

# Serveur de registre UXP 1.25

**Guide d'installation et de configuration**

UXP-IG-RS

# Table des matières

---

<b>Dernières notes de mise à jour</b>	<b>1</b>
<b>1. Introduction</b>	<b>1</b>
1.1. Public cible	1
1.2. Concepts UXP	2
1.3. Aperçu du processus	6
1.4. Références	6
<b>2. Installation</b>	<b>8</b>
2.1. Configuration requise	8
2.2. Informations requises	9
2.3. Ajouter le compte administrateur du serveur de registre	10
2.4. Installer les paquets Serveur de registre UXP	10
2.5. Installer la prise en charge du stockage externe des clés	11
2.6. Vérifications après l'installation	11
<b>3. Configurer le Serveur de registre UXP</b>	<b>13</b>
3.1. Informations requises	13
3.2. Configuration initiale	13
3.3. Générer des clés de signature de configuration internes et externes	14
3.4. Ajouter des classes de membres	15
3.5. Ajouter des services de certification	15
3.6. Ajouter des services d'horodatage	16
<b>4. Configurer le fournisseur de services de gestion</b>	<b>17</b>
4.1. Ajouter un membre UXP	17
4.2. Ajouter un sous-système à un membre	17
4.3. Désigner un fournisseur de services de gestion	17
4.4. Télécharger l'ancre de configuration interne	18
4.5. Configurer les services de gestion du serveur de sécurité	18
4.6. Terminer l'enregistrement du serveur de sécurité des services de gestion	18
4.7. Enregistrer le fournisseur de services de gestion en tant que client du serveur de sécurité	19
4.8. Ajouter le fournisseur de services de gestion en tant que client sur le serveur de sécurité	20

4.9. Configurer les services de gestion à partir du serveur de sécurité des services de gestion .....	21
4.10. Restreindre l'accès au service aux seuls serveurs sélectionnés (facultatif) .....	21
4.11. Configurer le serveur de sécurité des services de gestion situé dans un réseau externe (facultatif) .....	22
4.12. Informations complémentaires.....	24
<b>5. Dépannage.....</b>	<b>25</b>
5.1. Fichiers journaux .....	25
5.2. Cannot Set LC_ALL to Default Locale .....	25
5.3. PostgreSQL Is Not UTF8 Compatible.....	26
5.4. Could Not Create Default Cluster.....	26
5.5. Is Postgres Running On Port 5432?.....	27
5.6. Relation "public.databasechangelock" Does Not Exist.....	27
<b>Annexe A: Installation de la prise en charge des jetons matériels .....</b>	<b>28</b>
<b>Annexe B: Notes de mise à jour.....</b>	<b>31</b>

# Dernières notes de mise à jour

---

## 1.25.0 (11.2025)

- La période de validité par défaut pour la configuration globale a été augmentée de 10 minutes à 72 heures. Cette modification signifie que les serveurs de sécurité peuvent continuer à échanger des messages pendant 72 heures, même si le serveur de registre est hors service ou inaccessible. La configuration globale est toujours mise à jour aux intervalles habituels. Ainsi, en fonctionnement normal, les serveurs de sécurité continueront à recevoir régulièrement la dernière configuration (avec les paramètres par défaut, il faut quelques minutes pour que les modifications parviennent aux serveurs de sécurité).

Pendant la mise à jour, toutes les valeurs de configuration existantes définies sur 10 minutes seront automatiquement mises à jour sur 72 heures. Si une valeur personnalisée (autre que 10 minutes) a été configurée précédemment, elle restera inchangée.

Vous pouvez vérifier la valeur actuelle de `confExpireIntervalSeconds` avant et après la mise à jour en interrogeant la base de données. La procédure à suivre pour vérifier (ou mettre à jour) la valeur est décrite dans la section « Configuration supplémentaire » du guide d'utilisation.

- La fonction d'authentification automatique du jeton logiciel permet désormais de se connecter automatiquement au jeton après le démarrage de Serveur de sécurité UXP et de Serveur de registre UXP, ce qui permet un fonctionnement ininterrompu après les redémarrages. Cette fonction n'est disponible que lorsqu'elle est fournie par le service d'assistance sur demande et installée explicitement, car elle implique des considérations qui doivent être prises en compte au préalable.
- Java Runtime Environment est mis à jour vers la version 21. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Diverses corrections et améliorations mineures ont été apportées.

# 1. Introduction

---

## 1.1. Public cible

Ce guide s'adresse aux administrateurs système chargés d'installer et de configurer le logiciel Serveur de registre UXP.

Le fonctionnement quotidien et la maintenance du serveur de registre sont couverts par le guide de l'utilisateur [\[UXP-UG-RS\]](#).

Ce document s'adresse à des lecteurs ayant une bonne connaissance de la gestion des

serveurs Linux et des réseaux informatiques.

## 1.2. Concepts UXP

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UXP à l'infrastructure UXP.

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

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

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

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

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

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

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

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

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

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

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

**Services d'horodatage** sont des services utilisés pour préserver la valeur probante des messages échangés sur UXP.

**Services de certification** sont des services qui fournissent aux membres UXP les certificats nécessaires pour prouver la propriété d'une clé publique.

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

Un certificat UXP est soit :

- un **certificat de signature** — utilisé par les serveurs de sécurité pour signer numériquement les messages échangés ou
- un **certificat d'authentification** — utilisé par les serveurs de sécurité pour établir des canaux de communication sécurisés.

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

**Messages UXP** sont des demandes et des réponses de service formées conformément au protocole de message UXP. Les messages UXP sont créés par les systèmes d'information des membres UXP.

