sûr que votre serveur recevait des demandes de serveurs de sécurité de la version 1.17 ou inférieure, vous pouvez le vérifier à partir de `proxy.log` en utilisant les mots-clés `Received request from` et `security server version:`. Si vous recevez des demandes provenant de serveurs 1.17 ou inférieurs, demandez instamment aux clients du service de mettre leurs serveurs à jour. Leurs demandes commenceront à échouer après la mise à jour de votre serveur vers la version 1.24.

## Supprimer les paquets redondants

Si Connecteur 1 UXP n'est pas installé sur la même machine que le serveur de sécurité, le paquet `uxp-jetty` peut être supprimé.

1. Pour vérifier si Connecteur 1 UXP est installé, exécutez la commande et recherchez `uxp-connector` :

```
sudo dpkg -l | grep uxp
```

Si la commande **indique** `uxp-connector`, ne supprimez pas `uxp-jetty` et mettez-le à jour avec la dernière version :

```
sudo apt install uxp-jetty
```

2. S'il n'y a pas **Connecteur 1 UXP** sur la même machine, supprimez `uxp-jetty` à l'aide de :

```
sudo apt remove uxp-jetty
```

La prise en charge de la langue portugaise fait désormais partie d'un paquet linguistique unique : `uxp-securityserver-locale-pt`

1. Si la langue portugaise est installée, supprimez l'autre paquet de langues, désormais redondant :

```
sudo apt purge uxp-verifier-locale-pt
```

## Créer une sauvegarde du serveur de sécurité

Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.

## Mettre Ubuntu à jour vers la version 24.04

À moins que vous n'ayez Connecteur 1 UXP installé sur la même machine que le serveur de sécurité, il est recommandé de mettre à jour Ubuntu vers la version\*24.04\* LTS après la mise à jour des paquets du serveur de sécurité. Connecteur 1 ne prend pas encore en charge Ubuntu 24.04. Les machines équipées de Connecteur 1 peuvent être mises à jour vers Ubuntu 24.04 dès lors que Connecteur 1 prend en charge cette version.

Pour vérifier si Connecteur 1 est installé, exécutez la commande et recherchez `uxp-connector` :

```
sudo dpkg -l | grep uxp
```

Suivez les instructions du guide de mise à jour d'Ubuntu 22 vers Ubuntu 24 pour UXP [\[UXP-UPG-UB24\]](#).

## Mettre Zabbix à jour vers 7.0



Cette étape ne s'applique que si un Zabbix local a été configuré pour ce serveur de sécurité ; sinon, ignorez cette section.

La version **6.0** LTS de Zabbix est désormais obsolète, et sa prise en charge sera supprimée dans une prochaine version. Après avoir mis à jour les paquets du serveur de sécurité, il est recommandé de mettre à jour Zabbix vers la version 7.0 LTS.

Suivez les instructions fournies dans [la documentation officielle de Zabbix \[Zabbix-Upgrade-7.0\]](#).

## Mettre Elasticsearch/Kibana à jour vers 8.x



Cette étape ne s'applique que si un Elasticsearch local a été configuré pour ce serveur de sécurité ; sinon, ignorez cette section.

La version **7.x** d'Elasticsearch est désormais obsolète et sa prise en charge sera supprimée dans une prochaine version. Si vous utilisez actuellement la version 7.x, il est recommandé de mettre à niveau Elasticsearch et Kibana vers la version 8.x après avoir mis à niveau les paquets du serveur de sécurité.

Suivez les instructions figurant dans [la documentation officielle d'Elasticsearch \[Elastic-Upgrade-8.18\]](#).

# 8. Mise à jour de la version 1.24 à la version 1.25

## Notes sur la mise à jour

Avant de procéder à la mise à jour, consultez les notes de mise à jour de la version [1.25.0](#) du serveur de sécurité, ainsi que toutes les versions de correctifs existantes des versions 1.24 et 1.25 figurant dans l'Annexe.

Faites attention aux changements suivants dans la version 1.25 de Serveur de sécurité UXP et prenez les mesures décrites pour assurer le bon fonctionnement du serveur.