## Instance UXP

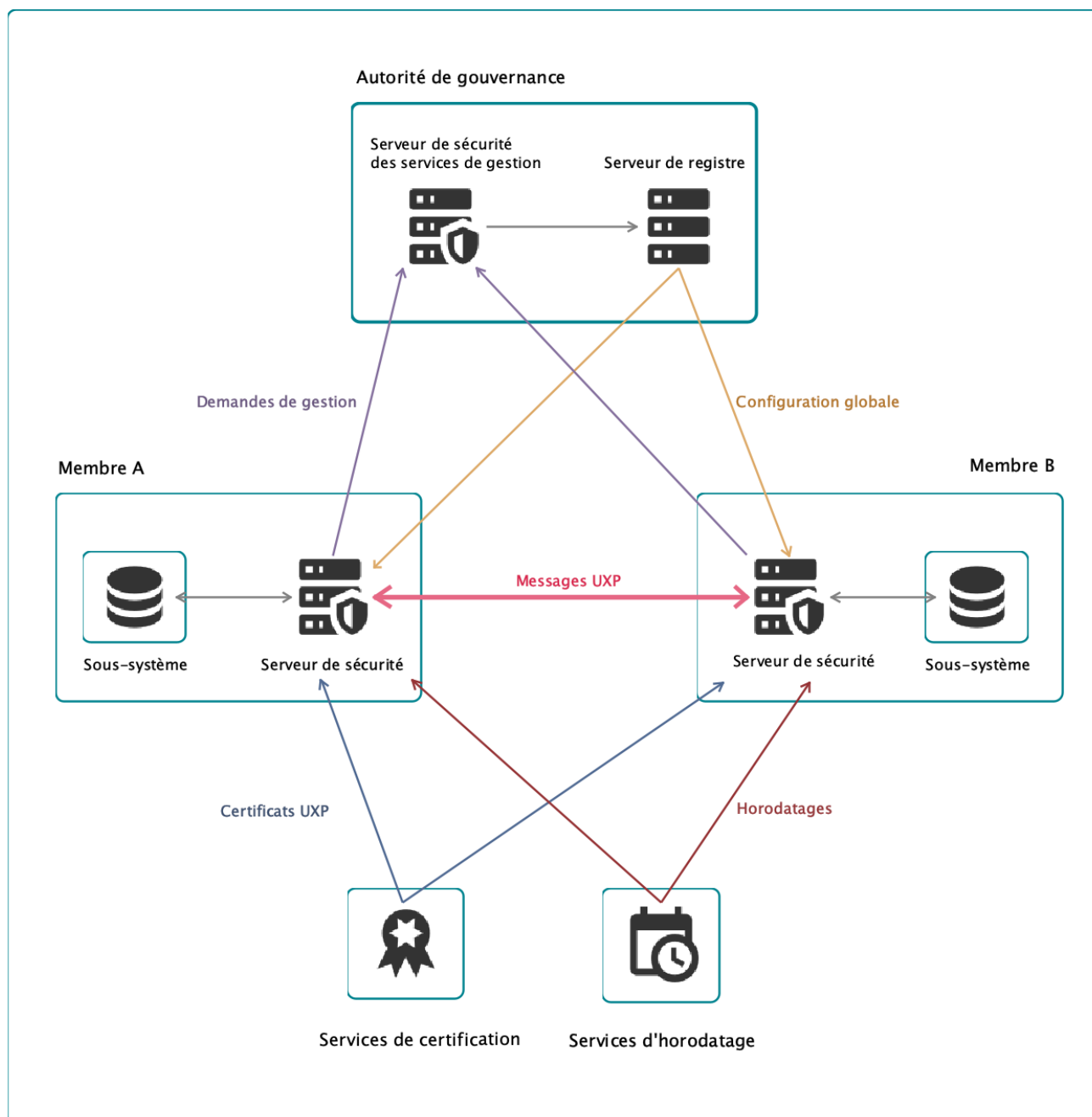


Figure 1. Diagramme montrant les composants d'une instance UXP



## 1.3. Aperçu du processus

La figure 2 ci-dessous donne un aperçu des étapes à suivre pour configurer un serveur de registre UXP pleinement fonctionnel. Chaque étape est décrite en détail dans les sections suivantes. Les étapes qui doivent être effectuées sur un serveur de sécurité gérant les services de gestion sont indiquées par le symbole (SS). Toutes les autres étapes s'appliquent au serveur de registre.

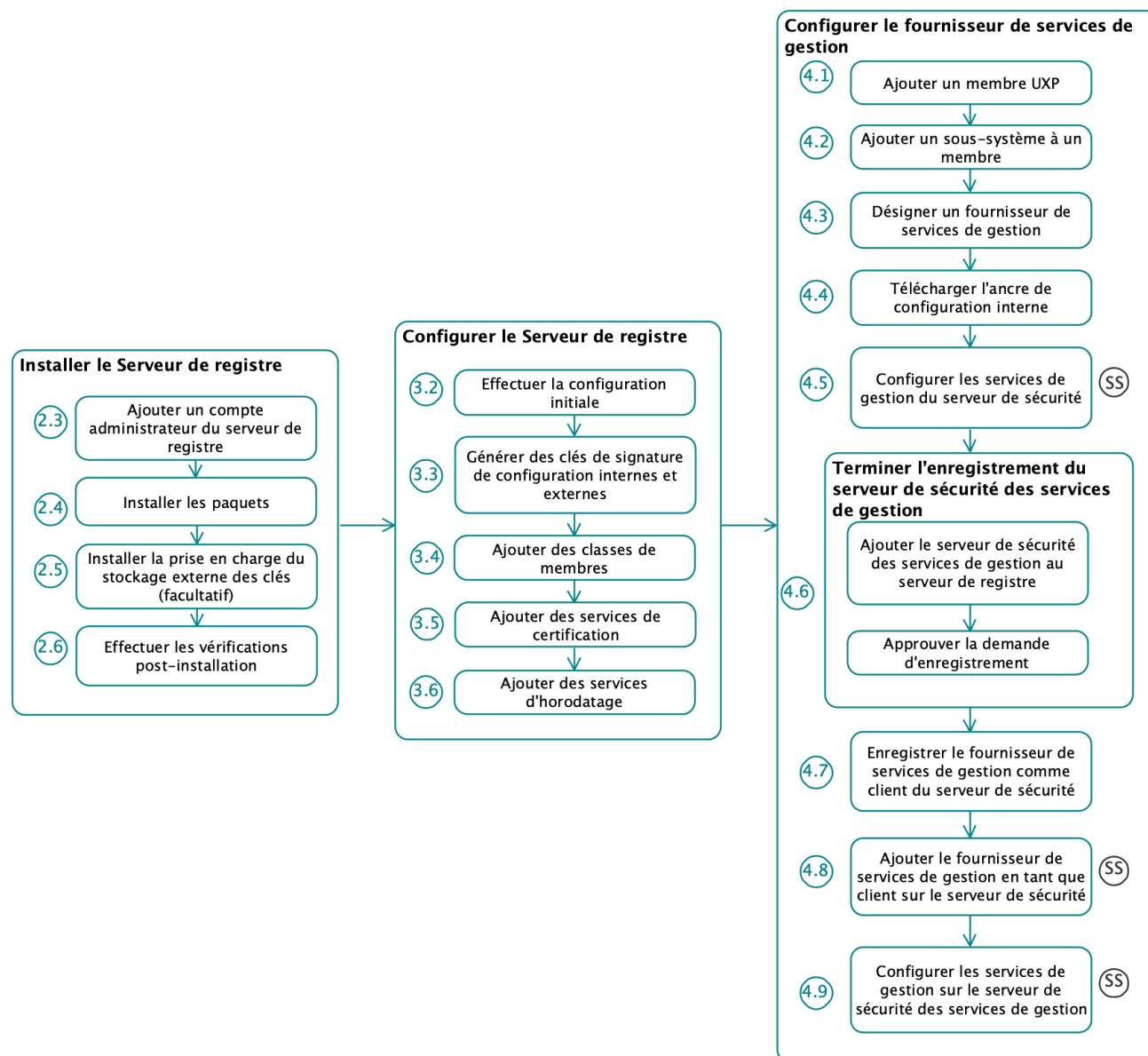


Figure 2. Étapes nécessaires à la mise en place d'un serveur de registre

## 1.4. Références

- [UXP-IG-MS] Cybernetica AS. Serveur de surveillance UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-MS
- [UXP-IG-RSHA] Cybernetica AS. Serveur de registre UXP : Installation et configuration de la haute disponibilité. Identifiant du document : UXP-IG-RSHA

- [\[UXP-UG-RS\]](#) Cybernetica AS. Serveur de registre UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-RS
- [UXP-IG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-SS
- [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

## 2. Installation

---

### 2.1. Configuration requise

#### Plates-formes prises en charge

Le système d'exploitation recommandé est **Ubuntu Server 22.04 Long-Term Support (LTS)** sur une plate-forme **64 bits**.

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



Si le serveur de registre fait partie d'une grappe pour obtenir une haute disponibilité, la grappe de base de données doit être installée et configurée avant d'installer le serveur de registre. Pour plus d'informations, veuillez consulter le Guide d'installation haute disponibilité du serveur de registre [\[UXP-IG-RSHA\]](#).

#### Paramètres matériels minimaux recommandés

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

#### Paramètres matériels recommandés

- Le matériel du serveur (carte mère, processeur, cartes réseau, système de stockage) doit être pris en charge par Ubuntu 22.04 en général ;
- Intel Xeon E5-2630 v4 64 bits (architecture Broadwell et plus récentes) ou AMD EPYC 7452 (et plus récentes) ;
- 1 CPU, 2 vCPU ;
- 8 Go de RAM ;
- 200 Go d'espace disque 3000 IOPS ;
- Carte d'interface réseau 1 Gbps.
- si nécessaire, des interfaces pour les jetons matériels.

#### Paramètres logiciels requis

- un système d'exploitation Ubuntu 22.04 LTS x86-64 installé et configuré ;
- si le serveur de registre est séparé d'autres réseaux par un pare-feu et/ou un NAT, les

connexions nécessaires vers et depuis le serveur de registre doivent être autorisées (voir les ports utilisés dans le tableau suivant) ;

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



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

## Ports requis pour les connexions entrantes au serveur de registre

Port (TCP)	Objectif	Portée du réseau
4000	Accès à l'interface utilisateur basée sur le web	PRIVÉ
4400	Connexions HTTP à partir des serveurs de sécurité des services de gestion	PRIVÉ
5432	Synchronisation avec d'autres nœuds de la grappe du serveur de registre	PRIVÉ
80	Demandes de configuration globale émanant de serveurs de sécurité ; demandes de WSDL des services de gestion émanant des serveurs de sécurité des services de gestion	PUBLIC
4001	Connexions HTTPS des serveurs de sécurité (y compris les serveurs de sécurité des services de gestion) et du serveur de surveillance	PUBLIC

En outre, les connexions sortantes requises pour les services supplémentaires (DNS, NTP, SSH) et les mises à jour logicielles (port 80/TCP) doivent être autorisées.

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

## 2.2. Informations requises

Déterminez les informations suivantes avant l'installation :

### Accès au logiciel Serveur de registre UXP

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

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

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

## 2.3. Ajouter le compte administrateur du serveur de registre

Le compte ajouté à cette étape se verra attribuer les privilèges d'administrateur du serveur de registre pendant l'installation.



Le nom d'utilisateur `uxp` est réservé aux opérations du serveur de registre et ne doit pas être utilisé pour un compte administrateur.

Ajouter un compte utilisateur :

```
sudo adduser <username>
```

L'ajout d'utilisateurs supplémentaires et l'attribution de rôles à ces derniers sont traités dans le Guide de l'utilisateur du Serveur de registre UXP [\[UXP-UG-RS\]](#).

## 2.4. Installer les paquets Serveur de registre UXP

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

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

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

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

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

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

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

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

```
sudo apt update
sudo apt install uxp-registryserver
```

Pendant l'installation, le système demande le nom d'utilisateur du compte qui sera le premier administrateur du serveur de registre (et qui aura tous les privilèges d'utilisateur dans l'interface Web). Saisissez le nom d'utilisateur du compte créé dans la section intitulée [Ajouter le compte administrateur du serveur de registre](#).

## 2.5. Installer la prise en charge du stockage externe des clés

Cette étape est facultative et s'applique **uniquement** lorsqu'un stockage externe pour les clés cryptographiques est nécessaire.

Le serveur de registre prend en charge trois types de stockage pour les clés cryptographiques :

- jeton logiciel — un jeton intégré pour les clés générées dans le serveur de registre ;
- jetons matériels — stockage externe, le support doit être installé séparément.

Voir les instructions sur l'installation de la prise en charge des [jetons matériels](#) dans l'annexe de ce guide.

## 2.6. Vérifications après l'installation

L'installation est réussie si les services système UXP ont démarré et si l'interface utilisateur répond.

1. Utilisez la commande suivante pour vérifier si les services système UXP sont actifs et en cours d'exécution :

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

uxp-jetty.service           loaded active running UXP Registry UI
uxp-registry-monitor.service loaded active running UXP Registry Monitor
uxp-signer.service          loaded active running UXP Message Signer
```

2. Si l'interface Web du serveur de registre a démarré correctement, le fichier `/var/log/uxp/jetty/jetty.log` contient des enregistrements similaires à :

```
[main] INFO o.e.j.s.h.C.registry_ui_xml - STARTUP - Registry Server UI started
successfully
[main] INFO o.e.j.s.h.C.registry_service_xml - STARTUP - Management Services started
successfully
```



Les enregistrements de niveau INFO présentant un modèle similaire `STARTUP - <UXP-service> started successfully` sont communs à tous les services UXP. Vous trouverez plus d'informations sur les fichiers journaux du serveur de registre UXP [log files](#) dans la section [Dépannage](#).

1. Assurez-vous que vous pouvez accéder à l'interface utilisateur du serveur de registre à l'adresse <https://<registry-server>:4000/>. Cela devrait être possible à partir d'un navigateur Web.

Remplacez `<registry-server>` par l'adresse privée du serveur de registre.



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

Bad Gateway.



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

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

## 3. Configurer le Serveur de registre UXP

---

### 3.1. Informations requises

Avant de poursuivre, assurez-vous que vous disposez de toutes les informations nécessaires à la configuration initiale :

#### Licence Serveur de registre

Le serveur de registre nécessite une licence valide pour fonctionner.

#### Informations spécifiques à l'instance UXP

- Identifiant de l'instance UXP ;
- classes de membres qui seront utilisées dans l'instance UXP ;
- un ou plusieurs services de certification, pour chaque service de certification :
  - un certificat de l'autorité de certification (CA) qui fournit le service ;
  - le nom complet de la classe Java qui décrit le profil de certificat (cette classe doit implémenter l'interface `ee.cyber.uxp.common.certificateprofile.CertificateProfileInfoProvider`) ;
  - l'URL du service OCSP de l'autorité de certification (peut être omise si l'autorité de certification ajoute l'URL du service OCSP dans l'extension `Authority Information Access` des certificats émis) ;
  - le certificat du service OCSP (peut être omis si le certificat du service OCSP est le même que le certificat de l'autorité de certification ou s'il est émis par l'autorité de certification) ;
  - les certificats d'une ou plusieurs autorités de certification intermédiaires (s'ils sont requis par le service de certification) ;
- l'URL et le certificat d'un ou plusieurs services d'horodatage.

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

- le nom d'utilisateur et le mot de passe du compte administrateur créé lors de l'installation ;
- l'adresse IP privée ou DNS du serveur de registre ;
- l'adresse IP publique ou DNS du serveur de registre ;
- PIN pour le jeton logiciel qui sera utilisé pour protéger les clés privées.

### 3.2. Configuration initiale

1. Allez à l'URL <https://<registry-server>:4000/> dans un navigateur Web.  
Remplacez `<registry-server>` par l'adresse privée du serveur de registre.





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

2. Connectez-vous à l'aide du nom d'utilisateur et du mot de passe de l'administrateur du serveur de registre.
3. Téléchargez la licence du serveur de registre.
4. Définissez l'identifiant de l'instance UXP.  
Lorsque la licence du serveur de registre est limitée à une seule instance, l'instance est déjà définie.
5. Définissez l'adresse publique du serveur de registre (IP ou DNS).
6. Définissez le code PIN du jeton logiciel.  
Le code PIN sera utilisé pour protéger les clés stockées dans le jeton logiciel. Conservez le code PIN dans un endroit sûr, car il ne sera plus possible d'utiliser ou de récupérer les clés privées contenues dans le jeton si vous perdez ce code.
7. Cliquez sur **Soumettre** pour terminer la configuration initiale.  
Vous serez redirigé vers le panneau d'administration du serveur de registre.

### 3.3. Générer des clés de signature de configuration internes et externes

Cette étape permet de générer deux clés de signature : une pour la configuration interne et une pour la configuration externe. Effectuez les étapes suivantes deux fois, une fois pour chaque type de configuration.

1. Dans le menu **Gestion**, sélectionnez **Configuration globale**, puis sélectionnez l'affichage **Configuration interne** ou **Configuration externe**, selon le cas.
2. Dans la section **Clés de signature**, cliquez sur **Nouvelle clé**.
3. Dans la fenêtre qui s'ouvre, sélectionnez un dispositif clé (jeton de sécurité).
4. Sélectionnez un type de clé approprié. Pour plus d'informations sur les types de clés, veuillez consulter le Guide de l'utilisateur du Serveur de registre UXP [\[UXP-UG-RS\]](#).
5. Insérez une étiquette pour la clé.
6. Cliquez sur **OK**.
7. Si nécessaire, entrez le code PIN du dispositif clé (le code PIN est requis une fois par session de connexion).

Le système génère automatiquement l'ancre de configuration correspondante contenant la partie clé publique de la clé générée.

Si la clé générée est la seule clé de signature pour la source de configuration, la clé sera automatiquement définie comme active (la clé active est affichée en caractères gras).

Répétez les étapes pour la configuration externe.

## 3.4. Ajouter des classes de membres

Pour ajouter des classes de membres :

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Classes de membres** et cliquez sur **Ajouter**.
3. Saisissez le code et la description de la classe de membres. Cliquez sur **OK**.



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

Ajoutez autant de classes de membres que nécessaire pour l'instance.

## 3.5. Ajouter des services de certification

Pour chaque service de certification, vous aurez besoin :

- du certificat de l'autorité de certification (CA) ;
  - du nom complet de la classe Java qui décrit le profil de certificat de ce service de certification ;
  - de l'URL et du certificat du service OCSP (s'il n'a pas été rendu disponible par l'extension Authority Information Access des certificats) ;
  - les certificats des autorités de certification intermédiaires (si requis par le service de certification).
1. Dans le menu **Configuration**, sélectionnez **Services de certification** et cliquez sur **Ajouter**.
  2. Localisez le certificat CA du service de certification et cliquez sur **Suivant**.
  3. Si le service de certification ne délivre que des certificats d'authentification, cochez la case **Cette autorité de certification ne peut être utilisée que pour l'authentification TLS**. Toutefois, si le service de certification émet d'autres certificats en plus des certificats d'authentification, laissez la case vide.
  4. Saisissez le nom complet de la classe Java qui décrit le profil de certificat.  
Le profil de certificat par défaut est