- La prise en charge de la version **7.x** d'Elasticsearch a été supprimée.

Si une instance Elasticsearch locale qui n'a pas été mise à jour vers la version 8.x est configurée pour ce serveur de sécurité, mettez-la à jour avant de poursuivre la mise à jour du serveur de sécurité.

Suivez les instructions figurant dans [la documentation officielle d'Elasticsearch \[Elastic-Upgrade-8.18\]](#).

- La RAM minimale recommandée passe de 4 à 6 Go.

Si votre serveur de sécurité dispose de moins de 6 Go de RAM, il risque de rencontrer des problèmes de performance. Nous recommandons d'ajouter de la mémoire.



Si vous disposez de moins de 6 Go de RAM, vous serez invité à confirmer la mise à jour.

Si vous annulez la mise à jour (par exemple, pour ajouter de la mémoire avant de poursuivre la mise à jour), le système crée un fichier à l'adresse `/tmp/UXP_ABORT_CONFIGURATION`.

Pour poursuivre la mise à jour ultérieurement (par exemple, après avoir ajouté de la RAM), supprimez ce fichier ou redémarrez le serveur à l'aide de la commande `sudo systemctl reboot`. Recommencez ensuite la mise à jour.

## Étapes de la mise à jour

1. Remplacez l'URL du dépôt des paquets UXP dans le 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
```

2. Mise à jour du serveur de sécurité :



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

3. Si le processus de mise à jour découvre que le fichier `/etc/uxp/monitor-agent.ini` a été mis à jour depuis l'installation, il vous demandera de choisir entre l'ancien et le nouveau fichier. Choisissez l'ancien fichier (N). Si vous utilisez Elasticsearch en local, consultez les nouvelles options de configuration dans les notes de mise à jour de [1.25.0](#).
4. Vérifiez si la version installée est maintenant 1.25 :

```
dpkg -s uxp-securityserver | grep Version
```

5. Vérifiez que les services système UXP sont actifs et en cours d'exécution :

```
systemctl list-units -t service "uxp-*
```

6. Créez une nouvelle sauvegarde du serveur pour vous assurer qu'une sauvegarde valide est disponible pour la nouvelle version. Suivez les instructions du guide de l'utilisateur de la nouvelle version.

## Mise à jour uxp-jetty



Cette étape ne s'applique que si Connecteur 1 UXP est installé sur la même machine que le serveur de sécurité.

Pour vérifier si Connecteur 1 UXP est installé, exécutez la commande et recherchez `uxp-connector` :

```
sudo dpkg -l | grep uxp
```

Si la commande **indique** `uxp-connector`, mettez à jour le paquet `uxp-jetty` avec la dernière version :

```
sudo apt install uxp-jetty
```

## 9. Mises à jour des correctifs

---

Vous pouvez appliquer les petites mises à jour (corrections de bogues, mises à jour de sécurité) qui ont été publiées pour votre version actuelle sans passer par une mise à jour plus importante vers une nouvelle version mineure.

1. Ajoutez la clé de signature du dépôt UXP au dossier `/usr/share/keyrings` (une fois cette opération effectuée, vous pourrez l'ignorer lors des prochaines mises à jour) :

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

2. Vérifiez la version actuellement installée :

```
dpkg -s uxp-securityserver | grep Version
```

3. Assurez-vous que le dépôt UXP pointe vers votre version mineure actuelle de `uxp-securityserver` (par exemple, 1.21), remplacez `<current-version>` et exécutez cette commande pour remplacer le fichier `uxp.list` :

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

4. Vérifiez si des mises à jour mineures sont disponibles pour votre version :

```
sudo apt update
apt policy uxp-securityserver
```

La sortie ressemble à ce qui suit :

```
uxp-securityserver:
  Installed: 1.21.7
  Candidate: 1.21.9
```

5. Si une nouvelle version du correctif est disponible, appliquez les mises à jour :

```
sudo apt upgrade
```

# 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.