```
ee.cyber.uxp.common.certificateprofile.impl.UxpCertificateProfileInfoProvider
```

**AVERTISSEMENT :** La version 1.10 ou inférieure du serveur de sécurité n'est pas compatible avec ce profil de certificat. Tant qu'il y a d'anciens serveurs de sécurité dans le système, utilisez l'ancien profil de certificat par défaut `ee.ria.xroad.common.certificateprofile.impl.UxpCertificateProfileInfoProvider` à la place pour assurer la compatibilité ascendante.

5. Si le certificat de l'autorité de certification ne contient pas d'informations sur le service OCSP, ajoutez l'URL et, si nécessaire, le certificat du service OCSP dans l'onglet **Répondeurs OCSP**.

6. Si le service de certification utilise des autorités de certification intermédiaires, saisissez leurs certificats dans l'onglet **Autorités de certification intermédiaires**.  
Pour ajouter des services OCSP pour les autorités de certification intermédiaires, ajoutez leurs informations dans l'onglet **Répondeurs OCSP** de la fenêtre **Détails CA intermédiaires**.

### 3.6. Ajouter des services d'horodatage

1. Dans le menu **Configuration**, sélectionnez **Services d'horodatage** et cliquez sur **Ajouter**.
2. Entrez l'URL et le certificat du service d'horodatage.
3. Vérifiez que vous avez chargé le bon certificat à l'aide de **Afficher le certificat** et cliquez sur **OK**.

## 4. Configurer le fournisseur de services de gestion

---

Dans la dernière étape, vous devez configurer et enregistrer un serveur de sécurité dédié qui fournira des services de gestion aux autres serveurs de sécurité. Ce serveur de sécurité est appelé serveur de sécurité des services de gestion.

Les tâches décrites dans cette section doivent être effectuées sur deux composants UXP : le serveur de registre et le serveur de sécurité des services de gestion. Chaque section suivante est accompagnée d'une note précisant le composant sur lequel elle doit être effectuée.

Pour effectuer toutes les étapes liées au serveur de registre avec un seul compte administrateur, le compte doit avoir les rôles de responsable de la sécurité et de Responsable d'enregistrement (voir la section « Gestion des utilisateurs » dans [\[UXP-UG-RS\]](#)). Il est recommandé d'utiliser le compte créé lors de l'installation ou d'ajouter un nouveau compte administrateur avec au moins ces deux rôles.

### 4.1. Ajouter un membre UXP

**Composant :** Serveur de registre

Ajoutez le membre UXP qui sera responsable des services de gestion :

1. Dans le menu **Configuration**, sélectionnez **Membres** et cliquez sur **Ajouter**.
2. Saisissez les informations relatives au membre et cliquez sur **OK**.



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

### 4.2. Ajouter un sous-système à un membre

**Composant :** Serveur de registre

Ajoutez un sous-système au membre ajouté à l'étape précédente :

1. Localisez le membre ajouté à l'étape précédente et cliquez sur **Détails**.
2. Dans la fenêtre qui s'ouvre, localisez la section **Sous-systèmes** et cliquez sur **Ajouter**.
3. Saisissez le code du sous-système et cliquez sur **OK**.



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

### 4.3. Désigner un fournisseur de services de gestion

**Composant :** Serveur de registre

Désignez un sous-système comme fournisseur de services de gestion :

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Services de gestion** et cliquez sur **Modifier**.
3. Recherchez le sous-système que vous avez créé à l'étape précédente et cliquez sur **Sélectionner**.

## 4.4. Télécharger l'ancre de configuration interne

**Composant :** Serveur de registre

1. Vérifiez que la génération de la configuration globale est réussie (aucun message d'erreur global ne doit s'afficher dans l'interface utilisateur à ce stade).  
L'ancre est nécessaire pour configurer le serveur de sécurité des services de gestion.
2. Dans le menu **Gestion**, sélectionnez **Configuration globale** et choisissez la vue **Configuration interne**.
3. Dans la section **Ancre**, cliquez sur **Télécharger** et enregistrez le fichier.

## 4.5. Configurer les services de gestion du serveur de sécurité

Installez, configurez et enregistrez un serveur de sécurité conformément au Guide d'installation et de configuration du Serveur de sécurité UXP [UXP-IG-SS].

Lors de la configuration initiale du serveur de sécurité, le système demandera :

- le fichier d'ancrage de configuration global – téléchargez l'ancrage de configuration interne téléchargé à l'étape précédente ([Télécharger l'ancrage de configuration interne](#)) ;
- la classe et le code de membre du propriétaire du serveur de sécurité – saisissez la classe et le code de membre du membre ajouté dans la section intitulée [Ajouter un membre UXP](#).

Terminez la configuration et l'enregistrement du serveur de sécurité. La dernière étape consiste à envoyer une demande d'enregistrement de certificat d'authentification (voir [UXP-IG-SS] Section « Configurer le serveur de sécurité UXP ») et revenez à ce guide.

## 4.6. Terminer l'enregistrement du serveur de sécurité des services de gestion

**Composant :** Serveur de registre



Cette étape nécessite qu'une demande d'enregistrement de certificat d'authentification ait été envoyée par le serveur de sécurité des services de gestion au serveur de registre.

Vous aurez besoin :

- du code du serveur de sécurité des services de gestion ;
- du certificat d'authentification pour le serveur de sécurité des services de gestion.

Pour terminer l'enregistrement du serveur de sécurité des services de gestion, il faut soumettre une demande complémentaire et approuver les demandes depuis le serveur de registre :

1. Dans le menu **Configuration**, sélectionnez **Membres**, puis le membre que vous avez créé pour les services de gestion et cliquez sur **Détails**.
2. Sélectionnez la section **Serveurs détenus** et cliquez sur **Ajouter**.
3. Saisissez le code du serveur de sécurité des services de gestion.



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

4. **Téléchargez** le certificat d'authentification pour le serveur de sécurité des services de gestion.
5. **Soumettez** la demande d'enregistrement.

Si la demande est soumise avec succès, un enregistrement correspondant apparaît dans la vue détaillée du membre dans la section **Demandes de gestion** (type de demande « Enregistrement du certificat d'authentification »). Elle apparaîtra également dans la liste des demandes de gestion (dans le menu principal, sélectionnez **Gestion** puis **Demandes de gestion**).

La requête côté serveur de registre est dans l'état « **En attente** » si la demande soumise via le serveur de sécurité des services de gestion n'est pas arrivée au serveur de registre au moment où la demande côté serveur de registre a été soumise. Si la demande est arrivée, les deux demandes sont dans l'état « **Soumise pour approbation** ».

6. Approuvez les demandes complémentaires sur le serveur de registre – ouvrez l'une des vues détaillées de l'une des demandes complémentaires et cliquez sur **Approuver**.

Lorsque la demande est approuvée :

- les demandes complémentaires passent à l'état « **Approuvée** » ;
- le serveur de sécurité enregistré apparaît à la fois dans la section **Serveurs détenus** de la vue détaillée de son propriétaire et dans la liste des serveurs de sécurité (dans le menu principal, sélectionnez **Configuration**, puis **Serveurs de sécurité**) ;
- le propriétaire du serveur de sécurité est ajouté au groupe global `security-server-owners`.

## 4.7. Enregistrer le fournisseur de services de gestion en tant que client du serveur de sécurité

## Composant : Serveur de registre

Pour enregistrer le fournisseur de services de gestion en tant que client du serveur de sécurité des services de gestion :



Le fournisseur de services de gestion ne peut être enregistré en tant que client d'un serveur de sécurité, comme décrit dans cette section, uniquement s'il n'est enregistré en tant que client d'aucun autre serveur de sécurité. Si le fournisseur de services de gestion est déjà client d'un serveur de sécurité, l'identifiant du serveur de sécurité s'affiche à la place du bouton **Enregistrer**.

1. Dans le menu **Gestion**, sélectionnez **Paramètres système**.
2. Localisez la section **Services de gestion** et cliquez sur **Modifier**.
3. Localisez la section **Informations sur le serveur de sécurité** dans le formulaire de demande d'enregistrement, cliquez sur **Rechercher** et sélectionnez le serveur de sécurité qui sera utilisé comme serveur de sécurité des services de gestion.
4. **Soumettez** la demande d'enregistrement.

Si l'enregistrement a réussi, l'identifiant du serveur de sécurité des services de gestion s'affiche à la place du bouton **Enregistrer**.

## 4.8. Ajouter le fournisseur de services de gestion en tant que client sur le serveur de sécurité

### Composant : Serveur de sécurité

Pour ajouter le fournisseur de services de gestion en tant que client au serveur de sécurité des services de gestion :

1. Dans le menu **Services** du serveur de sécurité, sélectionnez **Clients du serveur de sécurité**.
2. Cliquez sur **Ajouter un client**. Dans la fenêtre qui s'ouvre, vous pouvez soit saisir manuellement les informations relatives au client, soit cliquer sur **Sélectionner le client dans la liste globale** et localiser les informations relatives au client dans la liste de tous les membres UXP et de leurs sous-systèmes.



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

3. Cliquez sur **Ajouter** une fois que les informations relatives au client ont été saisies.

Le client doit apparaître dans l'état « **Enregistré** », car l'association entre le client et le serveur de sécurité a déjà été enregistrée dans le serveur de registre à l'étape précédente.

## 4.9. Configurer les services de gestion à partir du serveur de sécurité des services de gestion

**Composant :** Serveur de sécurité

Vous aurez besoin :

- de l'URL du fichier WSDL des services de gestion (<http://<registry-server>/managementservices.wsdl>) ;
- de l'URL des services de gestion (<http://<registry-server>:4400/management-service/>).

Remplacez <registry-server> par l'adresse du serveur ou affichez les URL requises dans **Gestion** → **Paramètres système** → **Services de gestion** à partir de l'interface Web du serveur de registre.

Configurez les services de gestion :

1. Dans le menu **Services** du serveur de sécurité, sélectionnez **Clients du serveur de sécurité**, sélectionnez le client qui fournira les services de gestion, puis cliquez sur l'icône **Services SOAP** de cette ligne.
2. Cliquez sur **Ajouter WSDL**, entrez l'URL du WSDL des services de gestion et cliquez sur **Ajouter**.
3. Activez le WSDL du service de gestion en cliquant sur **Activer**.
4. Choisissez l'un des services et cliquez sur **Modifier**.
5. Remplacez l'URL du service par l'URL des services de gestion (<http://<registry-server>:4400/management-service/>). Cochez la case **Appliquer tout** pour l'URL et cliquez sur **Enregistrer**. Assurez-vous que les URL de tous les services de gestion ont bien été modifiées.

Ajoutez des droits d'accès à tous les propriétaires de serveurs de sécurité :

1. Choisissez l'un des services de gestion et cliquez sur **Droits d'accès**.
2. Recherchez la section **Droits d'accès** et cliquez sur **Ajouter un accès**.
3. Recherchez le groupe global **security-server-owners**. Sélectionnez le groupe et cliquez sur **Ajouter la sélection**.
4. Répétez l'opération pour tous les autres services de gestion.

L'installation et la configuration d'un serveur de sécurité des services de gestion sont terminées.

## 4.10. Restreindre l'accès au service aux seuls serveurs sélectionnés (facultatif)

Les droits d'accès aux services publics fournis par le serveur de registre peuvent être restreints en fonction de l'adresse IP. Par défaut, ces services sont publics et leur accès n'est



pas limité :

- Service de téléchargement de la configuration globale (<http://<registry-server>/internalconf> et <http://<registry-server>/externalconf>).
- Service d'enregistrement des certificats d'authentification (<http://<registry-server>:4001/management/service/certreg>).

Pour accorder des droits d'accès à des hôtes spécifiques (tels que des serveurs de sécurité), ajoutez l'adresse IP de l'hôte correspondant au fichier de configuration de Nginx `/etc/uxp/nginx/service-access-list` et refusez l'accès à tous les autres hôtes en remplaçant `<allowed-host-IP-address>` par l'adresse IP publique de l'hôte auquel l'accès doit être accordé :

```
allow <allowed-host-IP-address>;
deny all;
```

Ajoutez autant de lignes de directives `allow` que nécessaire, en les terminant par un point-virgule. Veillez à mettre à jour cette liste lorsque de nouveaux hôtes nécessitant l'accès à ces services sont connus, tels que de nouveaux serveurs de sécurité sur le point d'être enregistrés, et à supprimer les lignes correspondant aux hôtes qui n'ont plus besoin d'accès. Notez également que l'ajout de la dernière directive `deny all;` est nécessaire pour garantir que toutes les autres connexions à ces services seront interdites.



L'accès aux services de téléchargement de la configuration globale est nécessaire pour les Serveurs de surveillance UXP. L'accès à ces services comprendra également les hôtes énumérés dans `/etc/uxp/nginx/monitoring-access-list`, voir [UXP-IG-MS] pour plus de détails.



Après avoir apporté des modifications à la configuration, vous devez recharger la configuration nginx :

```
sudo systemctl reload nginx
```

## 4.11. Configurer le serveur de sécurité des services de gestion situé dans un réseau externe (facultatif)

Par défaut, on suppose que le serveur de sécurité des services de gestion qui transmet les demandes de gestion au serveur de registre est situé dans un réseau privé avec le serveur de registre. Cela signifie que seules les demandes de gestion provenant d'un réseau privé sont autorisées par défaut.

Effectuez les étapes suivantes uniquement si le serveur de sécurité des services de gestion **n'est pas** dans le même réseau privé que le serveur de registre.

Si le serveur de sécurité des services de gestion est situé dans un réseau externe (par exemple, un service en nuage), vous devez modifier la configuration nginx du registre afin d'autoriser les connexions à partir de l'adresse IP du serveur de sécurité des services de

gestion.

Le fichier de configuration pour les connexions HTTPS est `/etc/uxp/nginx/uxp-registry.conf`. Pour les connexions HTTP, il existe un fichier de configuration distinct `/etc/uxp/nginx/insecure-uxp-registry.conf`, mais les connexions HTTP à partir d'un réseau public ne sont pas conseillées.

### Autoriser les connexions à partir de l'adresse du serveur de sécurité des services de gestion externes

Ajoutez la ligne suivante au bloc `location /` du fichier de configuration des connexions HTTPS (`/etc/uxp/nginx/uxp-registry.conf`), en remplaçant `<mgmnt-services-ss-IP-address>` par l'adresse IP publique du serveur de sécurité des services de gestion :

```
allow <mgmnt-services-ss-IP-address>/32;
```

AVERTISSEMENT : Conservez le `deny all;` pour interdire les autres connexions.



Vous pouvez également activer les connexions HTTP à partir d'un serveur externe en procédant de la même manière pour le fichier de configuration de la connexion HTTP, mais cela est fortement déconseillé.

### Activer l'authentification TLS du serveur de sécurité des services de gestion sur le serveur de registre



Si vous ne souhaitez pas que le serveur de registre authentifie le serveur de sécurité des services de gestion dans les connexions HTTPS, ignorez cette étape.

1. Dans le menu **Gestion** du serveur de sécurité, sélectionnez **Clés et certificats**, recherchez le bloc **Certificat TLS interne** et cliquez sur **Exporter le certificat** pour télécharger le certificat TLS interne du serveur de sécurité.
2. Copiez le certificat téléchargé dans le dossier `/etc/uxp/ssl/trusted/` du serveur de registre.
3. Ajoutez les deux lignes suivantes au bloc `server` du fichier de configuration de la connexion HTTPS, en remplaçant `<certificate-name>` par le nom du fichier que vous avez copié à l'étape précédente :

```
ssl_verify_client optional_no_ca;
ssl_client_certificate /etc/uxp/ssl/trusted/<certificate-name>;
```

Ajoutez les lignes suivantes au bloc `location /` :

```
if ($ssl_client_verify != SUCCESS) {
    return 403;
}
```

4. Redémarrez nginx pour appliquer les changements :

```
sudo systemctl restart nginx
```

## Activer l'authentification TLS du serveur de sécurité des services de gestion sur le serveur de registre



Si vous ne souhaitez pas que le serveur de sécurité des services de gestion authentifie le serveur de registre dans les connexions HTTPS, ignorez cette étape.

1. Téléchargez le certificat TLS interne du serveur de registre situé dans le fichier `/etc/uxp/ssl/internal.crt`.
2. Dans le menu **Services** du serveur de sécurité, sélectionnez **Clients du serveur de sécurité**. Sélectionnez le client qui fournira les services de gestion et cliquez sur l'icône **Systèmes d'information** sur cette ligne.
3. Recherchez le bloc **Certificats TLS internes des systèmes d'information**, cliquez sur **Ajouter** et téléchargez le certificat TLS du serveur de registre.
4. Cliquez sur l'onglet **Services SOAP** et cliquez sur l'icône > pour développer le WSDL des services de gestion. Sélectionnez un service et cliquez sur **Modifier**.
5. Assurez-vous que l'URL du service commence par `https://` et que le port est 4001. Cochez la case **Appliquer à tout dans WSDL** et cliquez sur **Enregistrer**. Assurez-vous que les paramètres de tous les services de gestion ont été modifiés.

## 4.12. Informations complémentaires

Après avoir suivi avec succès ce guide, le serveur de registre est prêt à être utilisé pour exécuter une instance UXP.

Pour plus de détails sur la gestion des membres UXP dans le serveur de registre et sur la manière d'optimiser le serveur, consultez le Guide de l'utilisateur du Serveur de registre UXP [\[UXP-UG-RS\]](#) (également disponible dans l'interface Web du serveur de registre).

# 5. Dépannage

## 5.1. Fichiers journaux

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

Emplacement du journal	Description
/var/log/uxp/audit.log	Enregistrement des actions réussies et échouées des utilisateurs dans l'interface utilisateur du serveur de registre
/var/log/uxp/signer.log	Enregistrements des activités liées à la gestion des clés et certificats UXP (erreurs de signature)
/var/log/uxp/cluster_<datetime>.log	Enregistrements créés pendant le processus d'initialisation de la haute disponibilité du serveur de registre ; uniquement lorsque la haute disponibilité du registre est configurée.
/var/log/uxp/configuration_client.log	Enregistrements des activités liées au téléchargement de la configuration globale des instances UXP fédérées ; uniquement lorsque la fédération est configurée.
/var/log/uxp/registry-monitor.log	Enregistrements des événements système liés au processus de surveillance du registre
/var/log/uxp/jetty/	Enregistrements des requêtes adressées au serveur d'applications fournissant l'interface utilisateur, les services de gestion et la génération de configurations globales
/var/log/postgresql/postgresql-<version>-main.log	Enregistrement des erreurs d'accès à la base de données

## 5.2. Cannot Set LC\_ALL to Default Locale

Si l'exécution de la commande locale génère le message d'erreur suivant :

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

le support pour la langue en question n'a pas été installé. Pour l'installer, exécutez la commande (exemple pour le pack de langue anglaise) :

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

Ensuite, pour mettre à jour les fichiers de paramètres linguistiques du système, exécutez les

commandes suivantes (exemple pour les paramètres linguistiques des États-Unis) :

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

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

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

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

### 5.3. PostgreSQL Is Not UTF8 Compatible

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

```
postgreSQL is not UTF8 compatible
```

alors le paquet PostgreSQL est installé avec une locale incorrecte.

Une solution consiste à supprimer le magasin de données créé lors de l'installation de PostgreSQL et à le recréer avec le codage correct. Utilisez la commande suivante, en remplaçant `<version>` par le numéro de version de PostgreSQL :



Toutes les données de la base seront effacées !

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

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

### 5.4. Could Not Create Default Cluster

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

```
Error: The locale requested by the environment is invalid.
Error: could not create default cluster. Please create it manually with pg_createcluster
<version> main -start
```

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

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

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

## 5.5. Is Postgres Running On Port 5432?

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

```
Is postgres running on port 5432 ?  
  
Aborting installation! Fix the issues and rerun installation with 'apt -f install'
```

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

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

Pour terminer l'installation interrompue, exécutez la commande :

```
sudo apt -f install
```

## 5.6. Relation "public.databasechangelock" Does Not Exist

Après avoir installé le serveur de registre, vous pourriez trouver des messages comme celui-ci dans le journal de PostgreSQL :

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

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

# Annexe A: Installation de la prise en charge des jetons matériels

Pour configurer la prise en charge des jetons de sécurité matériels (carte à puce, jeton USB, module de sécurité matériel), procédez comme suit.

1. Installez le module de prise en charge des jetons matériels à l'aide de la commande suivante :

```
sudo apt install uxp-addon-hwtokens
```

2. Installez et configurez un pilote PKCS#11 pour le jeton matériel conformément aux instructions du fabricant.
3. Ajoutez le chemin d'accès au pilote PKCS#11 au fichier `/etc/uxp/devices.ini` (comme indiqué dans l'exemple donné dans le fichier).
4. Après avoir installé et configuré le pilote, redémarrez le service `uxp-signer` :

```
sudo systemctl restart uxp-signer
```

Si vous utilisez une configuration matérielle de jetons à haute disponibilité (HA) (telle qu'une grappe avec des jetons répliqués), vous devrez peut-être limiter le format de l'identifiant du jeton de manière que les répliques du jeton puissent être considérées comme le même jeton. Le format de l'identifiant du jeton peut être modifié dans `/etc/uxp/devices.ini` via la propriété `token_id_format` (valeur par défaut : `{moduleType}{slotIndex}{serialNumber}{label}`). La suppression de certaines parties de l'identifiant permettra à la configuration HA de fonctionner correctement lorsque l'un des jetons tombe en panne et est remplacé par une réplique. Par exemple, si les répliques de jetons sont signalées comme étant sur des emplacements différents, la partie `{slotIndex}` doit être supprimée du format de l'identifiant.

Selon le matériel utilisé, il peut être nécessaire de procéder à une configuration supplémentaire. Tous les paramètres configurables possibles dans `/etc/uxp/devices.ini` sont décrits dans le tableau suivant.

Paramètres	Type	Valeur par défaut	Explication
enabled	BOOLEAN	true	Indique si ce dispositif est activé.
library	STRING		Le chemin d'accès à la bibliothèque PKCS#11 pour le pilote de périphérique.

Paramètres	Type	Valeur par défaut	Explication
library_cant_create_os_threads	BOOLEAN	false	True si les threads d'application qui exécutent des appels à la bibliothèque PKCS#11 ne peuvent pas utiliser les appels natifs du système d'exploitation pour créer de nouveaux threads (en d'autres termes, le code de la bibliothèque ne peut pas créer ses propres threads) ; false s'ils le peuvent.
os_locking_ok	BOOLEAN	false	True si la bibliothèque PKCS#11 peut utiliser le modèle de threading du système d'exploitation natif pour le verrouillage ; false dans le cas contraire.
find_certificates	BOOLEAN	true	Indique s'il faut rechercher les certificats de signature qui ne figurent pas dans le fichier de configuration des clés (/etc/uxp/signer/keyconf.xml) à partir du périphérique.
sign_verify_pin	BOOLEAN	false	Indique si le code PIN doit être saisi pour chaque opération de signature.
token_id_format	STRING	{moduleType}{slotIndex}{serialNumber}{label}	Spécifie le format de l'identifiant utilisé pour identifier de manière unique un jeton. Dans certaines configurations à haute disponibilité, il peut être nécessaire de limiter la prise en charge des jetons répliqués (par exemple en supprimant l'index des emplacements, qui peut être différent pour les jetons répliqués).
sign_mechanism	STRING	CKM_RSA_PKCS	Spécifie le mécanisme de signature. Valeurs prises en charge : CKM_RSA_PKCS, CKM_RSA_PKCS_PSS.
pub_key_attribute_encrypt	BOOLEAN	true	Indique si la clé publique peut être utilisée pour le cryptage.
pub_key_attribute_verify	BOOLEAN	true	Indique si la clé publique peut être utilisée pour la vérification.
pub_key_attribute_wrap	BOOLEAN		Indique si la clé publique peut être utilisée pour envelopper d'autres clés.



Paramètres	Type	Valeur par défaut	Explication
pub_key_attribute_allowed_mechanisms	STRING LIST		Spécifie les mécanismes de clé publique autorisés. Valeurs prises en charge : CKM_RSA_PKCS, CKM_SHA256_RSA_PKCS, CKM_SHA384_RSA_PKCS, CKM_SHA512_RSA_PKCS, et CKM_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS, CKM_SHA512_RSA_PKCS_PSS.
priv_key_attribute_sensitive	BOOLEAN	true	Indique si la clé privée est sensible.
priv_key_attribute_decrypt	BOOLEAN	true	Indique si la clé privée peut être utilisée pour le cryptage.
priv_key_attribute_sign	BOOLEAN	true	Indique si la clé privée peut être utilisée pour la signature.
priv_key_attribute_unwrap	BOOLEAN		Indique si la clé privée peut être utilisée pour déballer les clés enveloppées.
priv_key_attribute_allowed_mechanisms	STRING LIST		Spécifie les mécanismes autorisés pour les clés privées. Valeurs prises en charge : CKM_RSA_PKCS, CKM_SHA256_RSA_PKCS, CKM_SHA384_RSA_PKCS, CKM_SHA512_RSA_PKCS, et CKM_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS, CKM_SHA512_RSA_PKCS_PSS.



Seul le paramètre `library` est obligatoire, tous les autres sont facultatifs.

Le séparateur d'éléments de type `STRING LIST` est `,` (virgule).

# Annexe B: Notes de mise à jour

---

## 1.25.0 (11.2025)

- La période de validité par défaut pour la configuration globale a été augmentée de 10 minutes à 72 heures. Cette modification signifie que les serveurs de sécurité peuvent continuer à échanger des messages pendant 72 heures, même si le serveur de registre est hors service ou inaccessible. La configuration globale est toujours mise à jour aux intervalles habituels. Ainsi, en fonctionnement normal, les serveurs de sécurité continueront à recevoir régulièrement la dernière configuration (avec les paramètres par défaut, il faut quelques minutes pour que les modifications parviennent aux serveurs de sécurité).

Pendant la mise à jour, toutes les valeurs de configuration existantes définies sur 10 minutes seront automatiquement mises à jour sur 72 heures. Si une valeur personnalisée (autre que 10 minutes) a été configurée précédemment, elle restera inchangée.

Vous pouvez vérifier la valeur actuelle de `confExpireIntervalSeconds` avant et après la mise à jour en interrogeant la base de données. La procédure à suivre pour vérifier (ou mettre à jour) la valeur est décrite dans la section « Configuration supplémentaire » du guide d'utilisation.

- 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)

- Ubuntu 22.04 LTS est la plate-forme minimale prise en charge. Si la version Ubuntu du serveur n'est pas encore 22.04, mettez à jour Ubuntu comme décrit dans le guide de mise à jour (UXP-UPG-UB22) avant de mettre à jour la version UXP.
- Mise à jour des bibliothèques et des composants tiers pour garantir la sécurité du système.
- Diverses corrections et améliorations mineures ont été apportées.

## 1.22.6 (03.2025)

- Le journal d'audit inclut désormais l'adresse IP de la source de la demande.
- Ajout d'une option permettant de limiter l'accès au service de configuration globale et d'enregistrement des certificats d'authentification à certaines adresses IP spécifiques

uniquement. Consultez la section « Restreindre l'accès au service aux serveurs sélectionnés uniquement » dans le guide d'installation.

- Les services de certification et d'horodatage peuvent désormais être bloqués temporairement sans être supprimés du serveur de registre.
- Le serveur de registre bloque désormais temporairement les utilisateurs après un trop grand nombre de tentatives de connexion infructueuses afin d'empêcher les attaques par force brute.
  - Vous pouvez configurer le nombre de tentatives autorisées et le temps de verrouillage. Consultez la section « Verrouillage automatique après plusieurs tentatives d'authentification infructueuses » dans le guide d'utilisation.
- Ajout d'une section « Dépannage » au guide de l'utilisateur.
- Ajout d'un nouveau paramètre système `auth0cspFreshnessSeconds` qui permet de configurer le temps de rafraîchissement des réponses OCSP des certificats d'authentification séparément des certificats de signature.
- Ajout d'un nouveau paramètre système, `rsa-allowed`, qui peut être utilisé pour interdire l'utilisation de clés RSA sur le serveur de registre.
- Les journaux d'audit du serveur de registre 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.

### 1.21.7 (09.2024)

- Changement de version.

### 1.21.6 (08.2024)

- Changement de version.

### 1.21.5 (07.2024)

- Changement de version.

### 1.21.2 (02.2024)

- Corrections de traduction pour la langue *pt-BR*.

### 1.21.1 (01.2024)

- Résolution d'un problème avec la dépendance manquante de la bibliothèque `logback-classic`, qui provoquait des avertissements de journalisation.

### 1.21.0 (11.2023)

- 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)**

- Correction du script de restauration de la sauvegarde du registre qui ne réinitialisait pas correctement les séquences d'identification de la base de données dans certaines conditions.

### **1.20.0 (06.2023)**

- Migration de la base de données du serveur de registre d'Active Record vers Liquibase.
- Démarrage de l'utilisation du mot de passe généré pour la base de données du serveur de registre.
- 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)**

- Changement de version.

### **1.19.1 (11.2022)**

- Changement de version.

### **1.19.0 (11.2022)**

- 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)**

- Changement de version.

### **1.18.3 (10.2022)**

- Changement de version.

### **1.18.2 (09.2022)**

- Changement de version.

### **1.18.1 (09.2022)**

- Correction d'une dépendance manquante de l'utilitaire signer-console.

### 1.18.0 (06.2022)

- 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)

- Changement de version.

### 1.17.1 (12.2021)

- Changement de version.

### 1.17.0 (10.2021)

- 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)

- Le serveur de registre attribue désormais des noms uniques aux services d'horodatage en ajoutant un numéro si nécessaire.
  - Une fois la version 1.16 mise à jour, le serveur de sécurité et le serveur de registre attribueront des noms uniques aux services d'horodatage existants.
- Quelques corrections mineures.

### 1.15.2 (07.2021)

- Tous les journaux sont désormais affichés par défaut dans le fuseau horaire local.
- Autres corrections mineures.

### 1.15.1 (06.2021)

- Autres corrections mineures.

### 1.15.0 (04.2021)

- Nouvelle solution de surveillance du serveur de registre utilisant Serveur de surveillance et Zabbix.
  - Les paramètres spécifiques au système d'exploitation et à UXP peuvent être contrôlés.
  - Le serveur de surveillance peut automatiquement configurer Zabbix avec des serveurs de registre en tant qu'hôtes et leur associer les modèles appropriés.
  - Des informations spécifiques à UXP peuvent également être demandées par le biais d'une solution de suivi personnalisée. Voir la section « Surveillance » d'UXP-UG-RS.
- 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)

- Amélioration du nettoyage de la configuration globale expirée sur le serveur de registre.

### 1.14.0 (12.2020)

- Le serveur de registre dispose désormais d'un nouveau groupe global pour tous les sous-systèmes trouvés dans la configuration globale. Ce sous-système peut être utilisé pour mettre des services à la disposition de tous les membres de l'instance.
- Le serveur de registre est désormais incompatible avec les versions 1.x du Serveur de surveillance UXP.
- Le serveur de registre est désormais incompatible avec Répertoire UXP version 2.2 et suivantes. Avant de mettre à jour le serveur de registre, 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-RS 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 prise en charge.
- L'ancien document de statistiques sur les demandes (l'ancien format pour les statistiques UXP) n'est plus pris en charge dans le suivi local.
- Ubuntu 18.04 est désormais la plus ancienne plate-forme prise en charge.
- Java Runtime Environment est mis à jour vers la version 11. Les autres bibliothèques et composants tiers sont également mis à jour pour garantir la sécurité et les bonnes performances du système.
- Plusieurs corrections et améliorations mineures.

#### **1.11.4 (12.2019)**

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

#### **1.11.3 (12.2019)**

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

#### **1.11.2 (10.2019)**

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

#### **1.11 (08.2019)**

- Ajout d'une prise en charge complète de l'IPv6.
- Ajout de la prise en charge de Zabbix 4.0.
- Ajout de la prise en charge de AWS CloudHSM (module de sécurité matérielle basé sur le cloud).
- Ajout de la prise en charge d'une large gamme de jetons matériels basés sur la norme PKCS#11.
- Suppression de la fonction de services centraux qui n'était pas utilisée dans la pratique.
- Amélioration de l'emballage des composants UXP. L'emballage est désormais plus modulaire et seuls les modules essentiels sont installés pour chaque composant UXP.
- Ajout d'un nouveau profil de certificat UXP par défaut `ee.cyber.uxp.common.certificateprofile.impl.UxpCertificateProfileInfoProvider`.



- Le jeu de caractères des identifiants UXP est désormais limité à [a-zA-Z0-9\_-]. Ceci s'applique à l'identificateur d'instance, à la classe de membre, au code de membre, au code de sous-système, au code de groupe et au code de serveur.
- Correction de l'horodatage du type de média dans le manifeste des conteneurs ASiC produits par les serveurs de sécurité UXP.
- Mise en œuvre de diverses améliorations mineures et corrections de bogues.
- Versions des bibliothèques et composants tiers mises à jour afin de garantir la sécurité du système.
- Documentation améliorée (UXP-UG-RS, UXP-IG-SS, UXP-IG-SS, UXP-UG-SS, UXP-UG-PMA, UXP-IG-MS). Ajout de l'aide en ligne UXP-UG-PMA sur le serveur de sécurité.

## 1.10 (12.2018)

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

## 1.9 (06.2018)

- Le système de gestion des licences est amélioré.
  - Il est possible de déléguer la signature des licences à une autre entité.
  - Différents produits installés sur la même machine peuvent utiliser des licences distinctes.
  - Les licences peuvent être visualisées et gérées dans l'interface utilisateur.
- Le système de surveillance prend en charge la version 6.x des outils Elasticsearch et Kibana.
- La surveillance locale permet d'obtenir des statistiques plus détaillées sur les transactions.
- Ubuntu 14.04 n'est plus une plate-forme prise en charge.
- Les guides d'utilisation et d'installation contiennent des informations plus détaillées et sont restructurés pour une meilleure lisibilité.
- Le guide de l'utilisateur est également accessible à partir de l'interface utilisateur en tant qu'aide en ligne.
- Les bibliothèques et frameworks tiers sont mis à jour.

- Plusieurs améliorations mineures de la convivialité, des performances et de la sécurité.

## **1.8 (10.2017)**

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

## **1.7 (06.2017)**

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

## **1.6 (05.2017)**

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

## **1.5 (03.2017)**

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

## **1.4 (10.2016)**

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

## **1.3 (07.2016)**

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

## **1.2 (04.2016)**

- Le Serveur de surveillance UXP est introduit.  
Les serveurs de sécurité envoient des informations de surveillance au Serveur de surveillance UXP qui les met à la disposition de Zabbix. Aide à la collecte et à l'analyse des statistiques sur les transactions. Des informations statistiques sur les transactions sont collectées, analysées et visualisées.

## **1.1 (03.2016)**

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

## 1.0 (12.2015)

- Première publication des composants principaux UXP.